Universidade do Minho
Escola de Engenharia

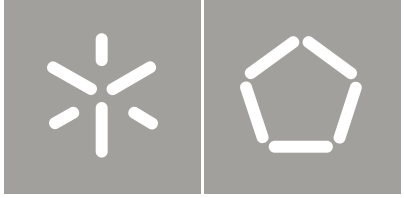
Isabel Maria Lopes

Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal

Janeiro de 2012

Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal
Isabel Maria Lopes

UMinho | 2012



Universidade do Minho
Escola de Engenharia

Isabel Maria Lopes

Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal

Tese de Doutoramento
Tecnologias e Sistemas de Informação
Engenharia e Gestão de Sistemas de Informação

Trabalho efectuado sob a orientação do
Professor Doutor Filipe de Sá-Soares

Janeiro de 2012

Dedico este trabalho à memória da minha mãe.
Expressando desta forma a saudade
e a falta que sinto pela sua ausência.

Agradecimentos

Durante o desenvolvimento deste trabalho recebi o apoio de diversas pessoas. Cabe-me aqui deixar expresso o meu reconhecimento a todos aqueles que, directa ou indirectamente, contribuíram para a realização deste trabalho.

Ao Professor Filipe de Sá-Soares por uma orientação à qual só consigo, sinceramente, apontar virtudes. Agradeço o apoio, a partilha do saber, disponibilidade, correcções e as valiosas contribuições para este trabalho. Acima de tudo, obrigada por me dar força para continuar em alturas menos positivas.

A Direcção da Escola Superior de Tecnologia e de Gestão do Instituto Politécnico de Bragança nas pessoas do Professor Albano Alves e da Professora Maria João Varanda pela facilidade nos horários lectivos que me permitiram ter mais tempo livre para dedicar a este trabalho.

Ao Directores de Departamento de Informática e Comunicações da Escola Superior de Tecnologia e de Gestão do Instituto Politécnico de Bragança, por me terem proporcionado as condições para desenvolver este trabalho.

Aos Docentes da parte lectiva do Doutoramento da Escola de Engenharia da Universidade do Minho, Professor João Álvaro Carvalho, Professor Luís Amaral, Professor Rui Dinis, Professora Isabel Ramos, Professor Henrique Santos e Professor Filipe de Sá-Soares, pelo muito que me ensinaram na parte lectiva deste doutoramento.

Aos meus colegas do Doutoramento e às funcionárias do Departamento de Sistemas de Informação da Universidade do Minho por toda a simpatia e carinho demonstrado.

Aos meus colegas do Instituto Politécnico de Bragança pelo apoio em momentos pontuais, e acompanhamento contínuo deste trabalho, nomeadamente o João Rocha, Luísa Miranda, Paulo Pereira.

Aos inquiridos (308) e aos entrevistados (44) das Câmaras Municipais, que sem a sua disponibilidade e contributo era impossível a realização deste trabalho de investigação.

A todos os meus amigos pelo apoio e incentivo incondicional durante este período nomeadamente à Beatriz Cachim, Regina Ferreira, Luís Moreno, Dr. José Moreno, Catarina Parreira, Fernanda Costa, Alice Pires, Teresa Fernandes, Adriana Ferreira, Carolina Cordeiro, Maria Teresa, Eng. Rui Caseiro, Eugénia Afonso.

Ao Pedro Oliveira, obrigada pelo amor, alegria e atenção sem reservas.

A todos os amigos que contribuíram com traduções, empréstimo de documentação, transcrição de entrevistas e outros apoios pontuais, nomeadamente ao Professor Luís Canotilho, Eng. Jorge Nunes, Pedro Santos, Dr. Nuno Reis, Dr.ª Estefânia Gomes,

Francisco de Assis. Agradeço também à Associação Nacional de Municípios Portugueses pela disponibilidade de informação.

Sou muito grata à minha avó Maria Luísa (in memorian), à minha mãe Lucília Lopes (in memorian) que faleceu ao longo do processo de escrita deste trabalho e ao meu pai Raul Lopes, os meus pilares e amores da minha vida. Ao meu irmão Amilcar Lopes e à minha sobrinha Isa Lopes estendo também os agradecimentos. Um agradecimento também aos meus Padrinhos e primos.

A todos os outros que, embora não sejam referidos, contribuíram de alguma forma para que fosse possível a concretização deste trabalho, estimulando-me intelectual e emocionalmente.

Um bem-haja, muito bem-haja, a todos.

Orientador
Prof. Filipe de Sá-Soares

Autora
Isabel Lopes

Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal

Resumo

Nas últimas décadas, com a crescente dependência das organizações dos seus Sistemas de Informação (SI), o valor da informação assumiu uma importância vital para as organizações. A atenção das organizações, que era focada primordialmente nos seus activos tangíveis (físicos e financeiros), passou também a focar-se no activo informação.

A Segurança de Sistemas de Informação (SSI) é um tema crítico a ter em conta nas organizações de todo o mundo. Face à importância das tecnologias de informação para o negócio e à utilização massiva da Internet e dos serviços que lhe estão associados, o número de ameaças que a informação está sujeita é cada vez mais elevado e consequentemente a necessidade de proteger os sistemas de informação torna-se mais premente.

Tanto ou mais importante que atingir os níveis de segurança de informação adequados a cada organização, é conseguir mantê-los. Não basta ter software e hardware que contribua para a segurança da informação, mas também uma política de segurança e uma boa gestão da segurança, de forma a alicerçar devidamente os esforços de protecção dos activos do Sistema de Informação.

No que diz respeito à Administração Pública Local, os munícipes esperam das autarquias o desenvolvimento e modernização dos seus SI, com vista a que a disponibilização de diversos serviços de forma interactiva e *online* se torne numa realidade cada vez mais acessível a todos e que a segurança dos dados associados a esses serviços tenha sido devidamente considerada.

No domínio da investigação observa-se um número razoável de estudos sobre a temática das políticas de segurança, contudo, o número de estudos é reduzido no que diz respeito a trabalhos empíricos acerca das questões de adopção de políticas de segurança. No caso da Administração Pública Local em Portugal, esses estudos são praticamente inexistentes.

Dada a ausência de estudos sobre esta temática nas Câmaras Municipais, foi elaborado e realizado um inquérito às 308 edilidades municipais, tendo por finalidade contribuir para a constituição de uma base de reflexão acerca das opções de investigação a desenvolver em torno da temática da "Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal".

O principal objectivo do inquérito foi a obtenção de resposta à seguinte questão: As Câmaras Municipais Portuguesas têm implementadas políticas de SSI? Com base no levantamento efectuado concluiu-se que das 308 Câmaras Municipais de Portugal, 12% (38) indicaram dispor de políticas de SSI e 88% (270) indicaram não ter ou ainda se encontrarem em processo de formulação da política para posterior implementação.

Esta constatação deu origem ao problema de investigação que se funda na reduzida adopção de políticas de SSI por parte dos Municípios em Portugal. A diluição do problema de investigação implicou satisfazer os seguintes objectivos: identificar as componentes e características das políticas de segurança existentes; identificar factores que afectam a adopção de políticas de SSI por parte das Câmaras Municipais, classificar esses factores e propor um enquadramento para auxiliar na compreensão da adopção de políticas de SSI nas Câmaras Municipais.

Para se alcançarem os objectivos mencionados, este trabalho passou, para além da realização do levantamento já referido, por mais dois momentos fundamentais. O segundo momento consistiu na realização de 44 entrevistas semi-estruturadas, conduzidas presencialmente, gravadas, transcritas e posteriormente codificadas. O objectivo da realização das entrevistas foi recolher um conjunto de dados que possibilitasse dar resposta a questões intrínsecas ao problema de investigação.

O terceiro momento fundou-se na recolha de políticas de SSI junto das Câmaras Municipais. O objectivo desta recolha foi, para além de verificar as características e componentes presentes nestes documentos, aferir-se a homogeneidade entre eles e com isso propor-se um modelo base de política de SSI a seguir pelos Municípios.

Depois de concluído o percurso de investigação descrito, constatou-se que não existe uma única política ou modelo base partilhado pelos Municípios que já aprovaram ou se preparam para aprovar uma política de SSI. Com efeito, a inexistência de um modelo de referência que possa ser seguido pelas autarquias constitui um obstáculo à adopção de políticas de SSI à escala administrativa local.

Assim, a adopção por via legislativa ou por recomendação da Associação Nacional de Municípios Portugueses de um modelo coerente, uniforme e flexível de políticas de SSI para as Câmaras Municipais, constituiria um contributo ou passo decisivo para a institucionalização dessas políticas.

Neste trabalho de investigação evidenciam-se como principais contributos, para além dos dois modelos base de política de SSI, o destaque no que diz respeito ao conteúdo das políticas, processo e contexto na sua adopção.

Advisor
Prof. Filipe de Sá-Soares

Author
Isabel Lopes

Uptake of Information Systems Security Policies in the Local Public Administration in Portugal

Abstract

Due to the growing dependence of organizations on their Information Systems (IS), the value of information assumed a vital importance to the organizations in the last decades. The organizations, which used to focus their attention mainly on their tangible assets (physical and financial), are now focusing their attention on the information asset.

Information Systems Security (ISS) is a critical issue to bear in mind in the organizations all around the world. With the information technology advent and the increasingly massive use of the Internet and its services, the number of attacks to which information is subject is higher and higher and, consequently, the need to protect information systems is now more important than ever.

Being able to maintain the information security levels adequate to each organization has become as important, or perhaps even more important than reaching those levels in the first place. Having the right software and hardware for information security is not enough. There must also be a security policy and a good security management in order to effectively lay the foundations of the efforts for the protection of IS assets.

As far as Local Public Administration is concerned, what citizens expect from their local government is the development and updating of their IS, hoping that the offer of several online interactive services becomes a reality available to all, and that the security of the data used in those services has been carefully handled.

In the IS research domain, there is a reasonable number of studies into the security policies theme. However, the number of studies is reduced when we consider empirical works related to the uptake of security policies. With respect to Local Public Administration in Portugal, these studies are almost inexistent.

In consequence of the absence of studies into this area in the Town Councils, a survey was made and carried out in 308 municipalities, aiming to contribute to the establishment of a basis for reflection on the research options to be developed concerning the theme “Uptake of Information Systems Security Policies in the Local Public Administration in Portugal”.

The main goal of this survey was to obtain an answer to the following question: “Do the Portuguese Town Councils have ISS policies implemented?” The results of the survey showed that 12% (38) of the 308 Town Councils in Portugal reported having ISS policies and 88% (270) reported either not having any ISS policy implemented, or still being in the process of creating one for further implementation.

These conclusions gave place to a research problem consisting in the reduced levels of ISS policies uptake by the Portuguese municipalities. The solution to this research problem implied the achievement of the following goals: identify the components and features of the existent security policies; identify factors which affect the uptake of ISS policies by the Town Councils, classify those factors and propose a framework to help understand the uptake of ISS policies by the Town Councils.

In order to achieve these goals, and apart from the referred survey, this work went through two more key moments. The second moment consisted in holding 44 semi-structured interviews, conducted personally, recorded, transcribed and then codified. The purpose of the interviews was to collect data that would enable us to answer the intrinsic questions of the research problem.

The third moment was grounded in collecting ISS policies by the municipalities. Apart from verifying the characteristics and components of these documents, the purpose of this data collection was to assess the homogeneity among them, and thus propose an ISS policy model to be followed by the Town Councils.

After completing the course of research described above, the conclusion was that there is not a single policy or model that is shared by the Town Councils which have approved or are preparing to approve an ISS policy. Indeed, the inexistence of a reference model which can be followed by the municipalities represents an obstacle to the uptake of ISS policies on a local administration scale.

Therefore, the uptake of a coherent, uniform and flexible model of ISS policies by the Town Councils, whether it is through legislation or on recommendation from the National Association of Portuguese Municipalities, would represent a contribution or a decisive step towards the institutionalization of such policies.

The main contributions of this research work lie on the two ISS policy models presented, and on the emphasis regarding the policies content, as well as their uptake process and context.

Índice

Índice de Figuras

Índice de Gráficos

Índice de Tabelas

Capítulo 1

Introdução

1.1 Enquadramento

A existência de Tecnologias e Sistemas de Informação (TSI) cada vez mais sofisticados e modernos que facilitem a recolha, armazenamento, processamento e disseminação de informação é crucial para o bom desempenho de uma organização.

No que concerne à Administração Pública Local, os munícipes esperam das autarquias o desenvolvimento e modernização dos seus Sistemas de Informação (SI), com vista à disponibilização de serviços que melhorem o seu bem-estar e a sua qualidade de vida. Para a satisfação deste propósito, defende-se que as tecnologias e sistemas utilizados têm de transmitir confiança aos munícipes, pelo que se torna necessário considerar aspectos relacionados com a segurança da informação e dos sistemas e tecnologias que manipulam essa informação.

A definição e implementação de mecanismos de Segurança de Sistemas de Informação (SSI) é uma preocupação que muitas vezes é deixada para segundo plano nas opções dos investimentos em TSI, ficando assim os SI sujeitos mais intensamente a ameaças e ataques de várias ordens [Veiga 2004]. Na verdade, muitas vezes as organizações desenvolvem o seu negócio e implementam soluções de segurança de acordo com necessidades pontuais, não definindo políticas, estratégias, normas, procedimentos, isto é, não contemplando expressamente a SSI.

No caso particular das autarquias, onde a informação pública e pessoal deve ser protegida pelos responsáveis, deve haver a preocupação de entender a segurança como algo a considerar, logo desde o início, nas actividades de planeamento e desenvolvimento de SI.

Há várias directrizes e medidas que podem e na verdade precisam de ser implementadas nas organizações para assegurar o funcionamento efectivo da SSI. Segundo Höne e Eloff [2002a, p. 402], “estas medidas abrangem desde soluções técnicas e regulamentos contratuais até advertências organizacionais de riscos usuais, ameaças e vulnerabilidades. Indubitavelmente a singularidade mais importante destas directrizes é a política de segurança da informação”. Assim, exige-se a aplicação de diferentes mecanismos de protecção, detecção e reacção, bem como a formulação de políticas de segurança que contribuam para a preservação da confidencialidade, integridade e disponibilidade da informação [Carneiro 2002].

De acordo com o *Joint Information Systems Committee* do Reino Unido, uma política de segurança da informação é um documento orientador dos esforços de protecção do Sistema de Informaçã da organização, mediante o enunciado do compromisso e apoio da gestão à segurança da informação e a definição do papel da

segurança da informação no alcance e apoio da visão e missão da organização [JISC 2001].

Neste contexto, uma política de segurança deve descrever a forma adequada de utilização dos recursos do Sistema de Informação, as responsabilidades e direitos dos utilizadores, os activos a proteger e os procedimentos a manter e a desenvolver com o objectivo de concorrer para um nível de SSI adequado [Carneiro 2002; Diver 2007; Kee 2001].

Após a definição, elaboração e aprovação de uma política de segurança, é necessária a sua implementação e, posteriormente, o recurso a auditorias internas e externas que verifiquem se as políticas de segurança estão a ser aplicadas de modo correcto e adequado.

O presente estudo tem por âmbito a Administração Pública Local, pelo que principiará por definir o que se entende por esta estrutura. Antes de definir o conceito na sua globalidade, é necessário compreender o que se entende por Administração. Segundo Caupers [1998, p. 30], administrar é uma "actividade que se caracteriza pela combinação de meios humanos, materiais e financeiros levada a cabo no seio de uma organização; administrar é uma acção humana que consiste exactamente em prosseguir certos objectivos através do funcionamento da organização".

A natureza das organizações contempla organizações privadas e públicas. Relativamente à Administração Pública, ainda segundo o autor anteriormente citado, existem duas grandes formas de entender a expressão: o sentido orgânico e o sentido material ou funcional. A Administração Pública em sentido orgânico é constituída "pelo conjunto de órgãos, serviços e agentes do Estado e demais entidades públicas que asseguram, em nome da colectividade, a satisfação disciplinada, regular e contínua das necessidades colectivas de segurança, cultura e bem-estar" [Caupers 1998, p. 33]. A Administração Pública em sentido material ou funcional "compõe-se do conjunto de acções e operações desenvolvidas pelos órgãos, serviços e agentes do Estado e demais entidades públicas e ainda por outras entidades para tanto habilitadas por normas de direito público" [Caupers 1998, p. 34]. Segundo Freitas do Amaral [1989], a Administração Pública é composta em sentido orgânico ou subjectivo por várias instituições públicas – o Estado, os institutos públicos, as associações públicas, as autarquias e as regiões autónomas.

Por sua vez, é habitual falar-se em administração central e em administração local, a primeira operando em todo o território nacional e a segunda sendo composta por entidades públicas territoriais (administração autárquica) e serviços da administração estatal (administração periférica do Estado).

Na Enciclopédia VERBO da Sociedade e do Estado [Polis 1983], Administração Local e Administração Pública são apresentadas separadamente, sendo a primeira definida num duplo sentido, considerando Administração Local do Estado e Administração Local Autárquica. A Administração Local do Estado decorre da descentralização de poderes pelos órgãos centrais do Estado nos órgãos locais das hierarquias do Estado. A Administração Local Autárquica é resultante da descentralização pelo Estado nas autarquias locais das atribuições relativas aos

interesses das respectivas populações. No primeiro entendimento está-se sempre dentro da pessoa colectiva Estado; no segundo entendimento passa-se do Estado para uma outra pessoa colectiva e autónoma em relação a ele: a autarquia local. Relativamente à designação de Administração Pública, toma-se em diversas acepções: em sentido material – designa o poder público empenhado na satisfação imediata de interesses da comunidade heteronomamente fixados; em sentido organizacional – é o complexo de órgãos que no Estado e nas outras pessoas públicas recebe o encargo específico de desempenhar essa função; em sentido funcional – designa a actividade destes órgãos administrativos.

Descendo-se na hierarquia do Estado, encontram-se as Autarquias, órgãos da Administração Pública Local. Na Constituição da República Portuguesa as autarquias locais são "pessoas colectivas territoriais dotadas de órgãos representativos, que visam a prossecução de interesses próprios das populações" [CPR 2005, artigo 235.º].

As categorias de autarquias locais e a divisão administrativa são definidas também na Constituição da República no artigo 236.º, da seguinte forma: "No continente as autarquias locais são as freguesias, os municípios e as regiões administrativas. As regiões autónomas dos Açores e da Madeira compreendem freguesias e municípios. Por sua vez os órgãos representativos do município são a Assembleia Municipal e a Câmara Municipal."

O presente estudo incidirá somente sobre as Câmaras Municipais, que se posicionam hierarquicamente em relação à Administração Pública da forma indicada na Figura 1.

Administração Pública	Central			
	Local	Autarquias	- Freguesias - Regiões Administrativas - Municípios	-Assembleia Municipal - *Câmara Municipal*

Figura 1: Posicionamento Hierárquico das Câmaras Municipais

A divisão territorial em Portugal é feita através de distritos e de regiões autónomas, sendo o número de distritos dezoito e as regiões autónomas duas (os Açores e a Madeira). Em relação aos municípios, o território está dividido em 308 entidades. A divisão territorial do país por distrito, município e a respectiva população residente encontram-se listadas no Apêndice A.

Existem estudos em Portugal, promovidos por entidades governamentais, que analisam a utilização das Tecnologias de Informação (TI) nas Câmaras Municipais. Estes estudos focam-se na presença das Câmaras na Internet e abordam sucintamente a segurança da informação. O ano de 2004 ficou na história da Sociedade da Informação como o ano da sua generalização concelhia, dado que pela primeira vez

se registou um índice de 100% de Câmaras Municipais ligadas à Internet [OSIC e UMIC 2004].

Em 2007, o número de Câmaras Municipais com endereço Web conhecido é de 306, o que representa 99,4% das Câmaras só 0,6, ou seja, duas Câmaras é que não tem endereço Web [Santos e Amaral 2008].

E quando se fala em Internet, fala-se necessariamente de protecção de dados. Ao nível da presença camarária na Internet, 51% dos respondentes indicaram que os seus *websites* contemplam os requisitos relativos à protecção de dados pessoais, mas apenas 15% indicou dispor de capacidade para garantir transacções seguras [OSIC e UMIC 2006]. Os *websites* autárquicos são actualizados permanentemente em 80% dos casos, uma vez por mês em 6% dos casos e de 15 em 15 dias em 8% dos casos.

No mesmo estudo, a preocupação em relação aos recursos humanos surge sublinhada pelo facto de 80% das Câmaras Municipais terem já pessoal afecto exclusivamente às TIC[1] e 39% considerarem que a inexistência ou a escassez de pessoal das TIC tem condicionado negativamente o desenvolvimento das suas actividades. Dois terços das autarquias, ou seja, 67% do total, têm uma estratégia específica para o desenvolvimento das TIC. Entre os trabalhos em desenvolvimento, 84% dão prioridade aos serviços ao cidadão via Internet, 80% à implementação de uma política de segurança na utilização das TIC e 46% à formação e certificação nas TIC. O último posto do *ranking* vai para o *e-commerce*, com apenas 18% do total.

Apesar de a Internet já ser uma realidade em todas as autarquias, o respectivo acesso generalizado situa-se nos 79%, e os trabalhadores que utilizam regularmente a Internet é de 28%. Nas actividades realizadas através da Internet destacam-se a procura e a recolha de informação (99% do total de respostas), o acesso ao correio electrónico (98% do total) e a troca electrónica de ficheiros (96% do total).

No que diz respeito aos requisitos contemplados no *Website*, segundo o mesmo estudo, a capacidade para garantir transacções seguras é de apenas 5% de forma total e 10% de forma parcial, o que implica que 85% das Câmaras inquiridas não têm essa capacidade. Relativamente à protecção de dados pessoais, 39% das Câmaras Municipais não contempla esta protecção nos seus *Websites*.

A detecção de problemas de segurança conta com um índice de 11%, destacando-se como principais problemas os ataques de vírus informáticos, resultando na perda de informação ou de horas de trabalho (71% do total) e o acesso não autorizado à rede de computadores ou a dados do organismo (18% do total de respostas).

Relativamente à implementação de políticas de SSI só se conhece a vontade e prioridade, faltando saber se essa intenção está a ser posta ou não em prática, bem como a forma como é elaborada, implementada e avaliada essa política de SSI.

[1] Neste trabalho optou-se pela designação TI (Tecnologias da Informação) em detrimento da designação TIC (Tecnologias da Informação e da Comunicação) por se entender que a primeira expressão já inclui as tecnologias de comunicação da informação. Todavia, por uma questão de rigor documental utilizar-se-á a designação TIC quando se estiverem a referir resultados de estudos que tenham empregado esse acrónimo em vez de TI.

1.2 Motivação da Investigação

No domínio da investigação em SSI observa-se a existência de um número considerável de estudos que se debruçaram sobre a temática das políticas de segurança [de Sá-Soares 2005]. Estes estudos abordam tópicos diversificados, nomeadamente, a importância das políticas, responsabilidades no desenvolvimento de políticas, tipos de políticas, principais elementos constituintes, método a seguir na formulação e implementação de uma política, tempo de vigência, quem tem de aprovar uma política, e características e factores a considerar para o sucesso dessa política de segurança. Contudo, o número de estudos é reduzido no que diz respeito a trabalhos empíricos sobre adopção de políticas de segurança. Esta constatação aplica-se também à falta de investigação substanciada acerca dos factores que afectam, positiva ou negativamente, a formulação e implementação bem sucedida de uma política.

O exposto foi já assinalado por diversos autores, os quais têm apontado certas limitações à investigação efectuada nessa área. As principais críticas prendem-se com a ausência de uma teoria coerente sobre políticas de segurança [Hong et al. 2003], com a inexistência ou reduzida expressão de estudos empíricos sobre a adopção, conteúdos e implementação de políticas de Segurança de Sistemas de Informação [Fulford e Doherty 2003; Knapp et al. 2006], falta de investigação em segurança da informação suportada empiricamente [Kotulic e Clark 2004] e com uma preocupação demasiado centrada nas questões do conteúdo e estrutura das políticas e no problema da obtenção de apoio da gestão no que respeita à formulação, implementação e cumprimento das políticas [Baskerville e Siponen 2002].

Embora as críticas à falta de investigação sobre políticas de SSI e à inexistência de estudos empíricos sobre essa área sejam frequentes, da revisão que se efectuou da literatura parece assistir-se a dificuldades no sentido de inverter esta situação.

Na sequência desta sugestão, este trabalho visa contribuir para colmatar esta falha, procurando-se desenvolver um trabalho de investigação que tenha em conta estas críticas, designadamente no que respeita à condução de estudos empíricos e à contextuação da aplicação das políticas de segurança.

Refere-se, ainda, que o trabalho desenvolvido pela autora aquando da preparação da dissertação de Mestrado, que versou a temática da SSI, bem como o contacto directo da autora com a realidade autárquica portuguesa, em consequência do desempenho de funções executivas num Município, concorreram de forma decisiva para o estudo e aprofundamento de conhecimentos no domínio científico da SSI.

Assim, pretende-se com este trabalho estudar o processo de adopção de políticas de SSI, não a nível geral das organizações, mas sim, num ambiente específico, que é a Administração Pública Local em Portugal, onde a existência de investigação nesta área é quase inexistente.

1.3 Objectivos

Da problemática que motivou a realização deste trabalho de investigação decorre um conjunto de objectivos a atingir, os quais se enunciam seguidamente.

- Estabelecimento de um quadro teórico inicial para o estudo das práticas de SSI na Administração Pública Local em Portugal, com especial incidência no que respeita à adopção de políticas de segurança;
- Identificação das componentes e características das políticas de SSI existentes na Administração Pública Local;
- Identificação de factores que condicionam a adopção de políticas de SSI por parte das Câmaras Municipais;
- Classificação dos factores condicionadores da adopção de políticas de SSI por parte das Câmaras Municipais e
- Proposta de um enquadramento para auxiliar na compreensão da adopção de políticas de SSI na Administração Pública Local em Portugal.

Para conseguir alcançar estes objectivos, julga-se necessário, para além da revisão da literatura, efectuar trabalho de campo, utilizando para esse efeito as estratégias de investigação que se coadunam com os objectivos a alcançar com este estudo. Os métodos e técnicas de investigação que se pretendem empregar neste trabalho de investigação são apresentados na secção seguinte.

1.4 Concepção da Investigação

As várias estratégias de investigação existentes definem um conjunto de métodos, técnicas e ferramentas para conduzir o processo de investigação. A adopção de um particular método de investigação, e respectivas técnicas associadas, está condicionada pela perspectiva filosófica adoptada pelo investigador, pelo objectivo do estudo e, principalmente, pelos objectivos da investigação [Caldeira e Romão 2002]. Tendo em conta os objectivos formulados anteriormente, julga-se que os métodos e técnicas que de seguida se enumeram se revestem de utilidade e relevância para a condução deste trabalho:

- Método de Investigação
    - Estudo de Casos
- Técnicas de Investigação
    - Inquérito
    - Recolha de documentos
    - Entrevistas

Relativamente ao método de investigação enunciado anteriormente, considera-se útil para esta investigação, uma vez que o método de investigação Estudo de Caso, e

conforme é definido por Benbasat et al. [1987], consiste numa estratégia de investigação que examina um fenómeno no seu estado natural, empregando múltiplos métodos de recolha e tratamento de dados sobre uma ou várias entidades (pessoas, grupos ou organizações). Este método é assim considerado o mais adequado para este trabalho, uma vez que se pretende estudar a problemática das políticas de SSI no contexto real da sua utilização.

No que concerne às técnicas de investigação propostas, a análise de documentos é fundamental para um melhor conhecimento dos documentos existentes. Para tal, será necessário fazer a recolha, leitura e análise dos documentos organizacionais considerados como políticas de SSI. Posteriormente, e de forma a aprofundar a temática em estudo, a entrevista a participantes nos processos de adopção de políticas de SSI nas Câmaras Municipais de Portugal será crucial. A transcrição das entrevistas e posterior análise com recurso a uma aplicação informática vocacionada para o apoio à análise de dados qualitativos, permitirá de forma mais ágil analisar as mesmas.

Para a execução do presente trabalho, procedeu-se ao levantamento dos dados através da concretização de um inquérito a cada uma das 308 Câmaras Municipais existentes, da recolha de 25 documentos de política de SSI e da realização de 44 entrevistas a responsáveis autárquicos pelas tecnologias e sistemas de informação.

1.5 Organização da Tese

Nesta secção descreve-se a organização deste trabalho de investigação e sintetiza-se o conteúdo dos nove capítulos que o consubstanciam. A forma como se encontram organizados é a seguinte:

Capítulo 1 (o presente) – É efectuada uma breve introdução, onde se estabelecem as motivações e o enquadramento do presente trabalho, identificando-se os objectivos, problema da investigação e a concepção da investigação.

Capítulo 2 – Apresenta-se a fundamentação do estudo, através da revisão da literatura, explanando-se desta forma o estado de conhecimento sobre políticas de SSI e estabelecendo-se as definições adoptadas para os conceitos cruciais em que a revisão da literatura se alicerça. Visa-se, desta forma, enquadrar conceptualmente esta investigação. Concretamente, aborda-se de forma mais destacada a revisão da literatura no que respeita à Formulação, Implementação e Revisão de políticas de SSI.

Capítulo 3 – É apresentada neste capítulo uma breve descrição que caracteriza as Câmaras Municipais em Portugal. As características principais como a dimensão dos Municípios, o seu financiamento e o perfil dos dirigentes Autárquicos são alguns dos assuntos revistos, as tecnologias e segurança dos sistemas de informação nas Câmaras são também abordados, através da apresentação de dados e legislação que regulamentam estas temáticas.

Capítulo 4 – São apresentadas as conclusões do levantamento realizado sobre políticas de SSI nas Câmaras Municipais em Portugal. Previamente, explanam-se as

estratégias de investigação e a população alvo deste estudo, e por último os resultados do inquérito, com a devida análise das respostas dos inquiridos.

Capítulo 5 – Elabora-se sobre os métodos e técnicas de investigação utilizados no presente estudo, discutindo-se as razões que levaram à sua selecção, as suas principais características e aspectos relacionados com o rigor, a validade e generalidade das conclusões que permitem alcançar.

Capítulo 6 – Debruça-se sobre prescrições intra-organizacionais no domínio de estudo deste trabalho, designadamente políticas de SSI. As políticas são inicialmente analisadas individualmente, seguindo-se a análise conjunta da totalidade dos documentos recolhidos.

Capítulo 7 – Apresenta os resultados da análise das entrevistas conduzidas no terceiro instante de geração de dados levado a cabo neste trabalho com o intuito de compreender com mais profundidade os factores que influenciam a adopção de políticas de SSI na Administração Pública Local em Portugal.

Capítulo 8 – É apresentada a discussão dos dados recolhidos no levantamento, nos documentos e nas entrevistas. É feita a análise crítica face a literatura sobre políticas. Por fim, são feitas recomendações sobre as componentes e as características que devem ter uma política de SSI, através da proposta de dois modelos de políticas de SSI a adoptar pelas Autarquias. Nas recomendações para além da vertente do conteúdo das políticas, avançou-se também com recomendações na vertente do processo e do contexto para a adopção de políticas de SSI.

Capítulo 9 – São apresentadas as conclusões, resumem-se as contribuições do trabalho realizado, identificam-se as limitações do estudo e discutem-se oportunidades para investigação futura

Apêndices e Referências – No Apêndice A é apresentada uma tabela onde são listados os municípios pertencentes a cada Distrito, bem como a população residente e eleitoral em cada um desses Distritos. O Apêndice B lista um conjunto de normas de Segurança de Sistemas de Informação. O Apêndice C apresenta as normas que abordam em particular as Políticas de Segurança de Sistemas de Informação. O Apêndice D lista o conteúdo do Artigo 64.º da Lei n.º 169/99, de 18 de Setembro, com as alterações introduzidas pela Lei n.º 5-A/2002, de 11 de Janeiro, que estabelece o quadro de competências dos órgãos das freguesias e dos municípios, com destaque, naturalmente, para a Assembleia Municipal e para a Câmara Municipal. O Apêndice E apresenta o total de fundos afectos a cada um dos Municípios Portugueses, listados por Distrito. O Apêndice F apresenta o Inquérito efectuado às Câmaras Municipais. O Apêndice G apresenta o *CodeBook* elaborado para a codificação das entrevistas. O Apêndice H apresenta o conteúdo das Políticas de Segurança, presente nos documentos recolhidos. O Apêndice I apresenta dois modelos de Políticas de SSI. Por último, são apresentadas as referências citadas neste trabalho.

Capítulo 2

Fundamentação do Estudo

2.1 Introdução

No capítulo anterior estabeleceram-se as motivações e o enquadramento do presente trabalho, identificando-se os objectivos e sintetizando-se a concepção da investigação. No presente capítulo, que precede a caracterização das Câmaras Municipais Portuguesas, apresenta-se a revisão da literatura relevante para a temática de investigação identificada, explanando-se o estado de conhecimento sobre políticas de SSI.

Da investigação empreendida em torno de trabalhos de investigação para a aferir o estado da arte, relativamente a políticas SSI, resultou a constatação de um número relevante de estudos nesta área, os quais, de forma diversa, vão abordando, avulsamente, temáticas como a importância das políticas, responsabilidades no desenvolvimento de políticas, tipos de políticas, principais elementos constituintes, método a seguir na formulação e implementação de uma política, tempo de vigência, quem tem de aprovar uma política e características e factores a considerar para o sucesso das políticas de segurança.

Nas últimas décadas, com a dependência em maior ou menor grau das organizações dos seus SI, o valor da informação assumiu uma importância vital para as organizações de todo o mundo. A atenção que anteriormente era focada primordialmente nos seus activos tangíveis físicos e financeiros passou a ser focada no activo informação. Neste contexto, as preocupações com a SSI acompanham esta evolução de forma ascendente, reflectindo-se, a título ilustrativo, no aparecimento de um número considerável de normas neste domínio [Macartney 2005].

Face ao exposto e aos propósitos deste projecto de investigação, o presente capítulo debruçar-se-á essencialmente sobre os tópicos dos SI, SSI e políticas de SSI, definindo-se, previamente, os conceitos cruciais para o presente trabalho.

2.2 Conceitos Fundamentais

Os conceitos de sistema de informação e segurança de sistemas de informação são de elevada relevância para esta investigação, uma vez que é sobre eles que se alicerça o presente trabalho.

Contudo, o consenso dentro da comunidade científica sobre a definição destes conceitos está longe de ser uma realidade. Seguidamente, apresentar-se-ão os entendimentos de diferentes investigadores, realçando-se as diferenças existentes entre os mesmos no que respeita aos conceitos de Sistema de Informação e

Segurança de Sistemas de Informação. Para cada um destes conceitos identificar-se-á a definição adoptada no âmbito deste estudo.

Os conceitos anteriormente referidos, bem como uma breve descrição do entendimento dos termos "sistema" e "informação", consubstanciam-se nas duas subsecções seguintes, com o propósito de clarificar as definições adoptadas nesta investigação.

2.2.1 Sistema de Informação

A expressão "sistema de informação" é composta pelos conceitos "sistema" e "informação", pelo que antes de se definir o seu significado conjunto, procede-se a uma definição de cada um daqueles termos de *per si*, clarificando-se assim, o entendimento dos mesmos neste estudo.

Neste trabalho assume-se a definição de Sistema proposta por Le Moigne [1990], o qual se insurge contra as designações que definem sistema como um conjunto, afirmando peremptoriamente que "Um sistema é um sistema, não é um conjunto" (p.76). Para Le Moigne, um sistema é:

alguma coisa	não importa o quê, presumivelmente identificável
que em alguma coisa	Ambiente
para alguma coisa	finalidade ou projecto
faz alguma coisa	actividade = funcionamento
por alguma coisa	estrutura = forma estável
que se transforma com o tempo	Evolução

Relativamente ao conceito de informação, segundo Carvalho [1999], é um objecto simbólico construído deliberadamente, externo à mente humana, de forma a facilitar a transmissão do conhecimento, as negociações do dia-a-dia e a gestão do conhecimento.

O conceito de informação acima difere do proposto pelo relatório FRISCO [Falkenberg et al. 1996]: A *Framework of Information System Concepts*, onde a informação é considerada como uma criação do conhecimento (incremento do conhecimento).

Na linha da definição anterior, neste trabalho assume-se a definição de Galliers [1987] para o termo informação que é o conjunto de dados que, quando fornecido de forma e a tempo adequado, melhora o conhecimento de quem a recebe.

O conceito de Sistema de Informação, composto pelos termos sistema e informação, apresenta um considerável número de definições, embora se venham a desenvolver esforços no sentido de encontrar uma definição que seja unanimemente aceite dentro da comunidade científica de SI, podendo-se apontar trabalhos de diversos investigadores, tais como, Carvalho [1999], Checkland e Holwell [1998], Falkenberg et al. [1996], Falkenberg et al. [2001], Khazanchi e Munkvold [2000] e Mingers e Stowell [1997].

Da pesquisa efectuada constata-se que as definições se situam basicamente entre dois níveis diferentes: no primeiro, a ênfase é colocada nos sistemas e tecnologias informáticas e no outro nível os sistemas sociais assumem o enfoque principal. Como exemplos desta última categoria encontram-se as definições de Buckingham et al. [1987, p. 18] que definem sistema de informação como "**…** um sistema que reúne, guarda, processa e faculta informação relevante para a organização (...), de modo que a informação é acessível e útil para aqueles que a querem utilizar, incluindo gestores, funcionários, clientes, (...). Um Sistema de Informação é um sistema de actividade humana (social) que pode envolver ou não a utilização de computadores". Dentro deste entendimento estão também os autores Angell e Smithson [1991] e Banville [1991].

Um autor que se aproxima do primeiro nível é Alter [1999], que define sistema de informação como uma combinação de procedimentos, informação, pessoas e tecnologias da informação organizadas para o alcance de objectivos de uma organização. Dentro desta perspectiva pode-se citar também os autores Ein-Dor e Segev [1993] que concebem um sistema de informação como um qualquer sistema informático que esteja ligado a pessoas.

Outro autor, Visala [1991, p. 349], define sistema de informação como um "sistema social e técnico que modela e fornece informação acerca de um universo", esta abordagem engloba os dois níveis anteriormente focados.

Dada esta diversidade de entendimentos, o relatório FRISCO [Falkenberg et al. 2001] considera que o conceito de sistema de informação é visto e definido de três formas diferentes, nomeadamente como:

> Um sistema técnico – implementado através de sistemas informáticos;
>
> Um sistema social – ligação da organização com as suas necessidades de informação;
>
> Um sistema conceptual – abstracção de uma das duas interpretações anteriores.

Numa perspectiva diferente, Amaral [1994] considera que um sistema de informação tem de ser visto e relacionado como o conceito de organização, uma vez que os dois são indistinguíveis.

Neste trabalho ter-se-á também em atenção os quatro objectos identificados e analisados por Carvalho [1999], que define Sistema de Informação segundo quatro prismas:

- SI 1 – É uma organização cujo negócio (propósito) consiste em fornecer informação aos seus clientes;
- SI 2 – É um subsistema organizacional que garante a comunicação entre o subsistema operacional e o subsistema de gestão. Trata-se de um subsistema

que existe em qualquer sistema autónomo (i.e., num sistema com capacidade de auto-governo);

- SI 3 – É qualquer artefacto que usa computadores e ou suportes apoiados em computadores para desempenhar actividades de manipulação (tratamento) de informação, entendida como objecto simbólico. Nesta perspectiva, o sistema de informação corresponde àquilo que é vulgarmente designado por sistema informático;

- SI 4 – É um subconjunto de uma organização que abarca todas as actividades que manipulam (tratam) informação. Se a organização lida apenas com informação, o Sistema de Informação 4 inclui todas as actividades organizacionais.

Das várias definições indicadas e de forma a sintetizar e clarificar o entendimento adoptado neste trabalho, propõe-se que um sistema de informação é um sistema social que tem a finalidade de realizar um conjunto de procedimentos que visam captar o que acontece na organização e no seu meio ambiente e apresentar de forma sucinta e organizada essa informação de forma a sustentar toda a actividade informacional, de modo mais ou menos automatizado.

2.2.2 Segurança de Sistemas de Informação

Previamente à definição de "políticas de segurança", procurar-se-á clarificar o que se entende por "segurança de sistemas de informação".

Da pesquisa efectuada sobre SSI, verifica-se que a sua denominação não é homogénea em todos os trabalhos de investigação. Os termos encontrados para além de SSI e que se passam a referenciar são: "segurança de computadores", "segurança da informação", "segurança de redes/informática" e "segurança de dados". Neste estudo o termo a utilizar será "Segurança dos Sistemas de Informação".

A ISO[2] (International Organization for Standardization) define segurança como a tentativa de minimizar a vulnerabilidade de valores e recursos, entendendo-se, neste domínio por vulnerabilidade o atributo de qualquer situação a partir da qual terceiros podem penetrar num sistema de informação sem qualquer autorização no sentido de tirar proveito do seu conteúdo ou das suas características [ISO/IEC 2005].

Para Mamede [2006], o termo segurança está associado a riscos e à prevenção e minimização dos mesmos. Segundo este autor, segurança significa "a existência de capacidade para se tomarem medidas preventivas que, se não forem suficientemente capazes para evitar as ocorrências indesejadas, maliciosas ou inesperadas, pelo menos prevejam acções a serem tomadas que minimizem as mesmas" (p.3).

[2] Procurando garantir que o acrónimo da Organização Internacional de Normalização não sofreria alterações, em consequência das diferentes traduções para as várias línguas, foi decidida a adopção de uma palavra derivada do grego *isos*, que significa "igual", pelo que independentemente do país ou da respectiva língua, o acrónimo da Organização será, sempre, ISO.

Outro entendimento, mais voltado para a organização, é proposto por Dhillon [1997, p. 88], que considera a SSI "como um estado de cuidado e protecção no que respeita às actividades de manipulação de informação de uma organização".

Outra definição que contempla meios para garantir a segurança, é apresentada por KPMG [2002], que define SSI como "as práticas, procedimentos e tecnologias que garantem que a informação está salvaguardada de acessos não autorizados, modificação ou alteração acidental, e que está prontamente disponível para utilizadores autorizados".

Por último, e na linha da definição anterior, encontra-se a definição proposta por Beatson [1992, p. 36], definição adoptada neste trabalho, em que se entende por segurança da informação o "enquadramento organizacional de cultura, políticas, estruturas organizacionais e ambiente operacional utilizado para assegurar a integridade, disponibilidade e confidencialidade da informação de uma organização", em suma, os meios necessários para garantir a integridade, disponibilidade e confidencialidade numa organização, sendo que um dos meios apontados são as políticas de SSI.

2.3 Políticas de Segurança de Sistemas de Informação

Nesta secção são abordadas várias temáticas relacionadas com políticas de SSI, nomeadamente a sua definição, importância, classificação das políticas, características e componentes de uma política de SSI, formulação, implementação, revisão e adopção de políticas, bem como os factores críticos de sucesso na adopção de políticas de SSI.

2.3.1 Definição

No Dicionário de Língua Portuguesa Contemporânea, o vocábulo política é definido como "orientação ou conjunto de directrizes que regem a actuação de uma pessoa ou entidade" [ACL 2001, p. 2897].

Para Guel [2007, p.3], uma política é considerada uma "declaração ou plano formal, breve e de alto nível que envolve as crenças gerais, metas, objectivos e procedimentos aceites por uma organização para uma área de um assunto específico."

Outra definição que vem de encontro às anteriores é apresentada por Gilbert [2003, p.3] que define política como "as regras e os procedimentos escolhidos que vão ditar acções futuras."

Quanto à definição de política de SSI podem-se apontar diferentes considerações, que se devem, segundo Baskerville e Siponen [2002], há existência de duas escolas de pensamento: a Escola Técnica/Segurança de Computadores e a Escola Não Técnica/Gestão da Segurança.

Escola Técnica/Segurança de Computadores

No âmbito desta escola, as políticas são as regras de controlo de acesso às componentes de um sistema informático, por exemplo em relação aos sistemas operativos. Dentro deste nível, enquadram-se as seguintes definições:

> As políticas de segurança são "linhas orientadoras quanto à protecção de dados e de recursos e devem indicar situações e/ou entidades de quem o sistema tem de estar protegido" [Carneiro 2002, p. 8].
>
> Uma política de segurança "estabelece o que deve ser feito para proteger a informação armazenada em um computador. Uma política bem escrita contém definição suficiente sobre "o que" fazer de modo que o "como" pode ser identificado e medido ou avaliado" [GIAC 2001, p. 3].
>
> Uma política de segurança, não é mais do que "uma estratégia bem escrita acerca da protecção e manutenção da disponibilidade da sua rede e dos seus recursos" [Bowden 2003, p. 1].
>
> Para o autor Bastos [2002], uma política de segurança é "uma série de normas internas padronizadas pela empresa que devem ser seguidas à risca para que todas as possíveis ameaças sejam minimizadas e combatidas efectivamente pela equipa de segurança."

Escola Não Técnica/Gestão da Segurança

No âmbito desta escola, as políticas são declarações ao nível da gestão em geral. Dentro deste nível, enquadram-se as seguintes definições:

> Políticas são "instruções de gestão que indicam como uma organização deve ser dirigida. São declarações de alto nível com o propósito de fornecer orientações, àqueles que devem tomar decisões presentes e futuras" [Wood 1995, p. 667].
>
> Uma política de segurança da informação é um documento orientador dentro de uma organização. É um documento que indica o compromisso e o apoio da gestão à segurança da informação, assim como, define o papel que a segurança da informação tem para alcançar e apoiar a visão e a missão da organização [JISC 2001].
>
> As políticas de SSI "consistem, fundamentalmente, em documentos que orientam ou regulam as acções das pessoas ou sistemas no domínio da SSI" [de Sá-Soares 2005 p. 56] (para os efeitos pretendidos com este trabalho, e atendendo-se à visão pessoal da autora, esta é a definição que se adopta para política de segurança de sistemas de informação).

De forma a melhor precisar o conceito de política de SSI, julga-se oportuno distingui-lo dos conceitos de normas, directivas e procedimentos. Na Tabela 1 apresenta-se um exemplo em que se visa ilustrar as diferenças entre estes conceitos no âmbito do acesso a sistemas por parte de utilizadores autorizados.

Política O acesso aos SI da organização é restrito a utilizadores autorizados.
Norma Os utilizadores autorizados necessitam de possuir um identificador único e uma *password* confidencial.
Directiva As *passwords* devem ser compostas por cinco a oito caracteres alfanuméricos.
Procedimento Os pedidos de identificador e *password* têm que conter a assinatura do dono da informação que autoriza o acesso aos sistemas. As assinaturas devem ser verificadas no Manual de Referência de Assinaturas Autorizadas mantido pela organização.

Tabela 1: Exemplos de Política, Norma, Directiva e Procedimento
Adaptado de Peltier [2002, p.26]

Outro enquadramento a dar à política, normas, directivas e procedimentos é apresentado por Pintos e Romanos (2007), que as relacionam com os níveis estratégico, táctico e operacional numa organização. Essa relação é apresentada na Figura 2.

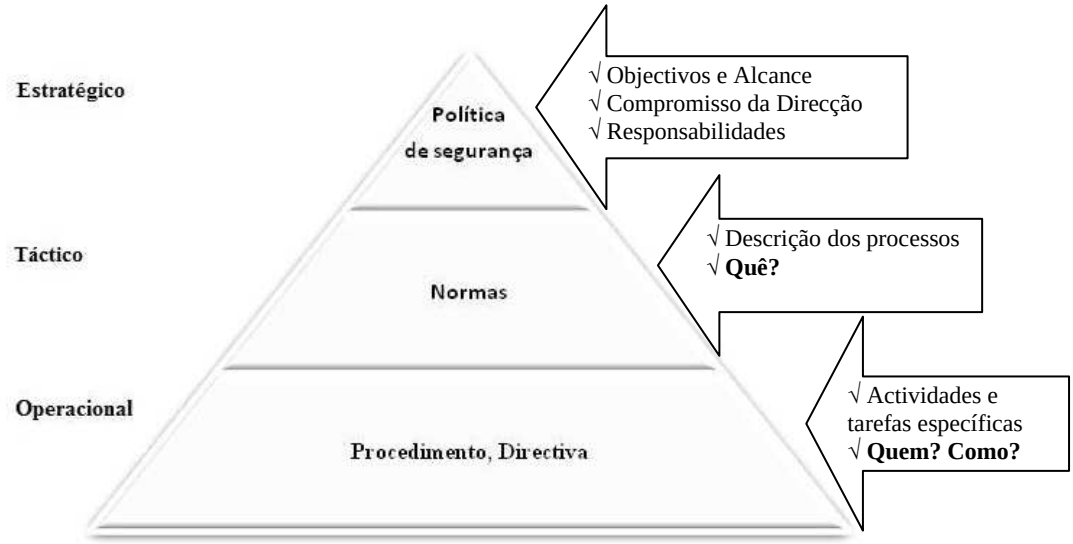


Figura 2: Posição Hierárquica das Políticas, Normas, Procedimento e Directivas
Adaptado de Pintos e Romanos [2007]

Hierarquicamente, as políticas são declarações de nível mais elevado que as normas, embora nos dois tipos de documentos esteja presente o compromisso da Direcção. As políticas fornecem declarações gerais e estabelecem-se para um tempo razoável. As normas fazem menção especial às tecnologias, métodos, procedimentos de implementação e outros detalhes, sendo o tempo da sua aplicabilidade inferior ao das políticas, tendo em conta a sua natureza mais técnica [Wood 1995].

As linhas de orientação são em relação as normas e às políticas, definidas da seguinte forma, segundo Guel [2007, p. 5]:

1. Declarações gerais, recomendações ou instruções administrativas desenhadas para atingir os objectivos da política, fornecendo um enquadramento através do qual se implementam procedimentos;
2. Uma linha de orientação pode alterar-se frequentemente dependendo do ambiente e deve ser revista mais frequentemente do que as normas e as políticas;
3. Uma linha de orientação não é obrigatória constituindo-se em mais uma sugestão para a melhor prática.

Outro autor – Walton [2002, p. 155] – especifica os pontos que uma norma deverá contemplar:

1. Estabelecer o programa de segurança;
2. Escolher a autoridade segundo a qual a norma é publicada;
3. Estabelecer os objectivos e metas de segurança da Tecnologia de Informação da organização;
4. Assumir responsabilidades de gestão do programa;
5. Definir responsabilidades e os papéis dos indivíduos e grupos que integram a equipa de segurança, incluindo os utilizadores;
6. Definir o programa de classificação de dados e o nível mínimo de segurança requerido para cada nível de classificação;
7. Definir os critérios para determinar a propriedade dos dados e do sistema;
8. Designar as responsabilidades dos proprietários dos dados e do sistema para alcançar o nível mínimo de segurança requerido para cada nível de classificação;
9. Definir a relação entre o programa de segurança e o pessoal do departamento de Tecnologias de Informação, incluindo a integração de funções de segurança para a gestão do ciclo de vida do sistema informático, gestão de configuração e alteração dos processos de controlo;
10. Incluir todos os recursos de Tecnologias de Informação;
11. Incluir uma visão global de todos os recursos de Tecnologias de Informação em relação aos quais a organização é responsável, tais como, estações de trabalho, LAN's, sistemas principais e computadores;
12. Realçar a todos os utilizadores a importância da segurança;
13. Clarificar o papel dos utilizadores individuais e definir as suas responsabilidades,
14. Estabelecer firmemente as responsabilidades dos utilizadores finais individuais;
15. Servir de reforço, descrevendo consequências específicas resultantes de falhas no comprimento de requisitos de segurança;
16. Descrever acções disciplinares concordantes com todos os níveis e tipos de infracções de segurança;

17. Incluir provisões para requisitar, avaliar e garantir excepções às normas de segurança.

Baskerville e Siponen [2002, p.337] afirmam ser "muito consensual que uma boa política de segurança da informação constitui a base da segurança da informação das organizações", no entanto, alegam ter encontrado pouca pesquisa no que diz respeito à criação de uma boa política de segurança. Em subsecções subsequentes abordar-se-ão aspectos que dizem respeito e que podem ajudar na criação de uma política de SSI, mas primeiramente focar-se-á a importância das mesmas.

2.3.2 Importância das Políticas

A informação é um dos principais activos das organizações actuais, estando os sistemas que suportam essa informação cada vez mais expostos a ameaças. A tríade CIA (*Confidentiality, Integrity and Availability*) – Confidencialidade, Integridade e Disponibilidade – representa as propriedades convencionais que orientam a análise, o planeamento e a implementação da segurança da informação. Outras propriedades estão a emergir, como é o caso da legitimidade e a autenticidade, isto porque a utilização de transacções comerciais em todo o mundo através de redes electrónicas se massifica.

Os princípios clássicos da CIA podem ser explicados da seguinte forma:

- Confidencialidade – acesso a informação somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- Integridade – a informação manipulada deve manter todas as características originais estabelecidas pelo proprietário da informação, garantindo que o conteúdo não é alterado de forma não autorizada.
- Disponibilidade – a informação está sempre disponível para o uso legítimo, sempre que dela se necessite.

Estes princípios são considerados tradicionais para os autores Dhillon e Backhouse [2000, p. 126], que consideram que são bons enquanto servirem, mas “são muito restritos e aplicam-se principalmente à informação vista como dados mantidos nos sistemas informáticos”. Estes autores acrescentam outros princípios sem os quais as futuras organizações enfrentarão sérios problemas. Estes novos princípios foram condensados no acrónimo RITE (*Responsibility, Integrity, Trust and Ethicality*) – Responsabilidade, Integridade, Confiança e Ética – e são entendidos por aqueles autores como instrumentais para a criação de uma cultura de segurança da informação para as organizações num futuro próximo.

Os princípios RITE podem ser explicados da seguinte forma:

- Responsabilidade – Assume importância com o abandono da estrutura organizacional vertical/hierárquica. Para os autores Dhillon e Backhouse [2000, p. 127], espera-se que os “membros desenvolvam as suas próprias práticas de trabalho com base numa compreensão clara das suas responsabilidades. Assim, ser responsável significa não apenas ter remédio para quando as coisas erradas

ocorrem, mas refere-se também em lidar com o desenvolvimento dos eventos futuros de uma esfera particular".

- Integridade – Lidar com a informação valiosa, não a divulgar, não ceder às pressões. Para os autores Dhillon e Backhouse [2000, p. 127], a informação "tornou-se uma propriedade das organizações. Tem propriedades que são peculiares – pode divulgar-se a informação a uma terceira parte sem removê-la de onde veio e sem necessariamente revelar que o fez". Dado o valor da informação para as organizações é necessário ter em conta a integridade dos funcionários que acedem à informação.

- Confiança – Autocontrolo e responsabilidade em abandono do controlo externo e supervisão. Para os autores Dhillon e Backhouse [2000, p. 128], nas empresas "onde se dá menos ênfase ao controle externo e à supervisão e mais ao auto-controlo e responsabilidade têm que existir sistemas de confiança mútua".

- Ética – As regras aplicam-se a situações concretas, a circunstâncias previstas e previsíveis. A ética deve estar sempre presente em situações informais, novas e dinâmicas, de forma a potenciar uma resposta adequada por parte dos colaboradores face a essas novas situações.

Para estes autores, a SSI deve nos próximos tempos assentar nos princípios CIA e RITE. Ou seja, é preciso ter em conta não só os aspectos técnicos, mas também e cada vez mais, os aspectos organizacionais e sociais, pois só assim será possível o bem-estar organizacional.

Para atingirem este nível de protecção, as empresas têm de se deixar de preocupar apenas com ataques de *crackers* ou com a implementação de *firewalls* e/ou antivírus, e deslocar a sua atenção para a criação de uma verdadeira política de SSI, onde estejam incluídos os meios identificados anteriormente, mas com um maior grau de abrangência e complexidade. Para Wood [1995], estabelecer apenas uma *firewall* não garante, por exemplo, que o acesso à Internet seja seguro, devendo-se, na opinião deste autor, estabelecer um conjunto de considerações, tais como, políticas, procedimentos, normas[3] e outras instruções de gestão.

Da revisão da literatura efectuada verifica-se unanimidade quanto à importância de uma política de SSI numa organização, sendo considerada por vários autores como a fundação da segurança da informação. Esta constatação pode ser validada com as afirmações que a seguir se apresentam:

> "A política de segurança é para o ambiente da segurança como a lei para o sistema legal. (…) Uma política é o início da gestão da segurança." [Higgins 1999, p. 217]

> "… um sistema de informação sem uma política de segurança é uma espécie de colecção deslocada de contra-medidas dirigidas a várias ameaças." [Schneier 2000, p. 55]

[3] Estas normas são internas à organização e não normas internacionais.

> "Uma política de segurança eficaz é tão necessária para um bom programa de segurança de informação como uma fundação sólida para uma casa." [King et al. 2001, p. 13]

> "A pedra angular de uma arquitectura de segurança de informação eficaz é uma declaração de política bem redigida." [Peltier 2002, p. 21]

> "A política de segurança da informação é um dos documentos mais importantes numa organização." [Höne e Eloff 2002a, p. 409]

> ". . . a política de segurança é o alicerce em que toda a segurança se baseia." [Shorten 2004, p. 917]

> "As políticas de segurança são a fundação e a linha da base da segurança da informação numa organização." [Kee 2001, p. 1]

> "As políticas de segurança são as directivas mais baratas de executar, mas as mais difíceis de implementar adequadamente." [Whitman e Mattord 2005]

As razões para esta elevação do grau de importância das políticas de SSI encontram-se na utilidade que estes documentos demonstram ao nível das iniciativas para a protecção dos SI desenvolvidas pelas organizações [de Sá-Soares 2005].

Para os autores Höne e Eloff [2002a], as políticas de segurança constituem um veículo privilegiado para os responsáveis explicarem a necessidade de segurança no sistema de informação da organização.

As políticas de segurança também revelam a sua utilidade mediante o estabelecimento das grandes linhas orientadoras para a SSI, fornecendo direcção às iniciativas de protecção dos recursos do sistema de informação e definindo o papel que a SSI desempenha no suporte da missão e objectivos da organização [JISC 2001].

As políticas de SSI são também úteis para os técnicos de segurança, na medida em que fornecem indicações sobre os activos que a organização quer proteger e sobre o grau de protecção com que cada um desses activos deve ser dotado [King et al. 2001].

As políticas de SSI auxiliam ainda na coordenação das acções de protecção dos recursos do sistema de informação, evitando a fragmentação dos esforços e servindo de guia para o processo de selecção, desenvolvimento e implementação de controlos apropriados de SSI [Barman 2001].

Outro aspecto a destacar é a política de SSI contribuir para que todos dentro da organização se comportem coerentemente de forma aceitável relativamente à segurança da informação [Lee 2001].

Pode também referir-se o seu papel na garantia de que a organização está a cumprir a legislação apropriada, nomeadamente através da evitação ou limitação de responsabilidades civis ou criminais [Dhillon e Backhouse 1997].

2.3.3 Classificação de Políticas

Da revisão da literatura efectuada, denota-se a existência de diversas considerações em relação aos tipos de políticas de SSI, variando muito de investigador para investigador. Baskerville e Siponen [2002, p. 338] consideram estas variadas considerações uma "selva de terminologia", pelo que propuseram uma divisão simples das políticas de segurança em três classes:

Políticas de alto nível – consistem em planos globais de alto nível que envolvem os objectivos gerais e os procedimentos aceitáveis de uma política. Um exemplo deste tipo de política é que os departamentos devem assegurar-se de que as políticas de segurança da informação são implementadas para proteger o conjunto da sua informação. Um plano de segurança da informação deveria ser formulado para lidar com riscos e potenciais ameaças ao seu conjunto de informação de forma comensurada com as prioridades, princípios e objectivos de negócio desse departamento.

Políticas de baixo nível – são métodos de acção da segurança da informação definidos e seleccionados entre as várias alternativas e à luz de dados e condições, que guiam e determinam as decisões da segurança da informação presente e futura, como por exemplo, a definição de directivas para a *password*.

Metapolíticas – são as denominadas pelos autores como "políticas para as políticas", ou seja, directrizes organizacionais para a criação e manutenção das políticas. Por exemplo, quem é o responsável por fazer políticas e quando é que a política deve ser implementada. A metapolítica na segurança da informação tem permanecido implícita, e os processos para as criar (às políticas de segurança) são *ad hoc*. As políticas de SSI devem desenvolver-se com a ajuda das normas e linhas de orientação gerais da gestão da SSI, e seguir o mais possível as directivas e normas de segurança existentes.

Por sua vez, Whitman et al. [2001] reconhecem a existência de três estruturas fundamentais para as políticas de SSI:

Políticas individuais – nesta estrutura, a organização cria uma política de segurança separada e independente para cada uma das tecnologias e sistemas utilizados.

Política completa – de acordo com esta estruturação, que segundo os autores é a mais comum, a organização define, controla e gere centralmente um único documento que engloba todas as tecnologias utilizadas e que fornece orientações gerais para todos os sistemas empregues pela organização.

Política completa modular – esta política é controlada e gerida centralmente, tal como no caso da política completa, e é composta por secções gerais com descrições das tecnologias empregues e por discussões sobre a utilização responsável e apropriada dos sistemas. Difere da estrutura anterior por incluir apêndices modulares que fornecem detalhes específicos acerca de cada tecnologia e que avançam observações, diferenças, restrições e funcionalidades particulares relacionadas com a utilização das tecnologias que o documento da política base não cobre adequadamente. Para os autores esta é a estrutura mais eficaz para as políticas de SSI.

Opinião diferente das anteriormente apontadas é a de Dhillon [1997], que distingue estratégia, política e procedimentos operacionais, destacando que em vez de políticas, as organizações deveriam formar uma visão e estratégia da segurança da informação ao nível da gestão de topo. Este autor critica a atenção excessiva que no mundo da SSI se dá às políticas, referindo também a total ausência de referências ao uso do termo "estratégia". Conforme observa aquele autor, é necessário considerar a segurança "como uma questão estratégica, especialmente nos dias de hoje em que começa a tornar-se difícil dissociar os processos negociais dos SI baseados em computadores" (p. 140).

Dhillon [1997] considera também que as organizações devem ter políticas de segurança que permitam esboçar procedimentos específicos, não ficando contudo "presas em disputas arbitrárias com origem em políticas em vez de fazerem progredir a sua organização" (p. 139). Na verdade, dever-se-ia dar especial importância ao desenvolvimento de uma visão global de segurança, que traria esta questão para o palco central da atenção organizacional e a ligaria aos objectivos organizacionais.

Segundo Siponen [2000b] diferentes tipos de políticas de segurança podem ser categorizados baseadas na sua atenção em elementos "técnicos" ou "organizacionais" ou baseados nos seus tópicos específicos como políticas de aplicação, políticas específicas do sistema ou políticas organizacionais.

Por outro lado, é necessário traçar uma "linha comum" entre as finalidades organizacionais e as actividades nucleares. Uma visão comum "ajudaria a desenvolver uma cultura de segurança na organização, estabelecendo assim uma estrutura normativa em relação às actividades relacionadas com a informação" [Dhillon 1997, p. 140].

O que propõe este autor é que primeiramente seja compreendido o propósito e o conteúdo das acções organizacionais e só depois se desenvolva uma cultura de segurança, devendo a formulação de uma política de segurança ser considerada uma actividade emergente.

A Figura 3 não se pretende constituir em um guia sequencial e racionalista para o planeamento da segurança, antes clarifica algumas das fases principais que constituem o processo de planeamento da SSI.

A figura ilustra os princípios-chave para o desenvolvimento de políticas de segurança. Contrariamente ao que é normalmente apontado, como se pode ver nas citações de alguns autores anteriormente apresentadas, em que as políticas de SSI são posicionadas no nível mais elevado dentro de uma organização, Dhillon [1997] reconhece igualmente a sua importância, mas com a formulação inicial de uma estratégia clara para a SSI e só depois a determinação das políticas e dos procedimentos de segurança necessários à concretização dessas estratégias.

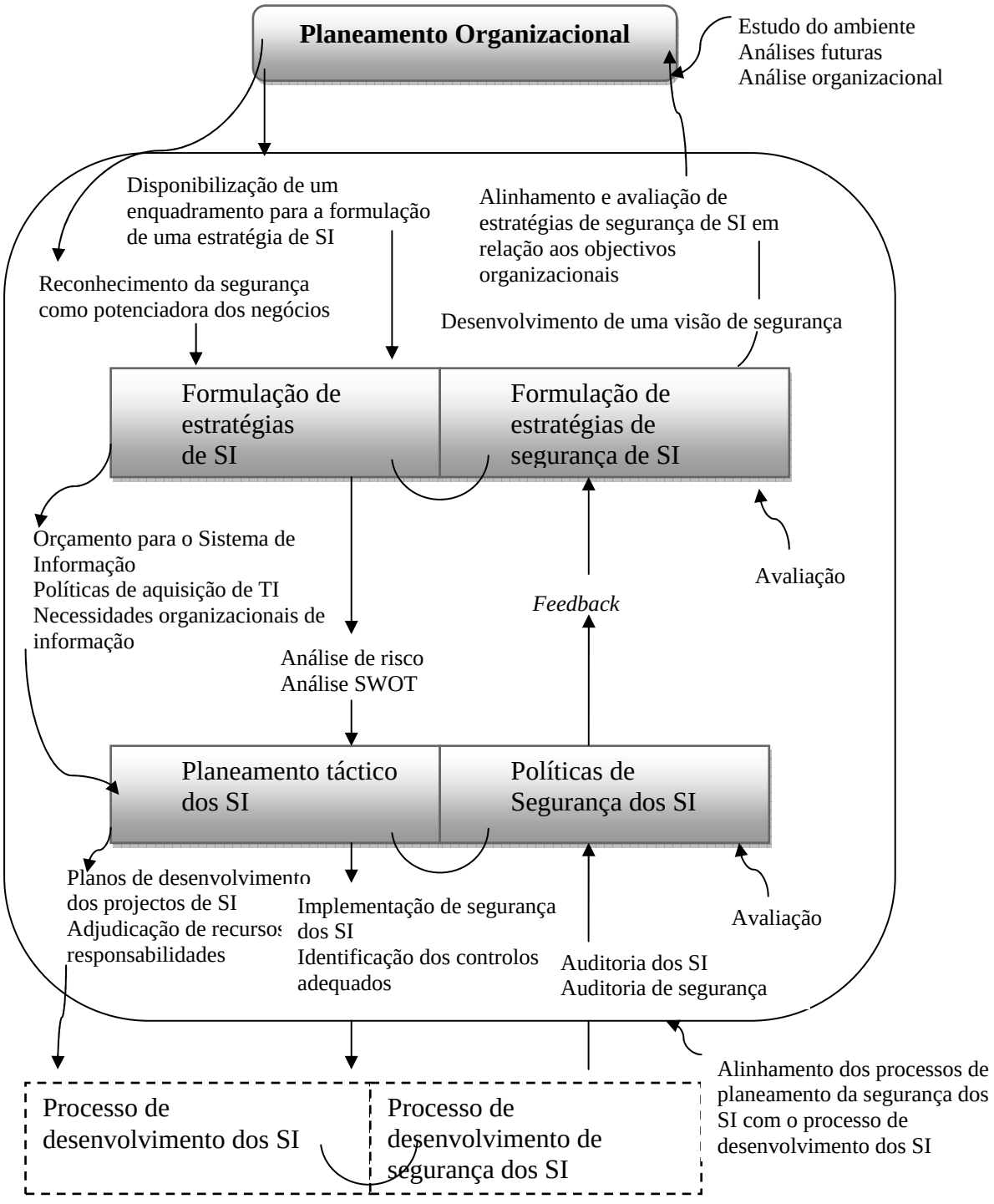


Figura 3: Enquadramento para o Processo de Planeamento da SSI
Adaptado de Dhillon [1997]

Como se pode observar na figura, a formulação da estratégia de SSI é posicionada ao mesmo nível que a formulação de estratégias de SI, localizando-se as políticas de SSI num nível inferior. Outra leitura possível é que ao posicionar a estratégia de SSI a este nível, este processo tem de ser conjunto com o planeamento estratégico do Sistema de Informação, ou seja não se pode dissociar a segurança e as políticas de segurança da visão e dos objectivos organizacionais, a estratégia de segurança não pode ser estruturada a posteriori, mas sim no planeamento global do Sistema de Informação.

Crê-se que esta perspectiva, "apesar de contrária ao que é advogado tradicionalmente na literatura, se reveste de grande importância, uma vez que contextua a orientação dos esforços de SSI no âmbito da orientação estratégica da organização" [de Sá-Soares 2005, p. 59].

Uma visão alternativa é avançada por Doherty e Fulford [2006], que consideram que os dois documentos mais importantes para assegurar o entendimento efectivo dos SI e tecnologias de informação dentro de uma organizações são o plano estratégico de SI e a política de SSI. Para estes autores, o plano estratégico de SI assegura que os novos sistemas e tecnologias são entendidos como uma forma de apoiar as metas estratégicas de uma organização, enquanto as políticas de SSI fornecem o enquadramento para assegurar que os sistemas são concebidos e operados de forma segura. Embora a literatura sobre a formulação de políticas ignore esta importante relação com o plano estratégico de SI e vice-versa, o seu alinhamento é crucial para um correcto e efectivo Planeamento de SI.

Desta posição destaca-se uma relação óbvia entre o planeamento estratégico de SI e a gestão da segurança da informação e, consequentemente, entre os dois documentos chave associados a estas duas actividades. Por exemplo, se um plano estratégico contemplar a instalação de uma *Intranet* na organização, então a política de SSI necessita de ser modificada para ter em conta esta significativa alteração na forma como a informação incorporada deve ser armazenada, disseminada e gerida.

Segundo aqueles autores, as políticas de SSI devem ser colocadas hierarquicamente ao nível do plano estratégico de SI e a estratégia ou gestão da SSI ao mesmo nível que o Planeamento de SI. Ambos os níveis têm de ser forçosamente associados, o que implica que uma política nunca pode ser construída sem a sua articulação com a visão e objectivos do Planeamento de SI, pois só assim se consegue um efectivo Planeamento de SI. Segundo Doherty e Fulford [2006], as organizações ao adoptarem esta abordagem podem sair de um estilo reactivo de gestão da segurança para um estilo mais pró-activo.

Por último, poder-se-á questionar quais os benefícios concretos que esta abordagem traz para a organização. Segundo Doherty e Fulford [2006] podem-se indicar os seguintes benefícios:

1. O alinhamento específico da formulação do plano estratégico de SI e a revisão da criação da política de segurança da informação vai ajudar a que a política tenha uma orientação de negócio mais forte.

2. A política de segurança da informação pode ser modificada prevenindo assim que uma nova iniciativa estratégica de SI não crie novos e inesperados riscos de segurança.
3. A abordagem integrada vai permitir que a política de segurança da informação seja modificada de forma pró-activa, pelo que se assistirá ao deslocamento da ênfase na rectificação para a prevenção.
4. Antes da sua implementação os planos estratégicos de SI podem ser revistos e modificados – numa perspectiva de segurança – para evitar a introdução de quaisquer iniciativas de TSI que estariam abertas a riscos significativos de segurança da informação.
5. Com esta revisão paralela é possível identificar importantes parâmetros de segurança que necessitam de ser incluídos nos novos sistemas que foram identificados no plano de Sistema de Informação avançando assim o seu desenvolvimento.
6. Integrando a revisão da política de segurança da informação no planeamento de SI, que é um exercício orientado para o negócio, deveria ser possível aumentar a consciência dos gestores dos consequentes impactos de falhas e considerar como eles podem ser mais bem integrados na política de SI.

Outra perspectiva de enquadramento da política de segurança, especificamente no que se refere à sua hierarquização no contexto global de segurança da organização, é a apresentada por Walton [2002], o qual situa as políticas de segurança no meio de uma pirâmide de segurança, cujo topo é ocupada pela liderança da segurança e a base pela protecção de tecnologia e continuidade. Esta estrutura é apresentada na Figura 4.

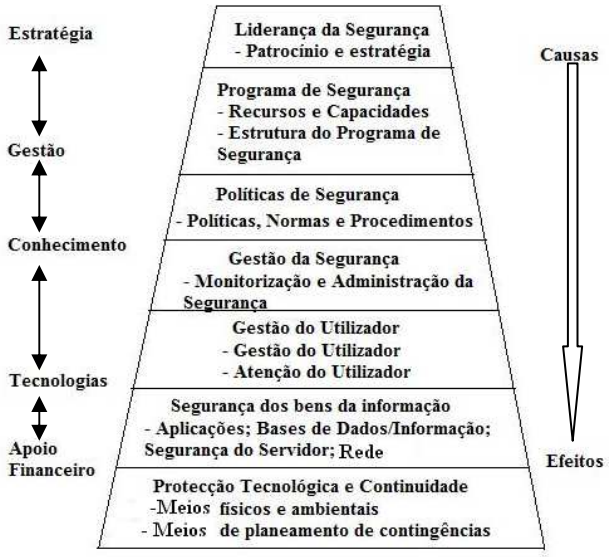


Figura 4: Modelo de Segurança
Adaptado de Walton [2002]

Neste modelo pode-se distinguir claramente as componentes da segurança mais ou menos próximas da estratégia ou da tecnologia, encontrando-se as políticas de segurança entre o programa de segurança e a gestão da segurança.

2.3.4 Características das Políticas

Quanto à forma ou às características que uma Política de Segurança deve contemplar, Höne e Eloff [2002b] defendem que o documento da política não deve incluir os aspectos técnicos relacionados com a implementação dos mecanismos de segurança, pois estes podem variar ao longo do tempo. Por outro lado, deve ser um documento de fácil leitura e compreensão, não contendo demasiado texto, ou seja, apresentar-se resumido, e de elevado nível de abstracção. Por último, no que respeita à sua durabilidade, as revisões do articulado da política devem ser efectuadas periodicamente, mas não constantemente.

Muitos dos factores anteriormente enumerados são também partilhados por Kee [2001], que entende que a primeira coisa a ter em conta quando se escreve uma política é escreve-la numa linguagem fácil de entender e não a tornar muito complicada. Para este autor as políticas deveriam ser escritas utilizando a regra SMART (***S**pecific, **M**easurable, **A**greeable, **R**ealistic and **T**ime-bound*), ou seja, devem ser escritas de uma forma Específica, Mensurável, Agradável, Realista e Delimitada no tempo.

2.3.5 Componentes das Políticas

No que diz respeito ao fundo da Política de Segurança, ou seja, às suas componentes, alguns autores advertem para a dependência da composição destes documentos da natureza da organização, da sua dimensão e dos seus objectivos, tornando-se desta forma difícil a generalização dos elementos que devem fazer parte de uma Política de Segurança.

Embora seja aceite que uma política de SSI varia consideravelmente de organização para organização, para Wood [1995] este documento deve incluir tipicamente os seguintes elementos: declarações gerais de metas, objectivos, crenças e responsabilidades, frequentemente acompanhadas dos procedimentos gerais para o alcance destes propósitos.

Whitman [2004] define que uma boa política de SSI deveria delinear responsabilidades individuais, definir que utilizadores estão ou não autorizados a utilizar o sistema, fornecer relatórios aos empregados de possíveis ameaças ao sistema, definir penalizações para possíveis violações da política e fornecer um mecanismo de actualização da política.

Atendendo ao disposto sobre políticas de SSI, em normas de gestão de SSI, importa atentar nas recomendações avançadas por uma das principais normas internacionais – a ISO/IEC 27002 – no que concerne às componentes de uma política de SSI.

De acordo com esse referencial, o documento da política de SSI deve estabelecer o comprometimento da gestão e deverá conter as seguintes declarações. [ISO/IEC 27002]:

1. Definição da segurança da informação, os seus objectivos gerais, abrangência e a importância da segurança como um mecanismo que possibilita a partilha ou troca de informação;
2. O estabelecimento das intenções da gestão, apoiando objectivos e princípios da segurança da informação em linha com as estratégias e objectivos do negócio;
3. Um enquadramento para estabelecer objectivos de controlo e controlos, incluindo a estrutura de avaliação de risco e gestão de risco;
4. Uma breve explicação das políticas de segurança, princípios, normas e concordância com os requisitos de particular importância para a organização;
5. Uma definição das responsabilidades gerais e específicas para a gestão da segurança da informação incluindo relatar incidentes de segurança da informação;
6. Referências a documentos que podem apoiar a política, por exemplo, políticas de segurança mais detalhadas e procedimentos para SI específicos ou com regras de segurança que os utilizadores devem observar.

Para Höne e Eloff [2002a] e para Forcht e Ayers [2001] uma Política de Segurança deve ter a estrutura enumerada na Tabela 2, que contém alguns pontos em comum nas abordagens destes diferentes autores, embora Forcht e Ayers [2001] se refiram a uma política específica para Tecnologias de Informação.

Höne e Eloff	**Forcht e Ayers**
1 - Necessidade e alcance da segurança da informação	1 – Alcance
2 - Objectivos da segurança da informação	2 - Definições
3 - Definição de segurança da informação	3 - Responsabilidade
4 - Compromisso da direcção em relação à segurança da informação	4 - Perfil de Risco
5 - Aprovação da Política SSI	5 - Requisitos
6 - Finalidades ou Objectivos da Política SSI	6 - Outras medidas de Segurança
7 - Princípios da segurança da informação	7 - Recuperação de Desastres
8 - Papéis e responsabilidades	8 - Segurança na Internet
9 - Violações da Política SSI e acções disciplinares	9 - Aplicação
10 - Monitorização e revisão	10 - Coordenador
11 - Declaração do utilizador e aceitação	
12 - Referências Transversais	
13 - Elementos Gerais	

Tabela 2: Elementos de uma Política de Segurança
Adaptado de Höne e Eloff [2002a] e Forcht e Ayers [2001]

Os elementos de uma política de segurança enumerados na tabela anterior por Höne e Eloff [2002a], e tendo em conta a sua importância numa política, são descritos seguidamente. O entendimento de vários autores sobre estes elementos é o seguinte:

1 – Necessidade e alcance da segurança da informação
É uma breve declaração introdutória que realça a dependência da organização da informação e assim da segurança da informação [OOIT 2007]. Esta declaração introdutória também fornece a justificação para a necessidade da política na organização.

2 – Objectivos da segurança da informação
Os objectivos da segurança da informação numa organização deveriam ser descritos de forma abreviada para informar o leitor acerca da finalidade específica da segurança da informação na organização. Estes objectivos deveriam estar claramente ligados à estratégia, metas e objectivos globais do negócio da organização e à natureza do negócio [OOIT 2007].

3 – Definição da segurança da informação
Uma política de segurança de informação é geralmente dirigida para uma audiência diversa, para quem a segurança da informação pode ser um conceito novo e estranho. É assim crucial que a política contenha uma definição breve e compreensível de segurança da informação para garantir uma compreensão uniforme do conceito através da organização.

4 – Compromisso da Direcção em relação à segurança da informação
A declaração do compromisso é a declaração mais importante numa política de segurança da informação. Sem esta declaração algumas actividades pretendidas pelo pessoal da segurança da informação não serão efectivas e não serão tomadas seriamente através de toda a organização [JISC 2001]. A declaração de compromisso da Direcção pode obrigar os empregados a tomar atenção à segurança da informação e demonstrar a intenção da Direcção no seu sucesso [Wood 1995].

5 – Aprovação da política da segurança da informação (assinatura)
A assinatura da aprovação pode também ser vista como a assinatura de apoio e tipicamente deve ser ao nível mais elevado possível dentro da organização [OOIT 2007]. Esta assinatura deve ser projectada numa posição proeminente como um sinal adicional do compromisso da Direcção para com a segurança da informação.

6 – Finalidade ou objectivo da política de segurança da informação
A finalidade ou o objectivo da política de segurança da informação não deveria ser confundida com as declarações introdutórias acerca da segurança de informação na organização. Estas declarações apenas descrevem as razões para o desenvolvimento de uma política de segurança da informação e estarão possivelmente ligadas a compromissos legais. Os principais objectivos da própria política são assim descritos nesta secção [JISC 2001].

7 – Princípios da Segurança da Informação
Os princípios da segurança da informação descrevem as regras gerais relacionadas com a segurança da informação numa organização. Estes princípios tentam explicar aos utilizadores qual é o comportamento correcto e incorrecto na organização tendo em vista vários tópicos e conceitos. Alguns destes princípios estarão intimamente ligados com a cultura da organização ou a requisitos regulamentares que governam o sector no qual funciona a organização. Outros conteúdos serão aplicáveis a todas as

organizações e encontram-se em qualquer política da segurança da informação, tais como, a protecção anti-vírus e avisos ao utilizador.

8 – Papéis e responsabilidades
Este é um dos componentes mais importantes da política de segurança da informação, pois esta parte diz ao leitor exactamente o que se espera dele em termos da segurança da informação na organização. Os papéis e responsabilidades devem cobrir todos os aspectos da segurança da informação, assim como, as responsabilidades individuais de todas as partes que utilizam os recursos da informação da organização [OOIT 2007].

9 – Violações da política de segurança da informação e acções disciplinares
A declaração acerca da violação da política de segurança da informação é muito importante pois assegura que se podem exercer acções disciplinares contra um utilizador se o mesmo não respeitar a política. É muito importante que esta declaração esteja directamente relacionada com a política disciplinar geral da organização.

10 – Monitorização e revisão
Esta declaração lida com a necessidade de monitorização e revisão frequente da aplicabilidade e efectividade continuadas das directrizes da segurança da informação implementadas na empresa. Sem esta declaração não há continuidade no aperfeiçoamento da implementação da segurança da informação na organização.

11 – Declaração do utilizador e aceitação
Este não é um elemento comum encontrado numa política de segurança da informação, sendo geralmente apresentado como apêndice ou documento separado. É contudo um elemento muito útil, pois geralmente é concebido como uma versão resumida da política de segurança da informação e completamente dirigida aos utilizadores da organização. Os utilizadores são levados a ler a secção inteira para terem uma melhor compreensão do que se espera deles [Tudor 2001].

12 – Referências transversais
A política de segurança da informação nunca deveria ser escrita isoladamente e necessitará do apoio de outras políticas, normas, procedimentos e processos relevantes. Estes documentos aplicáveis devem ser referenciados na política para assegurar que o utilizador obtenha uma imagem completa de todas as normas de segurança e medidas usadas na organização. Um outro aspecto importante é o facto de frequentemente as políticas terem de reflectir certas directrizes e medidas determinadas por legislação ou regulamentação do país.

13 – Elementos gerais
Os elementos que se recomenda que sejam incluídos numa política de segurança da informação para assegurar o seu status oficial na organização. Estes elementos são de fácil compreensão e encontrar-se-ão listados no final do documento, sendo os seguintes:

- Os autores da política
- Data de aprovação da política
- Data da revisão da política

Outro autor, Patrick [2001], define que uma política de SSI deve incluir os seguintes elementos na sua constituição:

1 – Sumário Executivo
2 – Alcance e aplicabilidade
3 – Política Geral
4 – Papéis e Responsabilidades
5 – Compromisso
    5.1– Acreditação
    5.2 – Gestão de Risco
        5.2.1 Controle de acesso
        5.2.2 *Backups*
        5.2.3 Resposta a incidentes
        5.2.4 Acesso não autorizado
        5.2.5 Monitorização
        5.2.6 Criptografia
        5.2.7 Existência de *Web*
        5.2.8 Disposição dos recursos
        5.2.9 *Passwords*
        5.2.10 Uso de recursos pessoais dentro da empresa
        5.2.11 Inspecções e revisões
        5.2.12 Software de entretenimento
        5.2.13 Meios de remoção
        5.2.14 *Freeware* ou *Shareware*
        5.2.15 Segurança física/pessoal
        5.2.16 Responsabilidades do vendedor
        5.2.17 Divulgação pública
        5.2.18 Sala de servidores/áreas
        5.2.19 Alteração da configuração do sistema
        5.2.20 Auditoria do compromisso de SSI
        5.2.21 Consciência da segurança e formação
        5.2.22 Inventário dos recursos do SI
        5.2.23 Documentação

Esta listagem surge porque é indissociável a gestão de risco dos elementos que constituem uma política SSI, os itens incluídos na gestão de risco cobrem um leque de elementos essenciais a considerar na elaboração de uma política.

As duas listas anteriormente apresentadas diferem principalmente no seu âmbito do enfoque, enquanto a primeira é constituída por componentes de política geral de SSI, a segunda dirige-se mais para a segurança de sistemas informáticos.

No Apêndice C resumem-se as principais recomendações sobre políticas de SSI constantes de diversas normas de gestão da SSI. Ressalva-se que a substância da maioria dessas recomendações é discutida ao longo deste Capítulo.

2.3.6 Formulação de Políticas

A criação de uma política de SSI segue um ciclo de vida completo desde a sua formulação até à sua revisão, passando pela sua implementação. O início deste ciclo, que se consubstancia na formulação da política, é apresentado nesta subsecção. As restantes fases do ciclo de vida são apresentadas nas subsecções seguintes.

Embora a política de SSI seja considerada vital dentro de uma estratégia organizacional, como forma de tornar os SI seguros, autores como Höne e Eloff [2002a] consideram nem sempre ser fácil redigir este documento. Na verdade, muitas vezes os autores recorrem a fontes comerciais ou minutas disponíveis, fazendo-se muitas vezes cópias desses documentos, não reflectindo assim a política a verdadeira cultura da organização, ou seja, não resultando, assim, num documento eficaz orientado para a SSI.

Escrever uma política de SSI é uma componente essencial de todos os esforços bem sucedidos de segurança da informação. As políticas estabelecem o estádio para uma grande variedade de esforços de segurança da informação [Wood 1995]. Contudo, a sua elaboração não é uma tarefa linear e está dependente de muitos factores.

A formulação de uma política faz-se num estádio de planeamento, na maioria dos casos como parte de um plano de segurança mais alargado que visa fornecer protecção adequada aos SI através de um conjunto de medidas e práticas de segurança [Peltier 1999].

Antes de se abordar o que envolve a formulação de uma política, convém clarificar o que se entende pelo termo formulação, que segundo o Grande Dicionário de Língua Portuguesa, é o "acto ou efeito de formular" [Tomo II, p. 129], definindo o vocábulo formular como "reduzir a fórmula; redigir na forma habitual; exprimir, expor, desenvolver com precisão; formar, organizar, compor" [Tomo II, p. 129].

Segundo Hartley e Locke [2001], o desenvolvimento de uma política de segurança numa organização envolve quatro actividades:

1. Avaliação e entendimento das necessidades de segurança;
2. Revisão das políticas e procedimentos em vigor, caso existam;
3. Definição dos requisitos de protecção;
4. Formalização da política de segurança.

Os dois primeiros pontos destinam-se essencialmente à recolha de informação e exigem uma combinação de conhecimentos técnicos de segurança e de análise e gestão do risco. O ponto três é puramente analítico e, portanto, exige conhecimentos de análise e técnicos, bem como um entendimento razoável dos princípios de gestão do risco. A quarta actividade é de índole mais administrativa, pois consiste na elaboração do documento final que formaliza a política de segurança da organização.

De modo a formular uma boa política de segurança Dhillon [2007, p. 106] recomenda que as organizações tenham presente os seguintes aspectos:

1. A importância de incorporar o sentido estratégico da organização tanto ao nível macro como ao nível micro do negócio.
2. A utilidade de clarificar a intenção estratégica com vista a dispor de uma base para o desenvolvimento do modelo de segurança. Tal modelo identifica a relação entre as áreas do negócio e as políticas de segurança para cada uma dessas áreas.
3. As políticas de segurança determinam os processos e técnicas necessários para fornecer segurança, mas não estabelecem directivas concretas no que respeita à tecnologia a empregar.
4. A implementação de políticas de segurança exige o desenvolvimento de procedimentos para implementar as técnicas definidas nas políticas de segurança. O estádio de implementação define a natureza e abrangência da tecnologia a ser utilizada.
5. Após a implementação existe uma necessidade constante de monitorizar os processos e técnicas de segurança. Isto permite fazer verificações para certificar a eficácia a três níveis: política, procedimento e implementação. Entre estas verificações assumem relevo particular a avaliação da aplicação das políticas de segurança, a avaliação da implementação de procedimentos e a detecção de falhas de segurança. A monitorização também deve incluir as acções de avaliação e reavaliação com vista a garantir que os procedimentos em utilização vão ao encontro dos requisitos originalmente especificados.
6. Uma política de resposta a incidentes é também uma parte integrante de uma boa política de segurança, servindo para antecipar a concretização de uma falha de segurança e, concomitantemente, determinar o seu impacto sobre as políticas, os procedimentos, o processo de implementação e o processo de monitorização.
7. Finalmente, um programa de segurança estabelece os procedimentos e práticas para formar e alertar os colaboradores para a importância da segurança. Os utilizadores também necessitam de formação que os capacite para identificar novas ameaças. No actual ambiente económico, em que a mudança é constante, surgem permanentemente novas vulnerabilidades e é importante dispor das competências para as identificar e gerir.

Baskerville e Siponen [2002] defendem a necessidade de se rever o processo de formulação das políticas de segurança, sugerindo que esse processo possa assumir um cariz federado e emergente, de forma a dar resposta à actual emergência de novas formas organizacionais e de novos negócios.

Apesar de a formulação e utilização de políticas de SSI ser prática comum e de as organizações gastarem recursos significativos em actividades de gestão da segurança é frequente a aplicação das políticas falharem na concretização das suas metas definidas [Karyda et al. 2005]. Embora existam diversos contributos que providenciam orientações para a formulação de uma política de SSI (normas para a gestão da segurança, melhores práticas, etc.), o processo de formulação consiste numa actividade muito exigente e de complexidade apreciável.

Na Figura 5 esquematiza-se o processo de formulação de políticas de segurança com base no estudo de Karyda et al. [2005]. A formulação de uma política de SSI, conforme representado nessa figura, inclui elementos de *input*, que alimentam o processamento de actividades, que por sua vez dão origem a um conjunto de *outputs*.

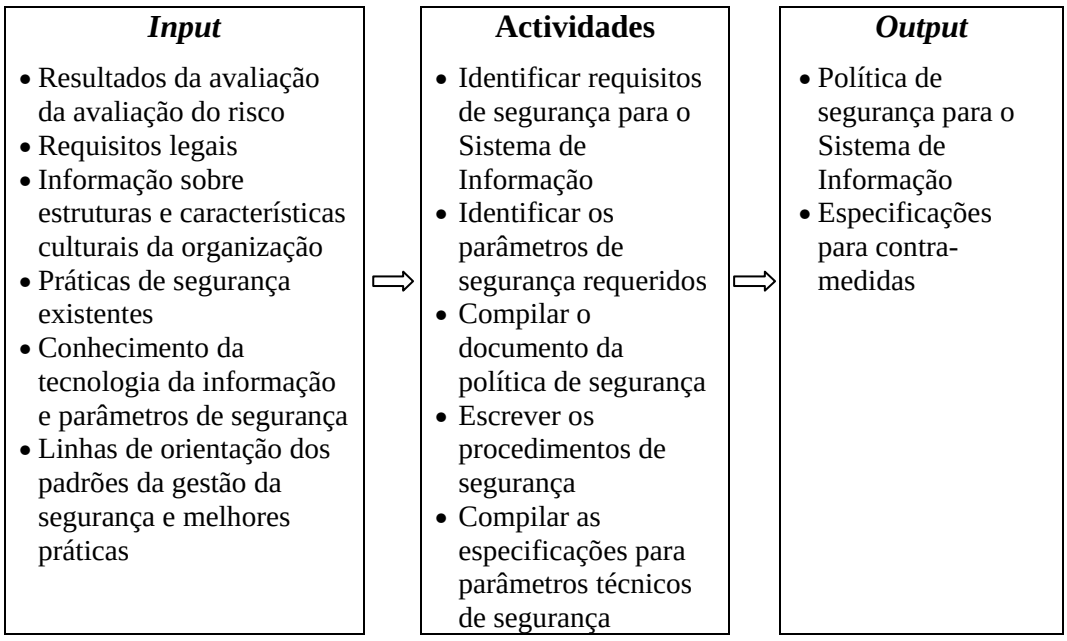


Figura 5: O Processo de Formulação de Políticas de Segurança
Adaptado de Karyda et al. [2005]

O processo de formulação de uma política de SSI, que tem como resultado último o documento das políticas de segurança, passa por um conjunto complexo de estudos, análises e compilações de um número significativo de elementos.

Para a sua compilação é necessário identificar os requisitos de segurança e os parâmetros desses requisitos, para isso, é preciso ter como dados de entrada a avaliação do risco, identificação dos requisitos legais, conhecimento da cultura organizacional, identificação da existência ou não de políticas de segurança, conhecimento das tecnologias da informação e parâmetros de segurança e estudo das linhas de orientação das normas da gestão da segurança existentes, que podem servir de base para a formulação da política de SSI (cf. Apêndices B e C).

Conforme se referiu anteriormente aquando da explanação das características das políticas de SSI, cabe ao processo de formulação desenvolver o esforço por conceber políticas que sejam claras nos seus objectivos, directrizes e procedimentos. Além disso, dever-se-á considerar a inclusão de uma cláusula bem definida de "excepção à regra" que permita dotar a política de um certo grau de flexibilidade necessário quando as circunstâncias o exigirem [Wills 2002].

Para além do anteriormente exposto, é importante saber que não há um único método para desenvolver uma política de SSI. Factores tão diversos como a audiência, o tipo de negócio, o tamanho da empresa e a existência ou não de uma política de SSI influenciam o processo de formulação das políticas de SSI [Diver 2007].

2.3.7 Implementação de Políticas

Implementar uma política de SSI apropriada é uma acção que extravasa a escrita de um manual de segurança [BS7799 1996]. Na verdade, torna-se necessário desenvolver uma cultura de segurança, iniciativa que normalmente se revela muito exigente em termos temporais [Gaunt 1998]. Só através de uma cultura organizacional receptiva às preocupações com a segurança dos SI será possível que a implementação das políticas seja um fiel reflexo dos procedimentos e normas que derivam dessas políticas, permitindo assim, a eficácia desejada de segurança na organização.

Entendendo-se pelo vocábulo implementação o definido na Lexiciteca, que expressa o "conseguir uma ou mais condições para a execução de alguma coisa" [Lexiciteca 1985, Vol I, p. 1252], apresentam-se no parágrafo seguinte os princípios fundamentais para uma correcta implementação da política de SSI.

Segundo Gaunt [1998], existem seis princípios fundamentais a levar em linha de conta no processo de implementação de uma política de SSI:

1. A organização assegurará que a sua informação seja mantida segura e utilizada de forma apropriada;
2. A organização fornecerá aos recursos humanos orientação clara relativamente à segurança da informação;
3. Todos os recursos humanos que trabalham para e em nome da organização colaborarão com a política de segurança da informação na organização;
4. A organização assegurará que os seus recursos humanos conhecem todas as orientações relevantes, acerca da segurança da informação da organização;
5. A organização informará os clientes como os seus registos serão mantidos seguros e a quem eles serão facultados;
6. A organização obedecerá a toda a legislação nacional e à melhor orientação relativamente à segurança da informação.

A implementação de uma política de SSI é o processo ao longo do qual as políticas de segurança são "traduzidas" em linhas de orientação, procedimentos e listas do que há a fazer, e são postas em prática pelos utilizadores do sistema de informação [Karyda et al. 2005]. Assim, a implementação de uma política pode ser considerada como um conjunto de actividades que visam prescrever o que se encontra no documento da política.

A implementação de uma política de SSI, conforme representado na Figura 6, inclui elementos de *input*, que alimentam certos processamentos de actividades que vão dar origem a um conjunto de *outputs*.

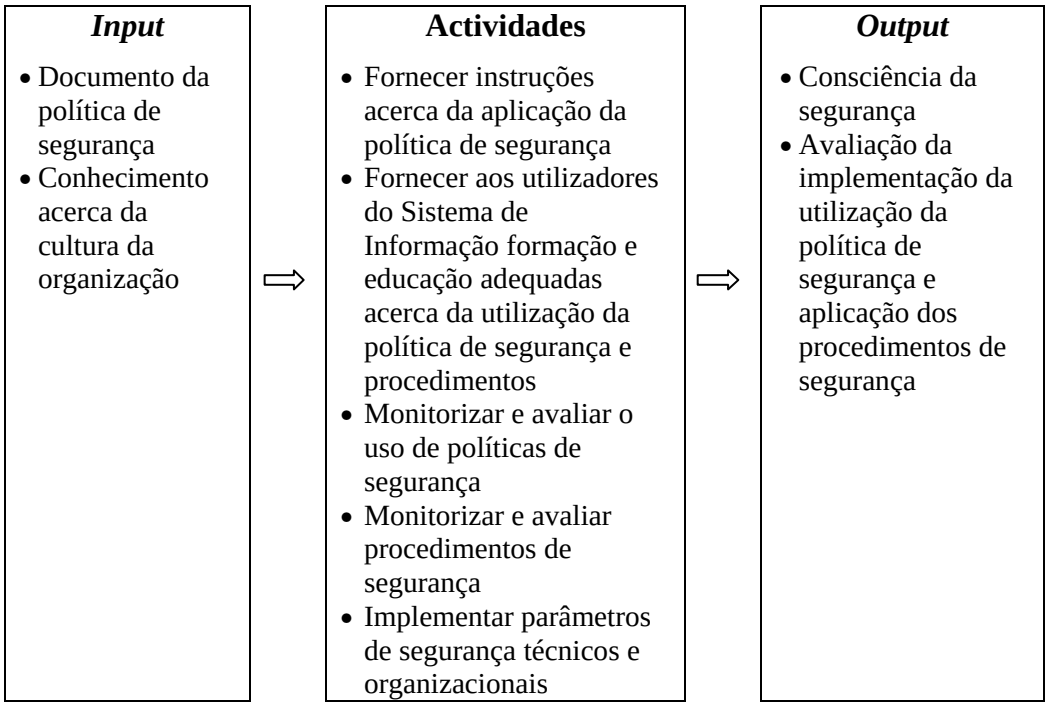


Figura 6: O Processo de Implementação de Políticas de Segurança
Adaptado de Karyda et al. [2005]

Este processo tem como resultado último a implementação e consequente consciencialização dos utilizadores e dirigentes da obrigatoriedade de utilizar essa política com o máximo de rigor e seriedade.

O processo de implementação de uma política de SSI tem como *inputs* o documento da política, mas também o conhecimento e informação relevante acerca dos aspectos sociais e culturais da organização. As actividades a desenvolver têm como base estes *inputs* e podem realçar-se as seguintes: formação e educação dos utilizadores da política no que concerne à sua aplicação adequada, aos seus procedimentos e á sua utilização. Após estes passos, os mesmos são monitorizados e avaliados.

Autores como Höne e Eloff [2002b] advertem para o elevado nível de cepticismo mantido quer pela generalidade dos investigadores da área da SSI quer pelos profissionais da SSI no que se refere à utilização eficaz das políticas de SSI. Laborando nesta observação, Karyda et al. [2005] avançam como possíveis factores explicativos para a falta de eficácia na utilização das políticas de SSI o entrave que as mesmas podem colocar à progressão do negócio no caso de serem demasiadamente rígidas e restritivas, a resistência manifestada pelos funcionários às mudanças impostas for esses documentos e a implementação de políticas universais, sem que as especificidades das organizações em causa sejam devidamente consideradas.

2.3.7.1 Ciclo de Implementação

A implementação de uma política de SSI, que se enquadra no ciclo total da implementação da política de SSI, tem incorporado um sub-ciclo, onde é feita a

avaliação, planeamento e correcção da política. Na fase da implementação é necessário fazer uma pré-avaliação do uso da política, sendo também importante saber a opinião dos utilizadores no planeamento e implementação da segurança, e poder desta forma redefinir o planeamento e posteriormente fazer as devidas correcções na política de segurança. Esta correcção é importantíssima nesta fase, porque muitas vezes só na fase da implementação se detectam problemas anteriormente impensáveis e imprevistos [Marta e Santiago 2004]. Este sub-ciclo existente na implementação encontra-se representado na Figura 7.

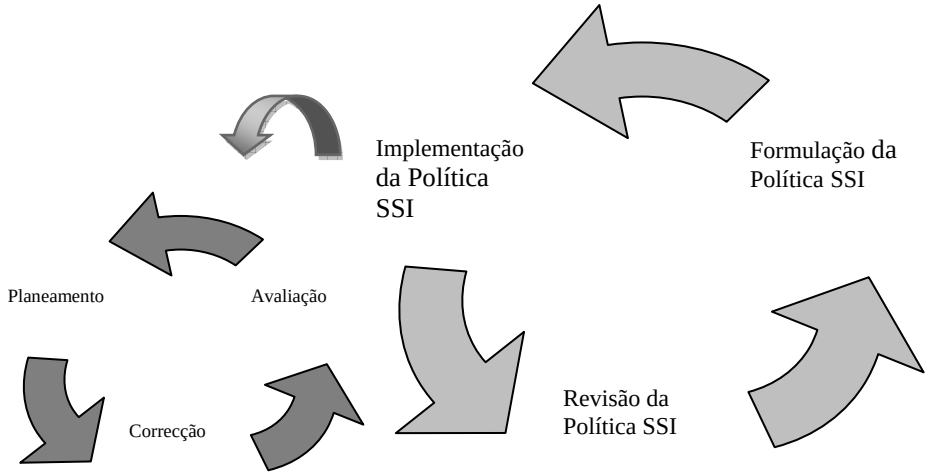


Figura 7: Sub-ciclo do Processo de Implementação
Adaptado de Marta e Santiago [2004]

Outro factor importante que justifica a existência do sub-ciclo é o facto de existirem variáveis como a experiência, os problemas na implementação, as limitações e os avanços tecnológicos, que se não forem tidos em conta podem levar a que a Política de SSI se torne inoperante e utópica.

A avaliação no processo de implementação poderá servir também para averiguar a necessidade de formação dos recursos humanos, contribuindo-se, assim, para a formação de uma verdadeira cultura de segurança, que se consegue se a equipa de implementação da política de SSI estiver preparada para repetidamente reforçar as melhores práticas através de um programa de formação contínua.

2.3.7.2 Método de implementação

O método adequado de planear a segurança numa organização deve partir sempre da formulação de uma política de segurança, que defina o "que" se quer fazer em termos de segurança na organização para seguidamente, com base nessa definição, e mediante um adequado plano de implementação que determine "como" alcançar os objectivos fixados.

Após a formulação da política de segurança, procede-se para a sua implementação, que depende directamente das directrizes nela contempladas. Ou seja, a implementação deve ser um fiel reflexo dos procedimentos e normas estabelecidos na política. Há duas questões fundamentais a ter em conta na implementação adequada da política. Primeiramente, é necessário que a política seja aprovada superiormente para ter a "autoridade" necessária perante os utilizadores da política, para além disso, é necessária a sua correcta divulgação junto dos recursos humanos da organização e utilizadores em geral do sistema de informação que a política contempla. Na Figura 8 ilustra-se o método discutido para a implementação das políticas de SSI.

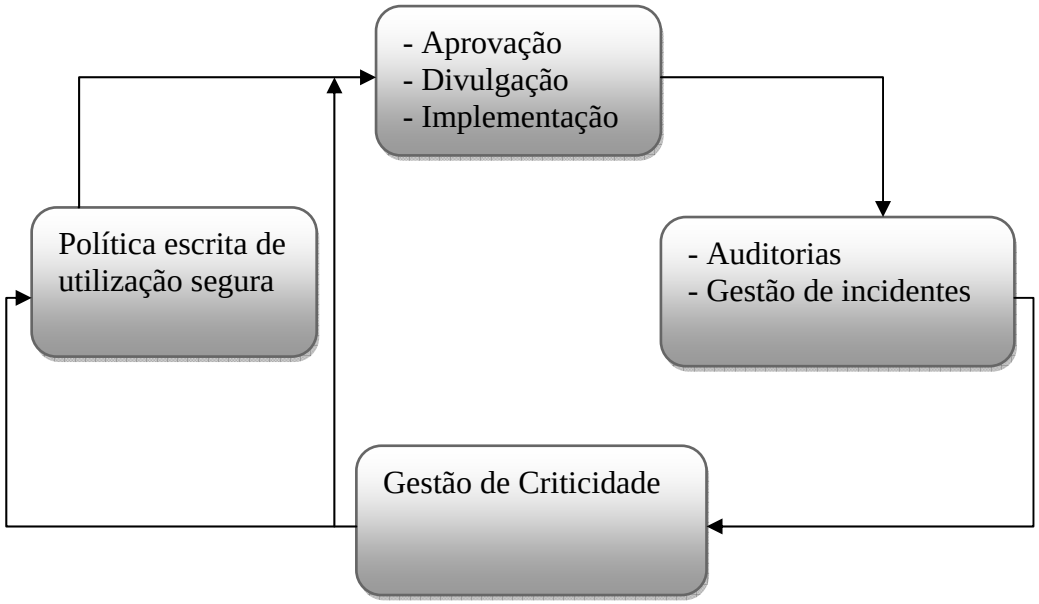


Figura 8: Método de Implementação da Política de Segurança
Adaptado de Marta e Santiago [2004]

O método de implementação contempla outros factores como a auditoria, ou seja, a verificação da conformidade com o definido na política de SSI. Contempla também a gestão de incidentes, que vai indicar se a política consegue dar resposta aos incidentes ou se pelo contrário não contempla algum aspecto e é necessário voltar a implementar a política ou rever a sua formulação, se for caso disso. Esse caminho é definido com base nas auditorias efectuadas e na gestão de incidentes tendo em conta a gestão da criticidade dos problemas detectados.

Conforme o grau de importância, ou criticidade, dos incidentes ou inconformidades detectados, fornecer-se-ão elementos relevantes para uma eventual reformulação das políticas ou para a sua aprovação, divulgação e implementação.

2.3.8 Revisão de Políticas

O processo de revisão das políticas normalmente é executado por técnicos e colaboradores da organização provenientes de domínios que necessitam de inter-operar [Casola et al. 2005]. Contudo, a revisão da política deve enfrentar incertezas que resultam de diferentes perspectivas, julgamentos verbais e falta de informação.

Técnicas difusas e raciocínios de forma incerta podem fornecer uma forma cheia de significado para lidar com estas questões. Por esta razão existem autores que propõem técnicas difusas para a avaliação das políticas [Casola et al. 2005].

Segundo o Grande Dicionário de Língua Portuguesa por revisão entende-se a "acção ou efeito de rever, de examinar de novo…para expurgar de erros" [GDLP 1991, Tomo V, p. 519].

A revisão feita a uma política de SSI tem de ser vista também na perspectiva das políticas já implementadas e já anteriormente avaliadas. Mesmo que uma organização já tenha uma política é aconselhável que seja revista e avaliada periodicamente, assegurando-se, assim, que a mesma permaneça relevante, ou seja, que cumpra os objectivos para a qual foi criada.

Na Figura 9 ilustra-se o processo de ciclo de vida de uma política de SSI, no qual se inclui o processo de revisão.

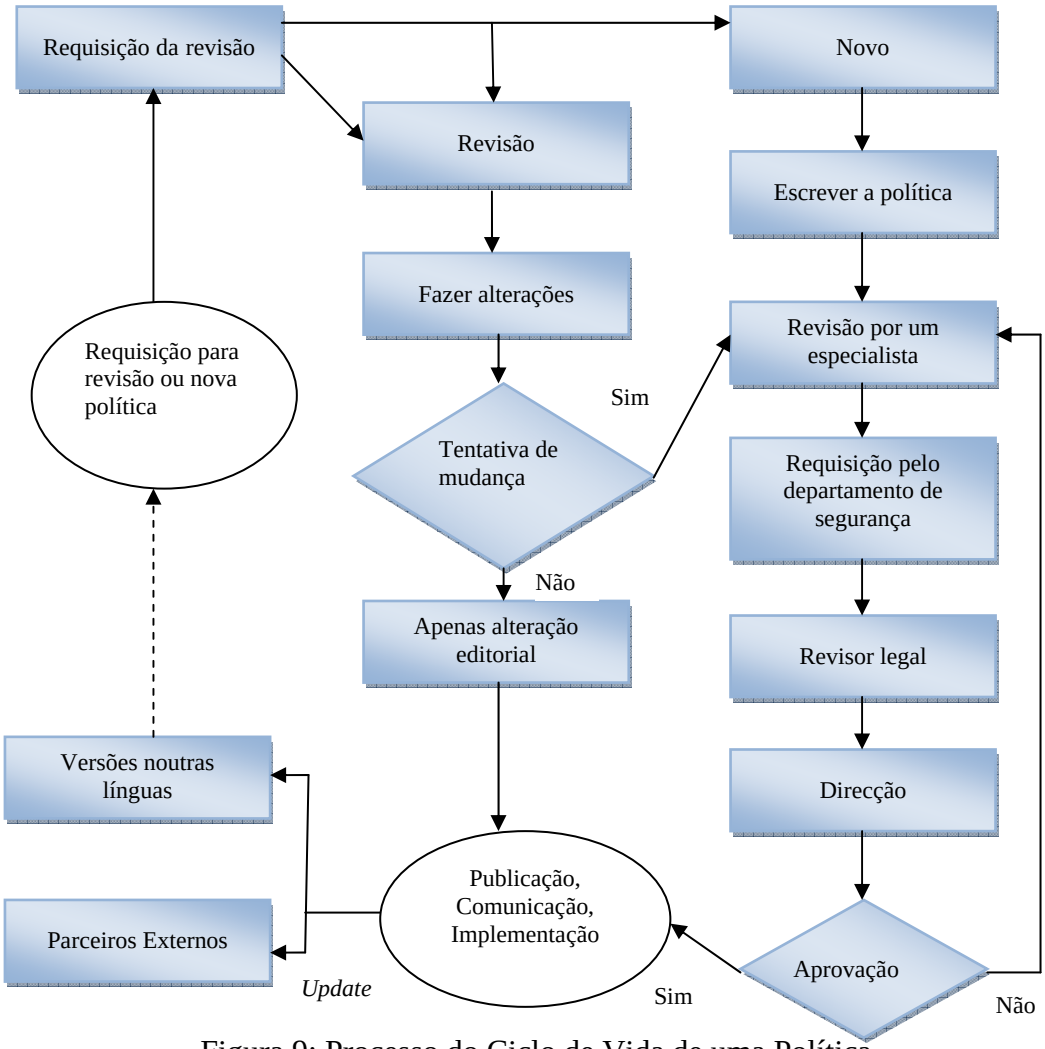


Figura 9: Processo do Ciclo de Vida de uma Política
Adaptado de Guel [2007]

No canto superior esquerdo da Figura inicia-se com a revisão da política através do item requisição do processo de revisão. Isto vai desencadear a actualização de uma

política já existente ou a necessidade de desenvolver uma nova política. Se a intenção for alterar uma política, a mesma deve ser dirigida através da revisão de um especialista e do departamento de segurança tal como são revistas as novas políticas. O processo de revisão da política envolve frequentemente várias partes de uma organização tais como o departamento jurídico. Uma vez revista e aprovada uma política pelos diferentes departamentos, deveria ser aprovada pela Direcção ou pelo dono da política. Depois de aprovada, é necessário publicá-la internamente e comunicá-la a todos os utilizadores. Em alguns casos, as políticas podem ter que ser traduzidas em diferentes línguas para empresas que operam em mercados internacionais.

Recuperando as orientações da norma ISO/IEC 27002 sobre políticas de SSI, constata-se a relevância dada ao processo de revisão das políticas de SSI, como se pode apreciar seguidamente. [ISO/IEC 27002]:

> A política de SSI deve ser revista em intervalos previstos ou quando ocorrem alterações significativas para garantir que continua a servir, adequada e efectiva.
>
> A revisão da política deverá incluir um conjunto de *inputs* (*feedback* das partes interessadas, alterações que podem afectar a gestão da segurança, tendências relacionadas com ameaças e vulnerabilidades, relatórios de incidentes etc.) e *outputs* (desenvolvimento de objectivos de controlo e controlos, desenvolvimento de recursos e ou responsabilidades, etc.), que permitiram que o propósito para o qual foi criado seja efectivo.

2.3.9 Adopção das Políticas

A adopção e concomitante observância das políticas, dada a natureza das diferentes organizações onde diferentes e variados tipos de utilizadores usam o Sistema de Informação, é fundamental, para dessa forma poderem ser observadas incoerências e falhas na adopção da política que conduzam à sua correcção.

Segundo o Grande Dicionário de Língua Portuguesa, o vocábulo adopção é definido como a "Acção ou o acto de adoptar, aceitação" [GDLP 1991, Tomo II, p. 125]. Por sua vez, a palavra – Aceitação, é definida na Infopédia [2008], como "Acto ou efeito de aceitar, bom acesso, acolhimento e consentimento".

A adopção de uma política de SSI, conforme representado na figura seguinte, inclui elementos de *input*, que alimentam certos processamentos de actividades que vão dar origem a um conjunto de *outputs*, conforme se ilustra na Figura 10.

O processo de adopção tem como *inputs* a avaliação efectuada à política aquando da sua implementação, os procedimentos e práticas de trabalho que implementam a política de segurança e os processos de formação e educação dos utilizadores. Com base nestes dados, o processo vertente inclui a resolução de possíveis conflitos e dificuldades detectadas na aplicação de certos parâmetros contidos na política, bem como manter os utilizadores e gestores informados acerca da agenda da SSI.

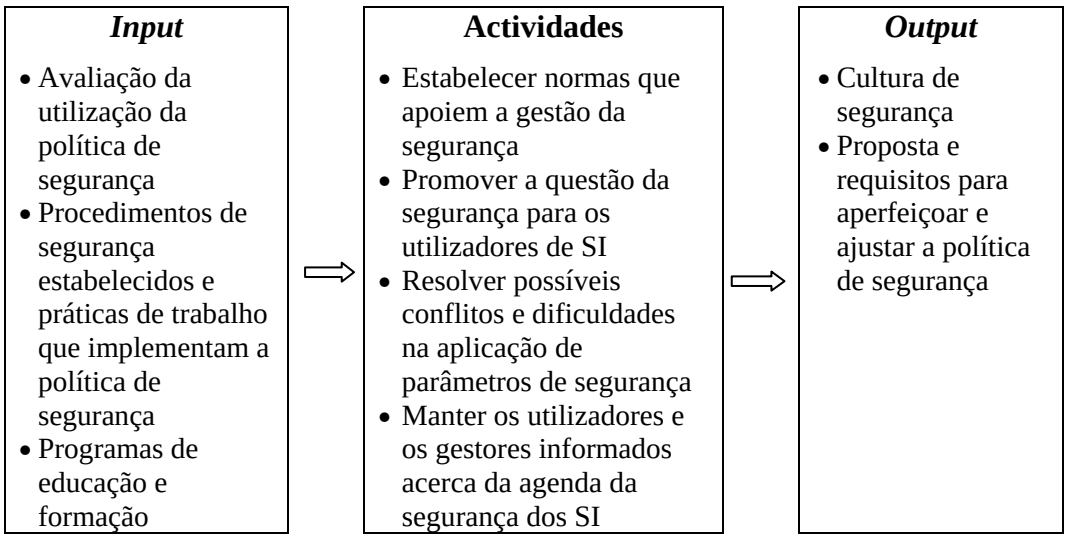


Figura 10: O Processo de Adopção de Políticas de Segurança
Adaptado de Karyda et al. [2005]

2.3.10 Factores Críticos de Sucesso na Adopção de Políticas de SSI

Esta subsecção tem por propósito identificar os pontos-chave que definem o sucesso na adopção de uma política de SSI. Estes pontos-chave, ou seja, os factores considerados fundamentais para o sucesso de uma política de SSI são aqui apresentados de forma resumida identificando-se os aspectos que a literatura tem apontado como cruciais.

O sucesso de uma política depende muito da adopção e cumprimento da política por parte dos utilizadores. Embora as linhas de orientação da SSI sejam de natureza prescritiva, constituindo um imperativo para os seus utilizadores, observa-se que estes falham frequentemente no que respeita ao seu cumprimento [Siponen 2000a].

Essa falha apontada aos recursos humanos pode ser superada através da delineação de responsabilidades individuais, por exemplo, através da clarificação de quem tem acesso a determinada parte do sistema.

Outro aspecto que é considerado um factor crítico de sucesso para uma boa implementação é a definição de penalizações para os utilizadores que não cumprem o estipulado pela política.

O apoio dos gestores das organizações na elaboração e adopção das políticas é também um factor crítico preponderante para o sucesso de uma política de SSI. Só com o envolvimento de todos os colaboradores e principalmente com o envolvimento dos gestores e chefias, se atinge uma boa elaboração e adopção da política.

A revisão periódica das políticas de SSI é também crucial. De pouco servirá uma política se a mesma não estiver actualizada. As organizações cada vez são mais dinâmicas e como consequência as alterações de funcionamento e de estrutura acontecem a um ritmo elevado, pelo que é necessário adaptar a política a essas novas realidades.

A comunicação e disseminação da política por todos aqueles que a devem conhecer e observar têm sido também apontadas como fundamental para o sucesso das políticas. Facilmente se aceitará que todos os actores organizacionais têm de ter conhecimento da política de segurança. Embora a forma de dar conhecimento possa variar (circular interna, disponibilização da política na Intranet da organização ou outros mecanismos), é necessário garantir que todos tiveram conhecimento do conteúdo da política.

A integração das políticas com os objectivos, processos e cultura da organização é fundamental para o sucesso da implementação da política. Uma Política de SSI tem que ser um veículo construtor e de protecção e nunca um mecanismo que impeça o bom desenvolvimento do trabalho da organização. Para tal, antes de se formular uma política, é necessário ter em linha de conta os objectivos da empresa bem como os seus processos e cultura organizacional.

A exequibilidade das políticas (em termos de implementação e observância) constitui outro factor essencial. De pouco ou nada servirá ter uma política de SSI se a sua exequibilidade se revela impossível.

Como forma de reforçar o exposto, apresenta-se como conclusão desta secção o entendimento de Guel [2007, p. 27] sobre os factores básicos a ter em conta numa política.

Para este autor, as políticas devem ser implementáveis e passíveis de serem revistas, ser concisas e fáceis de entender, equilibrarem a protecção com a produtividade. Para além disso, o mesmo autor defende que as políticas devem ainda expor as razões pelas quais são necessárias, descrever o que abrangem, definir as responsabilidades dos utilizadores e quem contactar em caso de dúvidas ou excepções, e definir como se deve lidar com as violações ao articulado na política.

Embora muitos dos factores anteriormente apontados pareçam óbvios têm de ser mencionados e levados em linha de conta ao longo do processo de formulação, implementação e revisão da política. A principal linha de fundo para as políticas é que realmente possam ser implementadas. Também se pretendem políticas concisas e fáceis de ler e entender. Deve ter-se em mente quando se desenvolve uma política de SSI se está de acordo com o sistema legal e outras infra-estruturas já existentes. Uma vez aprovadas, as políticas devem ser disponibilizadas para todos os utilizadores afectados com a sua implementação. Finalmente, todas as políticas deveriam ser actualizadas ou revistas pelo menos numa base anual para reflectir as alterações ocorridas na organização.

Os factores anteriormente enumerados facilmente serão aceites como importantes pelos interessados no estudo e na aplicação das políticas de SSI. No entanto, muitos destes factores denotam uma natureza genérica, o que parcialmente se entende por via do número reduzido de estudos empíricos realizados sobre a aplicação das políticas, bem como pela pouca atenção devotada aos aspectos contextuais e processuais da utilização das políticas, por contraste com a ênfase que tem sido dada aos aspectos de conteúdo. Estas observações relativas ao estudo da investigação

existente sobre políticas de SSI já tinham sido referidas no capítulo introdutório deste documento.

Ultimamente, parece assistir-se a um esforço da comunidade científica em estudar empiricamente os factores com impacto sobre a aplicação das políticas de SSI. Um exemplo ilustrativo desse esforço é o trabalho realizado por Karyda et al. [2005]. Neste estudo os autores exploram o processo de formulação, implementação e adopção de uma política de segurança em duas organizações diferentes. O objectivo destes autores foi identificar como é formulada e implementada uma política de segurança numa organização específica e quais os factores que afectam a sua adopção com sucesso, tendo isolado um conjunto de factores de natureza contextual que para os casos estudados influenciariam, significativamente, a aplicação das políticas. Os factores isolados foram os seguintes:

- Estrutura organizacional – Uma estrutura organizacional rígida pode constituir um obstáculo para a gestão da SSI, na medida em que a aplicação de uma política da segurança requer frequentemente uma organização flexível, em que seja possível a criação de novos papéis ou a adaptação dos papéis existentes.
- Cultura organizacional – As organizações que dispõem de uma cultura organizacional coerente estarão melhor capacitadas para adoptar e observar uma política de segurança, especialmente quando os seus colaboradores já seguem um código de prática ou de ética. A aplicação bem sucedida de uma política pressupõe, ainda, a promoção entre os utilizadores de um entendimento comum e partilhado, o que é facilitado pela existência de experiências prévias ao nível da adopção de um código de prática comum.
- Contribuição para as metas dos utilizadores – Os utilizadores tenderão a adoptar as provisões da política de segurança quando esta estiver alinhada com os seus objectivos profissionais e assistir de forma eficaz no cumprimento dos seus deveres profissionais.
- Participação dos utilizadores no processo de formulação – O envolvimento dos utilizadores no processo de formulação, a par da atribuição de responsabilidades acrescidas a esses agentes, potencia o desenvolvimento de uma cultura de segurança na organização e o aumento da sensibilização para a protecção dos activos informacionais da organização.
- Formação e educação – A existência de um programa continuado de formação e educação dos utilizadores no domínio da segurança de sistemas de informação, acompanhado da avaliação da eficácia da política de segurança, concorre para a implementação e adopção bem sucedidas das políticas de segurança de informação.
- Apoio da gestão – A participação activa e o apoio explícito dos gestores da organização constituem factores de máxima importância. Uma vez que a formulação e implementação de uma política de segurança da informação geralmente implica a assimilação de novos comportamentos e o abandono ou alteração de comportamentos anteriores, facilmente se compreenderá que o empenho que os gestores demonstram para com a segurança de sistemas de informação terá impacto substancial na aplicação prática das provisões da política.
- Responsável pela segurança – A existência de um actor organizacional com qualificações e motivação adequadas que seja capaz de conduzir a

formulação e implementação da política de segurança pode contribuir para a implementação e adopção bem sucedidas da política de segurança.

Até certo ponto, o trabalho agora proposto prossegue na mesma senda, havendo o interesse em identificar e compreender os factores que influenciam a adopção de políticas de SSI no contexto particular da Administração Pública Local em Portugal.

2.4 Conclusão

A política de segurança é um documento vital na medida em que funciona como principal orientador dos esforços de protecção de um Sistema de Informação, contudo, nem sempre é fácil o seu desenvolvimento, levantando-se diversas questões respeitantes à forma de as constituir. Daí que não seja de estranhar que muitos autores busquem apoio e orientação nas várias normas internacionais de segurança da informação. Estas normas são um bom ponto de partida para determinar em que é que a política de segurança deve consistir, mas segundo Höne e Eloff [2002a] a busca por orientação não deve resumir-se ao exposto nessas normas. A justificação para este posicionamento prende-se com o facto das normas nem sempre abarcarem tudo aquilo que importa para o processo de adopção das políticas, concentrando-se, muitas das vezes, em orientar os processos conexos à implementação bem sucedida de uma política. Ou seja, ainda que possam providenciar directivas e exemplos de aplicação, as normas estipulam orientações genéricas, não dispensando aqueles que as pretendem aplicar de proceder aos necessários ajustamentos impostos pela cultura e negócio da organização.

Estas constatações merecem também a concordância de Baskerville e Siponen [2002], que consideram inadequada a utilização de normas genéricas de gestão da segurança da informação nas organizações actuais, as quais são cada vez mais emergentes, uma vez que as normas não prestam suficiente atenção ao facto de diferentes organizações terem diferentes requisitos de segurança.

O valor da informação para as organizações torna clara a necessidade de uma gestão eficaz da SSI, mas este facto só se torna efectivo se o seu planeamento foi verdadeiramente realizado. No que concerne às políticas de SSI, este princípio aplica-se de igual forma.

Contudo, é necessário ter em conta que não existem “pacotes” de políticas universais que se aplicam a qualquer organização. Cada política de SSI é única, como o são as necessidades de segurança de cada organização [Diver 2007; Schweitzer 1982; Whitman et al. 2001; Wood 1999]. O desenvolvimento e implementação de uma política tem de ter sempre em conta a natureza do negócio, bem como a sua visão e objectivos, pois só assim a política poderá dar resposta eficaz às necessidades de segurança da organização.

A formulação e consequente implementação de políticas de SSI nas organizações requerem uma reflexão e estudo prévio cuidado. Todavia, este não é o único aspecto a ter em conta, sendo também necessário consciencializar os envolvidos de que a tecnologia não é o único elemento a considerar, sem a existência de uma política de

SSI, métodos de resposta a incidentes ou planos de continuidade do negócio, as tecnologias não serão eficazes na protecção da informação na organização.

Outro aspecto a ter em conta diz respeito à sensibilização dos utilizadores e dirigentes em relação às problemáticas da segurança, uma vez que o factor humano é apontado como o responsável por grande parte dos incidentes de segurança. A sua sensibilização é fundamental para se conseguir que a política de SSI organizacional produza o efeito desejado.

Capítulo 3

Caracterização das Câmaras Municipais

3.1 Introdução

No capítulo anterior apresentou-se a revisão da literatura relevante para a temática das políticas de SSI. No presente capítulo, que precede a apresentação dos resultados do levantamento realizado sobre a temática de investigação identificada, apresenta-se a caracterização das Câmaras Municipais Portuguesas, focando-se numa visão geral, na dimensão dos Municípios, o perfil dos dirigentes Autárquicos e a presença das TSI nas Câmaras Municipais.

Dado que o presente trabalho se debruça sobre a adopção de política de SSI na administração pública local em Portugal, impunha-se compreender a realidade do Poder Local português, designadamente pela respectiva contextualização legal, política, sociológica, económica e financeira.

Os Municípios portugueses apresentam características díspares e estádios diferenciados no domínio da utilização de SI e, consequentemente, das respectivas políticas de SSI. Assim, não poderia o presente estudo avançar sem antes se efectuar uma análise concreta ao quadro autárquico municipal nacional.

As Autarquias locais encontram-se previstas no Artigo 235.º n.º 1 da Constituição da República Portuguesa (CRP), determinando a Lei fundamental no n.º 2 daquele artigo que por Autarquias locais se devem compreender as "pessoas colectivas territoriais dotadas de órgãos representativos, que visam a prossecução de interesses próprios das populações respectivas". Assim prevê a CRP, no artigo 236.º, a existência de Autarquias Locais de três níveis: Regiões Administrativas, Municípios e Freguesias. Importa no entanto ressalvar que no que diz respeito às Regiões Autónomas (Açores e Madeira) a Lei fundamental do Estado Português apenas prevê a existência de Autarquias de âmbito Municipal e de Freguesia.

Os Municípios e Freguesias, desde o advento do regime democrático português, lograram conquistar uma posição plenamente consolidada na orgânica pública do País. Porém, no que se refere às regiões administrativas, mercê de vicissitudes políticas e constitucionais, estas continuam a não merecer a sua plena instituição, aguardando o encontro de vontades entre poder político e cidadãos.

Nas três décadas em que o País vive em regime democrático assistiu-se ao florescimento e afirmação de um poder Autárquico consolidado que pauta a sua acção pela lógica da proximidade da Administração com os administrados. Tal facto, aliado a uma forte tradição comunitária, ajudará a explicar a existência de 308 Municípios, dos quais 278 se encontram no território continental e 30 localizados nos territórios insulares, isto é, nas Regiões Autónomas dos Açores e da Madeira.

Porém, se se analisar o número de Municípios actualmente existentes no País em confronto com o número de habitantes e com a dimensão territorial deste, não deixará de surpreender qualquer observador que verifique a existência, actualmente, de 4259 Freguesias, das quais 4050 se localizam no território continental e 209 nos territórios insulares.

Como já referido, os Municípios compreendem, para a sua acção, a existência de dois órgãos colegiais, expressamente previstos na Constituição da Republica Portuguesa, designadamente no seu artigo 250.º, e que se denominam por Assembleia e Câmara Municipal com funções deliberativas e executivas, respectivamente (cf. Artigo 251.º e 252.º da CRP).

Como observado no início do presente trabalho focalizar-se-á a atenção e estudo em torno das dinâmicas de trabalho das Câmaras Municipais, uma vez que estas prosseguem a sua acção de forma permanente e continuada, assumindo as Assembleias Municipais uma acção mais cíclica ou sazonal, sempre decorrente das cinco sessões ordinárias que anualmente este órgão realiza.

Assim, e atenta a natureza do presente trabalho de investigação, centrar-se-á a análise ou avaliação do fenómeno Municipal Português em torno dos seguintes parâmetros: caracterização geral das Câmaras Municipais, aspectos que se prendem com as tecnologias e sistemas de informação, vertente da segurança de sistemas de informação nestas edilidades, sendo por fim apresentada uma breve conclusão que sumaria a discussão desenvolvida.

3.2 Caracterização Geral

Sendo o órgão executivo dos Municípios, às Câmaras Municipais estão acometidas um conjunto de competências para a persecução das atribuições legalmente conferidas àquelas pessoas colectivas de direito público territorial. Assim, pode-se agrupar as várias dezenas de competências legalmente atribuídas às Câmaras Municipais pelo artigo 64.º da Lei 169/99 de 18 de Setembro, na redacção introduzida pela Lei n.º 5-A/2002 de 11 de Janeiro, em sete grandes capítulos, a saber:

1. Competências decorrentes da sua organização, funcionamento e gestão corrente

Entre as competências contidas neste ponto encontram-se fixar as tarifas e os preços da prestação de serviços ao público, apoiar ou comparticipar no apoio à acção social escolar, organizar e gerir os transportes escolares e deliberar sobre a atribuição de subsídios a instituições legalmente existentes.

2. Competências no âmbito das suas actividades de planeamento e desenvolvimento

Das competências aferidas a este ponto, podem-se destacar a elaboração e submissão à aprovação da assembleia municipal e ao executivo de uma série de documentos obrigatórios para a prossecução das suas competências.

3. Competências de natureza e âmbito consultivo

As competências incluídas neste ponto são emitir parecer, nos casos e nos termos previstos na lei, sobre projectos de obras não sujeitas a licenciamento municipal e participar em órgãos consultivos de entidades da administração central, nos casos estabelecidos por lei.

4. Competências de apoio às actividades de interesse municipal

De entre as competências de apoio às actividades de interesse municipal pode-se destacar o apoio ou comparticipação no apoio a actividades de interesse municipal, de natureza social, cultural, desportiva, recreativa e participar na prestação de serviços a extratos sociais desfavorecidos ou dependentes.

5. Competências de licenciamento e fiscalização

Compete à câmara municipal, em matéria de licenciamento e fiscalização, emitir licenças para construção, reedificação, utilização, conservação ou demolição de edifícios, assim como para estabelecimentos insalubres, incómodos, perigosos ou tóxicos. É também competência das Câmaras realizar vistorias e executar, de forma exclusiva ou participada, a actividade fiscalizadora atribuída por lei, nos termos por esta definidos e ordenar, precedendo vistoria, a demolição total ou parcial ou a beneficiação de construções que ameacem ruína ou constituam perigo para a saúde ou segurança das pessoas.

6. Competências no âmbito das suas relações com os demais órgãos autárquicos

Compete às câmaras municipais, no que respeita às suas relações com outros órgãos autárquicos, deliberar sobre formas de apoio às freguesias e propor à assembleia municipal a concretização de delegação de parte das competências da câmara nas freguesias.

7. Competência de carácter regulamentador

Compete ainda às câmaras municipais elaborar e aprovar posturas e regulamentos em matérias da sua competência exclusiva, administrar o domínio público municipal, deliberar sobre declarações de utilidade pública para efeitos de expropriação, etc.

Para melhor conhecimento e aprofundamento das competências legalmente consignadas às Câmaras Municipais dever-se-á consultar a Lei n.º 169/99 de 18 de Setembro que estabelece o quadro de competências, assim como o regime jurídico de funcionamento dos órgãos dos municípios e das freguesias, cujo artigo 64.º, que apresenta as competências atribuídas por esta lei às Câmaras Municipais, se encontra no Apêndice D.

O fenómeno Municipal Português não apresenta linhas de caracterização uniformes ou comuns à universalidade de Municípios actualmente existentes. Com efeito, os Municípios Portugueses, como fenómenos locais que são, e por maioria de razão, os órgãos que os representam, acabam por reflectir as vicissitudes e constrangimentos do meio físico e humano em que se integram.

Assim, dos 308 Municípios Portugueses pode-se afirmar sem qualquer margem para dúvidas que assumem a primazia legal e hierárquica os Municípios de Lisboa e do Porto, não só por razões de natureza populacional, mas sobretudo por questões de natureza histórica que acabaram por se plasmar na Lei das Autarquias Locais 169/99 de 18 de Setembro, a qual acaba por determinar no seu artigo 57.º n.º 2 um regime diferenciado para a composição das Câmaras de Lisboa e do Porto em relação às demais edilidades do País. De facto, verifica-se que o número de membros dos executivos municipais se encontra taxativamente fixado para Lisboa e para o Porto, enquanto para os demais Municípios o número de membros dos seus executivos varia em função das flutuações populacionais.

Efectivamente, na já referida norma legal determina-se expressamente que as Câmaras de Lisboa e do Porto compreendem respectivamente 16 e 12 Vereadores, além dos respectivos Presidentes, enquanto, para os demais municípios se fixa um critério populacional na seguinte razão:

- 1 Presidente mais 10 Vereadores nos municípios com 100000 ou mais eleitores
- 1 Presidente mais 8 Vereadores nos municípios com mais de 50000 e menos de 100000 eleitores
- 1 Presidente mais 6 Vereadores nos municípios com mais de 10000 e até 50000 eleitores
- 1 Presidente mais 4 Vereadores nos municípios com 10000 ou menos eleitores

Este será de resto o critério metodológico a adoptar no presente estudo para efeito de análise da dimensão dos executivos municipais.

3.2.1 Dimensão dos Municípios

Atento o critério previamente determinado e do qual já se deu conta, bem como dos fundamentos da sua adopção, procede-se nesta subsecção a uma análise global da dimensão das edilidades municipais pela atribuição de uma designação específica em função da respectiva dimensão eleitoral, conforme se explana na Tabela 3.

Classes de Dimensão Eleitoral	
A	Mais de 100.000 eleitores (autarquias muito grandes)
B	50.000 a 100.000 eleitores (autarquias grandes)
C	10.000 a 50.000 eleitores (autarquias médias)
D	Até 10.000 eleitores (autarquias pequenas)

Tabela 3: Classes de Dimensão Eleitoral

Considerando estas dimensões em termos de número de eleitores por município, o agrupamento resultante é o constante da Tabela 4.

A - Muito Grandes	B - Grandes	C – Médios	D - Pequenos
20 Municípios	21 Municípios	150 Municípios	117 Municípios

Tabela 4: Número de Municípios por Classe de Dimensão Eleitoral

Não surpreenderá que a dimensão dos executivos municipais reflicta as disparidades e assimetrias de distribuição populacional reconhecidas de forma quase empírica, sem a atenção devida à importância da dimensão territorial destas unidades administrativas. Assim, e tendo em conta os critérios fixados para a composição das Câmaras Municipais, bem como aqueles que estão fixados para o seu financiamento, e que terão reflexos na dimensão do seu quadro de pessoal, não será difícil concluir que as Câmaras Municipais de maior dimensão se encontrarão localizadas, no que se refere ao território continental, na faixa litoral deste território, enquanto as Câmaras Municipais de menor dimensão se encontram localizadas no interior do País, debatendo-se não raras vezes com graves problemas ou dificuldades financeiras com implicações ao nível do seu funcionamento, dimensão e quadro de funcionários.

As prioridades de ordem política fixadas pela generalidade dos executivos nas últimas três décadas consistiram fundamentalmente na infra-estruturação do País, em particular nos domínios da salubridade, do abastecimento de água e vias de comunicação terrestres, tendo as Câmaras Municipais, no início da sua actividade, actuado numa lógica de auto-suficiência procurando a satisfação das suas necessidades de acção pelo provimento dos seus respectivos quadros de pessoal, facto que concorre para a forte restrição na capacidade de recrutamento de técnicos em novas áreas do conhecimento e de execução de políticas públicas, já que os quadros se encontram esgotados nas áreas anteriormente prioritárias.

Este facto será aliás uma das razões que poderá explicar o exíguo número de lugares actualmente preenchido por técnicos de informática nos múltiplos quadros de pessoal das Câmaras Municipais.

A representação gráfica evidenciada na Figura 11, em confronto com o Apêndice A, revela a correcção e sustentação da análise e reflexão exposta no parágrafo anterior, já que procura cruzar os dados relativos à dimensão eleitoral dos municípios com os financiamentos, designadamente por via das transferências do orçamento geral do Estado de 2010 (cf. Apêndice E), de que estes foram beneficiários e que serão tão mais importantes quanto menor for o número de eleitores desses municípios.

3.2.2 Financiamentos

A Constituição da República Portuguesa prevê no artigo 338.º n.º 1 que as Autarquias Locais têm um património e finanças próprios, prevendo o n.º 3 daquele artigo que as receitas próprias das autarquias locais incluem obrigatoriamente as provenientes da gestão do seu património e as cobradas pela utilização dos seus serviços, podendo mesmo dispor de poderes tributários nos casos e termos previstos por Lei. Determina ainda o artigo 254.º n.º 1 da lei fundamental da República Portuguesa que os Municípios participam por direito próprio nas receitas provenientes dos impostos directos.

Verifica-se, assim, que as Câmaras Municipais, que constituem o verdadeiro poder executivo dos municípios, sofrem pela redacção daquelas normas constitucionais o seu primeiro grande constrangimento financeiro, porquanto indexando-se as receitas obtidas pelos municípios quer às prestações de serviços por si efectuados quer por via da participação nos impostos directos, que a lei determina que se faça em

referência ao seu universo populacional, resultará numa limitação do seu quadro de receitas. Assim será tanto maior a capacidade de prestar serviços quanto maior for o número de potenciais beneficiários desses serviços, facto que também ocorre ao nível da participação nos impostos directos, já que quanto maior for o número de contribuintes maior será a capacidade de receita tributária.

Convirá, no entanto, referir que a participação das autarquias nos impostos directos do Estado se faz por via das transferências, previstas anualmente na Lei do Orçamento Geral do Estado (aprovada pela Assembleia da República em Novembro ou Dezembro) e executada pela Direcção Geral das Autarquias Locais e compreendendo sobretudo três capítulos fundamentais: o Fundo Geral Municipal (FGM), o Fundo de Coesão Municipal (FCM) e o Fundo de Financiamento das Freguesias (FFF).

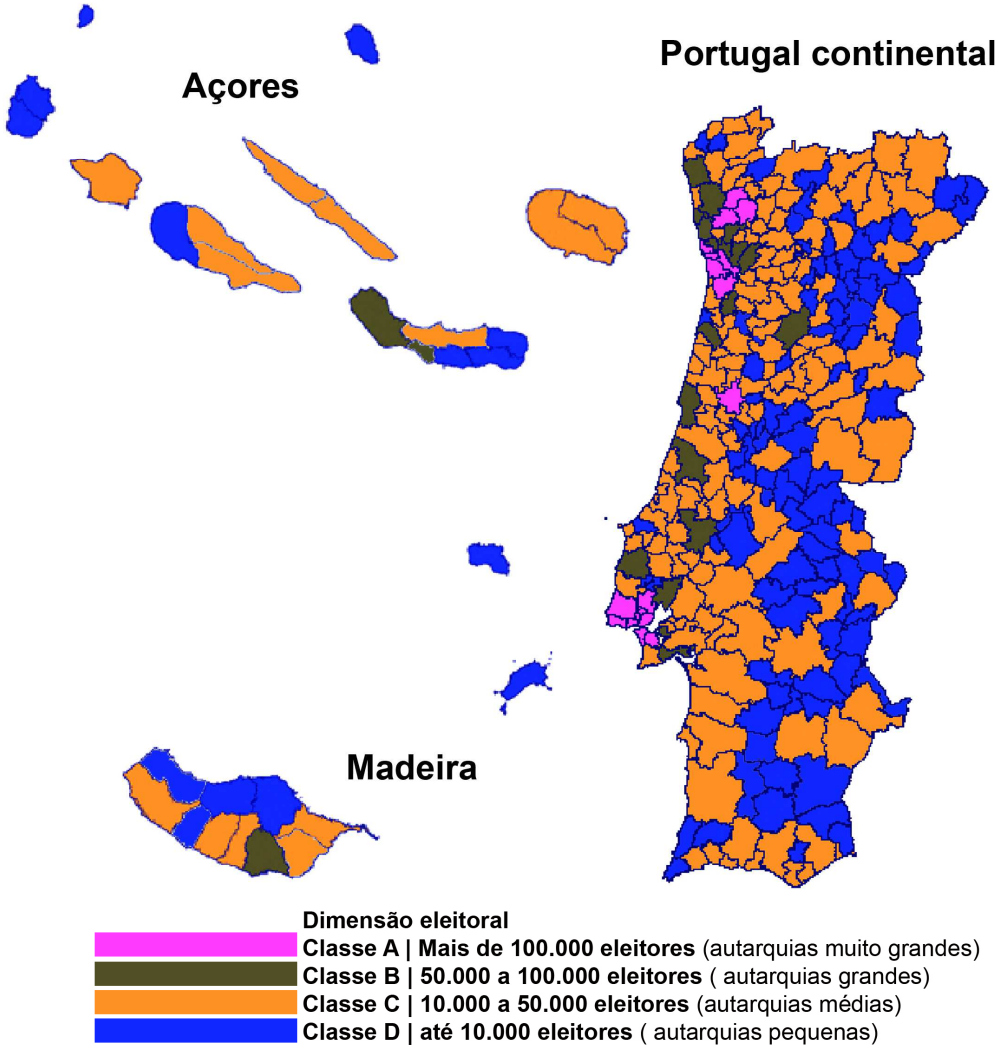


Figura 11: Distribuição Geográfica das Câmaras segundo a sua Dimensão

Os impostos directos do Estado têm o seu peso nos resultados económicos das autarquias, mas os seus impostos directos, como o Imposto Municipal de Imóveis (IMI), o Imposto sobre o Rendimento das Pessoas Singulares (IRS) e o Imposto

sobre Veículos, tem igualmente o seu valor. O Anuário Financeiro dos Municípios Portugueses de 2006 e de 2009, elaborado por uma equipa de Professores da Universidade do Minho com o apoio do Tribunal de Contas, da Câmara dos Técnicos Oficiais de Contas e da Fundação para a Ciência e Tecnologia, cujo objectivo é analisar o grau de implementação do Plano Oficial de Contabilidade das Autarquias Locais (POCAL) e as suas consequências na gestão dos municípios, apresenta um número elevado de dados, dos quais se apresentam neste trabalho de investigação os Municípios com maiores e com menores Resultados Económicos, os quais podem ser apreciados nas Tabelas 5 e 6.

	Município	Valor (Euros)
1	Lisboa	35 611 849
2	Oeiras	23 339 640
3	Castelo Branco	12 323 729
4	Braga	12 088 000
5	Guimarães	10 789 777
6	Ponta Delgada	9 325 482
7	Sesimbra	8 757 150
8	Pombal	8 497 740
9	Sintra	7 079 024
10	Amadora	6 930 108
11	Porto	6 373 035
12	Alcobaça	6 231 774
13	Grândola	4 483 890
14	Leiria	4 344 182
15	Vale de Cambra	4 232 226
16	Montemor-o-Novo	4 091 994
17	Ílhavo	4 033 704
18	Tavira	3 909 434
19	Oliveira do Bairro	3 508 472
20	Ribeira Grande	3 428 731
21	Gondomar	3 269 514
22	Serpa	3 118 083
23	Arouca	2 931 323
24	Viana do Castelo	2 764 101
25	Coimbra	2 553 922
26	Odivelas	2 457 870
27	Odivelas	2 306 810
28	Ponte de Sor	2 251 140
29	Resende	2 175 001
30	Oliveira do Hospital	2 169 730

Tabela 5: Municípios com Maiores Resultados Económicos (valores absolutos)
Adaptado de Carvalho et al. [2011]

	Município	Valor (Euros)
1	Portimão	-40 115 633
2	Marco de Canaveses	-37 694 151
3	Aveiro	-21 244 711
4	Vila Real de Santo António	-19 544 319
5	Évora	-18 331 888
6	Matosinhos	-18 097 181
7	Cascais	-18 084 234
8	Loures	-14 304 622
9	Covilhã	-11 378 706
10	Olhão	-10 978 976
11	Mafra	-10 548 614
12	Palmela	-9 907 991
13	Seixal	-9 653 485
14	Trofa	-6 624 903
15	Figueira da Foz	-8 440 120
16	Santa Cruz	-8 383 833
17	Vila Franca do Campo	-8 038 615
18	Lourinhã	-7 938 943
19	Lagos	-7 142 851
20	Lagoa (Algarve)	-7 108 687
21	Valongo	-7 108 577
22	Moura	-7 002 177
23	Albufeira	-6 154 624
24	Vila Verde	-5 494 585
25	Torres Vedras	-5 424 676
26	Oleiros	-5 338 911
27	Vagos	-5 264 372
28	Ribeira Brava	-5 095 328
29	Espinho	-5 016 580
30	Vila do Bispo	-4 891 336

Tabela 6: Municípios com Menores Resultados Económicos
Adaptado de Carvalho et al. [2011]

O valor global de Resultados Líquidos foi de 656 milhões de Euros (contra 570 milhões de Euros em 2005), o que representa uma melhoria da situação económica dos municípios e um aumento dos Fundos Próprios [Carvalho et al. 2006]. As tabelas anteriores apresentam os 30 municípios com melhores e piores resultados económicos, respectivamente.

Relativamente aos resultados económicos verificou-se que: 236 municípios apresentaram resultados económicos positivos (226 em 2005), continuando no entanto a interpretação deste indicador a ser muito subjectiva e carecendo de uma análise simultânea de outros indicadores, nomeadamente com o saldo efectivo. Os resultados líquidos globais para os 307 municípios foram de 664 milhões de Euros, o que corresponde a cerca de 66,1 euros por habitante (52,9 euros por habitante em 2005) [Carvalho et al. 2006, p. 175]. Em 2009, face aos fracos resultados económicos, o rácio "Resultados económicos por habitante" apresenta o valor negativo de -21 euros [Carvalho et al. 2011, p. 168].

A variação global dos Fundos Próprios entre 2006 e 2009 em +1.829,3 milhões de euros (+8,1%) foi inferior em 73,5 milhões de euros, ao aumento do fundo patrimonial no mesmo período. A causa desta situação esteve na diminuição sucessiva dos resultados líquidos do exercício, que entre 2006 e 2009 baixaram 890 milhões de euros apresentando, para a globalidade das autarquias, um resultado líquido negativo, em 2009, de -226,2 milhões de euros. Em 2008, os resultados líquidos já tinham apresentado um decréscimo de cerca de 38% relativamente a 2007 [Carvalho et al. 2011, p. 145].

3.2.3 Perfil dos Dirigentes Autárquicos

Pelo número elevado de funcionários e eleitos adstritos ao funcionamento das Câmaras Municipais e pelo constrangimento decorrente das balizas temporais para a realização do presente trabalho, concentrar-se-á na análise do perfil dos Presidentes de Câmara dos 308 Municípios Portugueses e de cujos números se visualizam na Tabela 7 em termos de profissão.

Profissão	Número
Professor	58
Engenheiro	38
Advogado	29
Bancário	21
Economista	19
Gestor	16
Médico	15
Aposentado	14
Empresário	9
Engenheiro Técnico	7
Técnico Superior	6
Funcionário Público	5
Político	4
Jurista	3
Escriturário	2
Arquitecto	2
Sociólogo	2
Notário	2
Comerciante	2
Industrial	2
Analista de Sistemas	2
Electricista	2
Empregado de Escritório	2
Director de Departamento	2
Operário	2
Técnico	2
Agente Técnico Agrícola	1
Operador de Sistemas Informáticos	1
Funcionário de Partido Político	1

Chefe de Finanças	1
Delegado de Informação Médica	1
Oficial de tráfego	1
Gerente Hospitalar	1
Topógrafo	1
Psicólogo	1
Administrador	1
Licenciado em História	1
Licenciado em Filosofia	1
Desenhador/Projectista	1
Membro de Ordem Religiosa	1
Contabilista	1
Consultor Jurídico	1
Não enviaram os dados	24
Total	308

Tabela 7: Profissão dos Presidentes de Câmara
STAPE [2008a]

Os números evidenciados pela Tabela 7 revelam que os presidentes de Câmara possuem, regra geral, formação superior provindo de profissões ligadas ao ensino ou a profissões liberais, as quais se caracterizam pelo contacto com o público e tradicionalmente pautadas pela militância e por uma cidadania activa.

3.3 Tecnologias e Sistemas de Informação nas Câmaras Municipais

Na secção anterior foram caracterizadas as Câmaras Municipais de uma forma geral. Essa classificação teve por base aspectos que poderão importar ter em conta para o estudo das práticas de SSI. Nesta secção serão apresentados os estudos existentes e de que se tem conhecimento, acerca das tecnologias e sistemas de informação nas Câmaras Municipais, bem como a principal legislação aplicável nestas áreas. Ressalva-se o facto de a discussão apresentar uma forte vertente na Internet, em virtude dos estudos disponíveis e consultados.

3.3.1 Dados de Estudos Realizados

Neste domínio foi realizado um estudo em 2006 às Câmaras Municipais cujo principal objectivo foi analisar a utilização das TIC. Existem estudos mais recentes contudo não abordam esta temática. Os promotores desse estudo foram o Observatório da Sociedade da Informação e do Conhecimento e a Agência para a Sociedade do Conhecimento (cf. OSIC e UMIC [2006]).

Os principais resultados desse inquérito à utilização das TIC nas Câmaras Municipais foram:

1. 93% das Câmaras Municipais dispõe de uma velocidade de ligação à Internet superior ou igual a 512 Kbps, sendo que 64% tem ligações superiores ou iguais a 2 Mbps (crescimento de 68% de 2005 para 2006);

2. 96% da Câmaras Municipais tem presença na Internet;

3. Nos serviços disponibilizados nos *websites* das Câmaras Municipais na Internet prevalece o correio electrónico (78%), sendo que 74% das Câmaras Municipais com presença na Internet disponibiliza o *download* e a impressão de formulários e 36% conduz processos de consulta pública aos cidadãos via Internet;

4. 14% das Câmaras Municipais disponibiliza nos seus *websites* fóruns de discussão entre o executivo camarário e os cidadãos (crescimento de 40% de 2005 para 2006);

5. As Câmaras Municipais que declaram manter os seus *websites* permanentemente actualizados aumentou de 69% para 80%, de 2005 para 2006;

6. As Câmaras Municipais que cooperam com outras no desenvolvimento ou aquisição de aplicações informáticas cresceu de 38% para 44%, de 2005 para 2006;

7. Respectivamente 43% e 30% das Câmaras Municipais usa software de código aberto para os sistemas operativos e para os servidores de Internet;

8. 16% das Câmaras Municipais efectua encomendas através da Internet, sendo que os produtos mais adquiridos são os consumíveis informáticos.

Pode-se destacar destes resultados a forte presença na Internet e, embora ainda numa percentagem reduzida de Câmaras Municipais, a efectuação de encomendas através da Internet. Outro aspecto que se destaca é a crescente disponibilização de acesso à Internet aos funcionários da Câmara, ainda que em 2006 pouco mais do que metades dos Municípios o facultem. Algumas destas constatações são evidenciadas na Tabela 8 (sendo TMCA a Taxa Média de Crescimento Anual).

Indicadores da Presença na Internet	2003 (%)	2004 (%)	2005 (%)	2006 (%)	TMCA
Câmaras Municipais que dispõem de uma velocidade de ligação à Internet superior ou igual a 512 Kbps	31	61	85	93	44
Câmaras Municipais com presença na Internet	84	91	96	96	5
Câmaras Municipais que têm uma política de disponibilização do acesso à Internet a todos os trabalhadores	33	42	49	56	19

Tabela 8: Síntese dos Principais Indicadores
Fonte: OSIC e UMIC [2006]

Serviços/informações internas disponibilizados na Intranet

Os serviços disponibilizados *online* para os funcionários e outros que tenham acesso à Intranet são apresentados na Tabela 9, onde se observa que os principais serviços ou informações internas que as Câmaras Municipais disponibilizam na Intranet são os

contactos do Município, Legislação, Bases de dados, Composição dos órgãos executivos e administrativos do Município e o Organigrama. É de destacar que 46% das Câmaras Municipais têm implementada uma Intranet.

Serviços e Informação Disponibilizados na Intranet	(%)
Contactos (telefone, fax, correio electrónico, etc.)	73
Legislação	65
Base de dados	58
Composição dos órgãos executivos e administrativos do município	56
Organogramas	55
Calendário de reuniões e eventos	49
Contabilidade e orçamentos	39
Política de recursos humanos	33
Lista de Questões Frequentes (FAQ's)	32
Acções de formação interna	32
Fórum de discussão electrónica	17
Shareware	14

Tabela 9: Serviços e Informação Disponibilizados na Intranet
Fonte: OSIC e UMIC [2006]

Utilização da Internet

O estudo efectuado pelo OSIC e UMIC [2006] concluiu sobre este ponto que todas as Câmaras têm ligação à Internet. Contudo, só 28% dos funcionários utilizam regularmente a Internet. As actividades realizadas através da Internet estão em evidência na Tabela 10, onde se observa que a busca de informação, o correio electrónico e a troca electrónica de ficheiros são as actividades mais realizadas pelos funcionários das Câmaras Municipais.

Actividades Realizadas através da Internet	(%)
Procura e recolha de informação/documentação	99
Correio electrónico	98
Troca electrónica de ficheiros	96
Consulta de catálogos de aprovisionamento	83
Acesso a bases de dados	83
Comunicação externa com outros municípios, Juntas de Freguesias e organismos da AP Central	79
Divulgação de produtos e serviços da Câmara	74
Interface com o cidadão	51
Venda de produtos e serviços da Câmara	12

Tabela 10: Actividades Realizadas através da Internet
Fonte: OSIC e UMIC [2006]

Presença na Internet

Enquanto 100% das Câmaras Municipais se encontram ligadas à Internet, 96% das Câmaras disponibilizam um *site* na Internet. As razões apontadas para essa presença, através da criação de *websites*, deve-se fundamentalmente a três aspectos. O primeiro

aspecto é a promoção turística e cultural, a divulgação institucional ocupa o segundo lugar, sendo a divulgação dos eventos culturais e outras actividades promovidas pela Autarquia o terceiro motivo mais apontado (cf. Tabela 11).

Razões Determinantes para a Criação do *Website*	(%)
Promover o turismo e a cultura	99
Divulgar informação institucional da Câmara Municipal	99
Divulgar a agenda cultural/desportiva e outras actividades	97
Estreitar o relacionamento entre o poder local e os cidadãos	89
Promover o desenvolvimento socio-económico do município	82
Aproximar as comunidades emigrantes do seu município	75
Promover as tecnologias da informação junto dos municípios	74
Disponibilização de serviços *online*	62

Tabela 11: Razões Determinantes para a Criação do *Website*
Fonte: OSIC e UMIC [2006]

Funções e tipo de informação disponíveis no *website* da Câmara Municipal

As funções disponíveis nos *Websites* das Câmaras Municipais encontram-se listadas na Tabela 12. Esta Tabela evidencia que as funções que com mais frequência são disponibilizadas pelas autarquias são o correio electrónico e a disponibilização de *download* e impressão de formulários.

Funções Disponíveis no *Website*	(%)
Correio electrónico para emissão de sugestões e reclamações	78
Download e impressão de formulários	74
Subscrição de *newsletters*	41
Processos de consulta pública (e.g. PDM)	36
Apoio ao utilizador	27
Inquéritos aos cidadãos	24
Encomenda de material referente ao município	22
Preenchimento e submissão *online* de formulários	21
Plataformas de votação *online*	15
Fóruns de discussão entre o executivo camarário e os cidadãos	14
Pagamentos *online* através do *website*	2
Transmissão através de videoconferência, das reuniões e sessões camarárias	2

Tabela 12: Funções Disponíveis no *Website*
Fonte: OSIC e UMIC [2006]

O tipo de informação que contém o *Website* e que está desta forma disponível para os munícipes e público em geral pode ser observado na Tabela 13, destacando-se o organograma da Câmara, informação municipal e planos locais, anúncios, actas e contactos.

Tipo de Informação Disponível no *Website*	(%)
Organograma da Câmara Municipal	83
Informação municipal e planos locais	81
Anúncio de reuniões e eventos camarários	79
Actas e resoluções tomadas em reuniões e sessões camarárias	75
Contactos e curriculum dos principais responsáveis camarários	73
Informação sobre serviços, direitos e deveres dos cidadãos	72
Consulta de taxas municipais	65
Actos administrativos camarários	49
Planos de actividade e relatórios de actividade	49

Tabela 13: Tipo de Informação Disponível no *Website*
Fonte: OSIC e UMIC [2006]

Taxas de evolução dos orçamentos 2008 versus 2007

De acordo com Meneses [2008, p. 21], os investimentos em TI têm tido uma tendência de incremento dos orçamentos. Em 2003, a extrapolação da amostra indicava que a totalidade do segmento valia cerca de 20 milhões de euros. Aplicando o mesmo método, esse valor subiu para 33 milhões em 2004 e 47 milhões em 2005, ano do último pico de investimento. Em 2006 registou-se uma retracção para 35 milhões, seguida de uma subida para 40 milhões em 2007. As taxas de evolução dos orçamentos de 2007 para 2008 podem ser visualizadas no Gráfico 1.

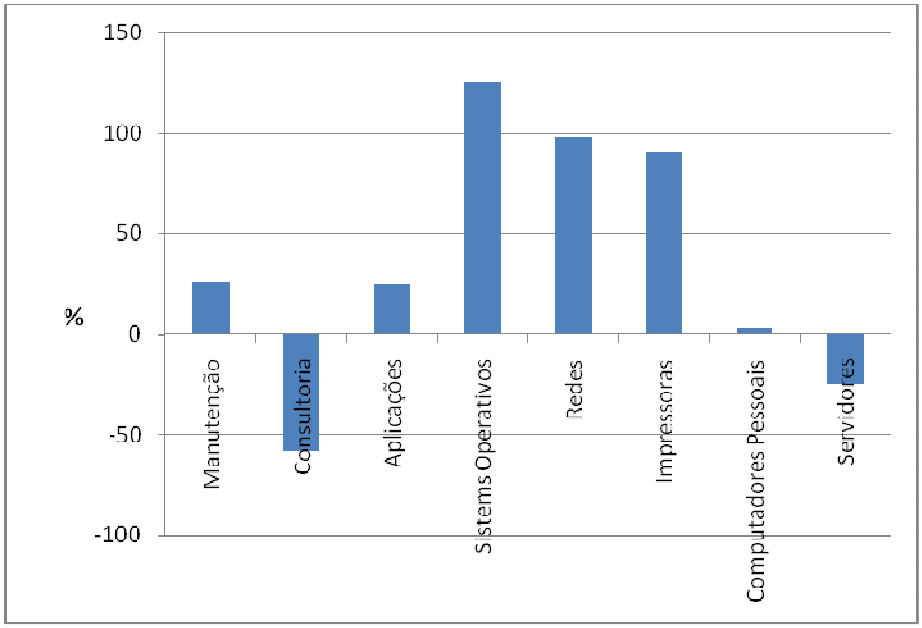


Gráfico 1: Taxas de Evolução dos Orçamentos 2008 versus 2007
Adaptado de Meneses [2008]

Estrutura dos Investimentos em TI

Da leitura dos Gráficos 2 e 3, nota-se que no ano de 2007 mais de metade do orçamento destinado à aquisição de TI se dirige para investimentos em servidores e computadores pessoais. No ano de 2008, embora com um decréscimo, os servidores continuam a ser a principal aquisição seguindo-se o investimento em redes.

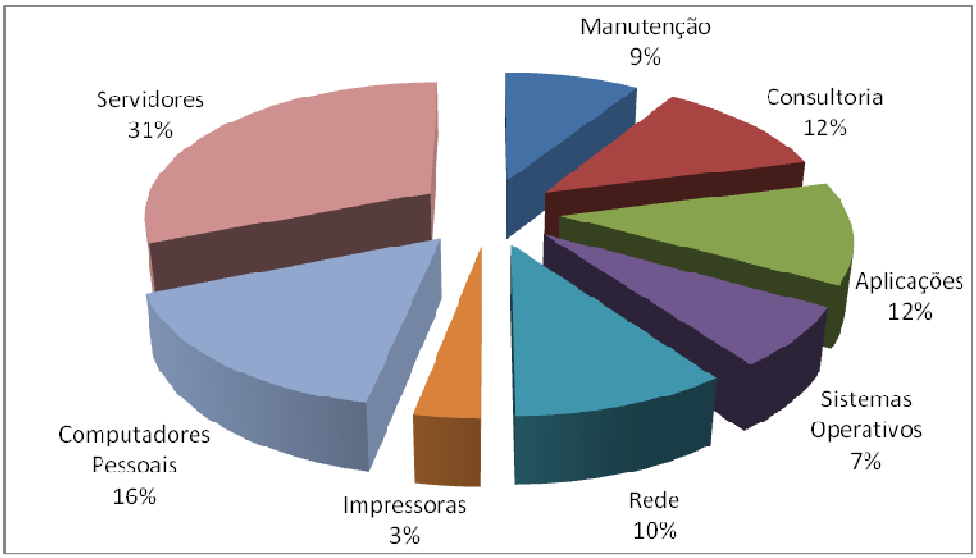


Gráfico 2: Estrutura dos Investimentos em TI em 2007
Adaptado de Meneses [2008]

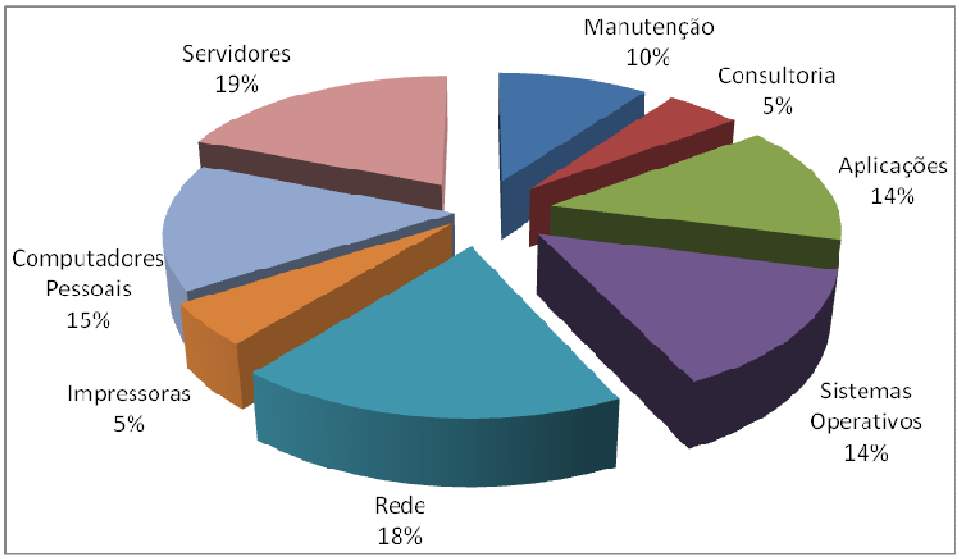


Gráfico 3: Estrutura dos Investimentos em TI em 2008
Adaptado de Meneses [2008]

Para Meneses [2008], as autarquias estão a informatizar-se em maior escala, quer em quantidade de equipamento quer em abrangência das funções informatizadas. Esta interpretação deve-se, em grande parte, ao facto de os equipamentos, nomeadamente os computadores pessoais, estarem com preços cada vez mais reduzidos, e se a percentagem de aquisição ainda é considerável quer dizer que se compram em maior número.

Pessoal das TIC por grau de ensino

Os funcionários das Câmaras Municipais afectos às TIC têm em 54% dos casos o ensino secundário, o que quer dizer que mais de metade do pessoal afecto às TIC são técnicos profissionais, seguindo-se 35% com Bacharelato ou Licenciatura que corresponde a mesma percentagem de técnicos superiores, conforme se apresenta na Tabela 14.

Pessoal TIC por Grau de Ensino	(%)
1º Ciclo/2º Ciclo do Ensino Básico (4ºano/6ºano)	3
3º Ciclo do Ensino Básico (9º ano)	7
Ensino secundário (12º ano)	54
Bacharelato/Licenciatura	35
Mestrado	1

Tabela 14: Pessoal TIC por Grau de Ensino
Fonte: OSIC e UMIC [2006]

No citado estudo promovido pelo OSIC e UMIC [2006], para além do grau de ensino dos trabalhadores afectos às TIC, também é dada a indicação de que 84% das Câmaras têm funcionários exclusivamente afectos às TIC. Embora esta percentagem possa parecer satisfatória, a escassez de pessoal nas TIC é reconhecida por 53% dos inquiridos, contra 41% que não consideram que faltem recursos humanos nessa área.

3.3.2 Legislação Aplicável às Tecnologias e Sistemas de Informação

Após levantamento da regulamentação existente com interesse para a área das Tecnologias e Sistemas de Informação nas Câmaras Municipais, verificou-se a existência de um número considerável de documentos normativos. Estes documentos abordam tópicos como Acessibilidades, Aquisição de bens e serviços, Assinatura digital, Correio e Comércio Electrónico, Comunicações Electrónicas, Conteúdos Digitais, Facturação electrónica, Internet e Sociedade da Informação. Seguidamente, apontam-se os principais regulamentos constituintes de cada uma daquelas classes.

Acessibilidades

Dentro deste tópico destaca-se a resolução do Conselho Europeu de como melhorar o acesso das pessoas com deficiência à sociedade do conhecimento através do e-Acessibilidade. As acessibilidades dos sítios *Web* foi também alvo de um parecer do Comité Económico e Social que considera que, para as pessoas com deficiência, o acesso à informação é um direito humano fundamental, sem o qual não podem usufruir de quaisquer direitos sociais ou políticos; é por isso necessária uma estratégia global e coerente para garantir que haja uma política de desenvolvimento e de inclusão para as pessoas com necessidades especiais. Esta iniciativa tornará o acesso à informação mais fácil e traduzirá o reconhecimento do facto de que a falta de informação origina um elevado grau de exclusão. Dentro deste tópico pode-se referenciar a seguinte regulamentação e pareceres:

- Resolução do Conselho Europeu de 6 de Fevereiro de 2003 relativa à "e-Acessibilidade" – Melhorar o acesso das pessoas com deficiência à sociedade do conhecimento. Jornal Oficial das Comunidades Europeias.
- Parecer do Comité Económico e Social sobre a "Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das regiões sobre eEurope 2002: acessibilidades dos sítios *Web* públicos e do respectivo conteúdo". Jornal Oficial das Comunidades Europeias.

- Resolução do Conselho de Ministros n.º 135/2002, DR n.º 268, I Série B de 20 de Novembro – Define o novo enquadramento institucional da actividade do governo em matéria de sociedade da informação, da inovação e do governo electrónico. – Acessibilidades.

- Despacho n.º 12 029/2002, DR n.º 122, II Série de 27 de Maio - delegação de competências. – Acessibilidade.

- Resolução do Conselho Europeu de 25 de Março de 2002 relativa ao Plano de Acção de 2002 eEuropa sobre a acessibilidade dos sítios *Web* e do seu conteúdo. Jornal Oficial das Comunidades Europeias.

- Comunicação da Comissão ao Conselho Europeu, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões, de 25 de Setembro de 2001 – eEurope 2002: acessibilidades dos sítios *Web* públicos e do respectivo conteúdo. Comissão das Comunidades Europeias.

- Resolução do Conselho de Ministros n. 97/99, DR n.º 199, I Série B, de 26 de Agosto – Estabelece regras relativas à acessibilidade pelos cidadãos com necessidades especiais aos conteúdos de organismos públicos na Internet.

- Resolução do Conselho de Ministros n. 96/99, DR n.º 199, I Série B, de 26 de Agosto – Iniciativa Nacional para os cidadãos com necessidades especiais na sociedade da Informação – documento orientador.

Aquisição de bens e serviços

No tópico Aquisição de Bens e Serviços, a regulamentação fixa regras gerais relacionadas com a aquisição e utilização de tecnologias de informação na Administração Pública, estabelece também o regime jurídico de realização de despesas públicas, e inclui um Decreto-Lei que aprova o regime de aquisição de bens por via electrónica por parte dos organismos públicos. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Decreto-Lei n.º 1/2005, DR n.º 2, I Série A de 4 de Janeiro. Este Decreto-Lei visa dinamizar o clima de concorrência entre fornecedores e promover a aquisição mais eficiente, competitiva e transparente de bens e serviços de comunicações, bem como optimizar as condições técnicas e comerciais de contratos com ou sem vínculo, em vigor ou em vias de renovação. Pretende igualmente dinamizar o desenvolvimento da banda larga na Administração Pública e racionalizar os custos de comunicações.

- Resolução do Conselho de Ministros n.º 111/2003, DR n.º 185 I Série B de 12 de Agosto. Aprova o Programa Nacional de Compras Electrónicas.

- Resolução do Conselho de Ministros n.º 36/2003, DR n.º 60 I Série B de 12 de Março. Determina a adopção de várias medidas concretas visando a generalização da prática da aquisição de bens e serviços por via electrónica na Administração Pública e no tecido empresarial e incumbe a Unidade de Missão Inovação e Conhecimento de proceder à respectiva implementação e acompanhamento, em estreita articulação com outras entidades.

- Decreto-Lei n.º 104/2002, do DR n.º 86, I Série A, de 12 de Abril. Aprova o regime de aquisição de bens por via electrónica por parte dos organismos públicos.

- Decreto-Lei n.º 153/2001, do DR n.º 105, I Série A de 7 de Maio. Estabelece regras em matéria de alienação a título gratuito de equipamento informático pelos organismos da administração central no quadro dos respectivos processos de reequipamento e actualização de material informático.

- Resolução do Conselho de Ministros n.º 25/2001, do DR n.º 51, I Série B de 1 de Março. Medidas que estimulem o apoio à aquisição de computadores e outro material informático pelos funcionários públicos e trabalhadores, bem como à disponibilização aos mesmos desse equipamento pelas empresas e outros empregadores.

- Despacho Normativo n.º 28/2000, do DR n.º 150, I Série B de 1 de Julho. Determina que o cumprimento de comunicação à respectiva entidade de coordenação sectorial dos dados relativos às locações e aquisições onerosas ou gratuitas de bens e serviços de informática seja concretizado através do fornecimento dos dados previstos num novo modelo.

- Portaria n.º 949/99, do DR n.º 252, I Série B de 28 de Outubro. Aprova os modelos de documentos de contratação pública.

- Declaração de rectificação n.º13-A/99, do DR n.º 203, I Série A de 31 de Agosto. Altera uma inexactidão do artigo 12.º, n.º 1, do Decreto-Lei n.º196/99.

- Decreto-Lei n.º 197/99, do DR n.º132, I Série A, de 8 de Junho. Aprova o novo regime jurídico de realização de despesas públicas e da contratação pública relativa à locação e aquisição de bens móveis e serviços.

- Decreto-Lei n.º 196/99, do DR n.º 132, I Série A, de 8 de Junho. Fixa as regras gerais relativas à coordenação da aquisição e utilização de tecnologias de informação na Administração Pública e estabelece regras específicas para a locação, sobre qualquer regime, ou aquisição de bens ou serviços de informática.

<u>Assinatura Digital</u>

O tópico Assinatura Digital tem um conjunto de regulamentação que aborda a aprovação do regime jurídico dos documentos electrónicos e da assinatura digital. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Resolução do Conselho de Ministros n.º 109/2009, do DR n.º 192, 1.ª Série de 2 de Outubro. É referente à identificação, autenticação e assinatura electrónica de cidadãos perante a Administração Pública.

- Decreto Regulamentar n.º 25/2004, do DR n.º 165, I Série B de 15 de Julho 2004. Regulamenta o Decreto-Lei n.º 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital.

- Decreto-Lei n.º 165/2004, do DR n.º 157, I Série A de 6 de Julho 2004. Altera o artigo 29.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto, que aprova o regime

jurídico dos documentos electrónicos e da assinatura digital, na redacção que lhe foi dada pelo Decreto-Lei n.º 62/2003, de 3 de Abril.

- Decreto-Lei n.º 62/2003, do DR n.º 79, I Série A de 3 de Abril 2003. Altera o Decreto-Lei n.º 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital.

- Decreto-Lei n.º 290-D/99, do DR n.º 178, I Série A de 2 de Agosto. Aprova o regime jurídico dos documentos electrónicos e da assinatura digital.

- Directiva 1999/93/CE do Parlamento Europeu e do Conselho Europeu, de 13 de Dezembro. Relativa a um quadro legal comunitário para as assinaturas electrónicas. Jornal Oficial das Comunidades Europeias.

Correio e Comércio Electrónico

Pode-se destacar dentro deste tópico uma Resolução do Conselho de Ministros que determina a adopção de várias medidas concretas visando a generalização da prática da aquisição de bens e serviços por via electrónica na Administração Pública. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Decreto-Lei n.º 7/2004, do DR n.º 5, I Série A de 7 de Janeiro. No uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de Maio, transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico no mercado interno.

- Lei n.º 7/2003, do DR n.º 107, I Série A de 9 de Maio. Autoriza o Governo a legislar sobre certos aspectos legais dos serviços da sociedade da informação, em especial do comércio electrónico, no mercado interno, transpondo para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho Europeu, de 8 de Junho.

- Resolução do Conselho de Ministros n.º 36/2003, do DR n.º 60, I Série B de 12 de Março. Determina a adopção de várias medidas concretas visando a generalização da prática da aquisição de bens e serviços por via electrónica na Administração Pública e no tecido empresarial e incumbe a Unidade de Missão Inovação e Conhecimento de proceder à respectiva implementação e acompanhamento, em estreita articulação com outras entidades.

- Decreto-Lei n.º 104/2002, do DR n.º 86, I Série A, de 12 de Abril. Aprova o regime de aquisição de bens por via electrónica por parte dos organismos públicos.

- Directiva 2000/31/CE do Parlamento Europeu e do Conselho Europeu de 8 de Junho de 2000. Relativa a certos aspectos legais dos serviços da sociedade da informação, em especial do comércio electrónico, no mercado interno.

Comunicações Electrónicas

No tópico Comunicações Electrónicas pode-se destacar o Decreto-Lei n.º 1/2005 que define sete eixos de actuação que visam colocar o sector público entre os melhores prestadores de serviços do País, com serviços públicos de qualidade, transparentes, eficientes e suportados por soluções tecnológicas racionalizadas. A melhoria da qualidade e eficiência das infra-estruturas de comunicações da Administração Pública é um factor determinante para a modernização dos serviços prestados pelo Estado aos cidadãos e às empresas. Dentro deste tópico pode-se referenciar a seguinte regulamentação e pareceres:

- Decreto-Lei n.º 1/2005, do DR n.º 2, I Série A de 4 de Janeiro. Visa dinamizar o clima de concorrência entre fornecedores e promover a aquisição mais eficiente, competitiva e transparente de bens e serviços de comunicações, bem como optimizar as condições técnicas e comerciais de contratos com ou sem vínculo, em vigor ou em vias de renovação. Pretende-se igualmente dinamizar o desenvolvimento da banda larga na Administração Pública e racionalizar os custos de comunicações.

- Resolução do Conselho de Ministros n.º 181/2004, do DR n.º 298 I SÉRIE B de 22 de Dezembro. Aprova o Guia para as Comunicações na Administração Pública.

- Resolução do Conselho de Ministros n.º 109/2003, do DR n.º 185 I Série B de 12 de Agosto. Aprova a Iniciativa Nacional para a Banda Larga.

- Directiva 2002/77/CE da Comissão Europeia, de 16 de Setembro de 2002. Relativa à concorrência nos mercados de redes e serviços de comunicações electrónicas.

- Directiva 2002/22/CE do Parlamento Europeu e do Conselho Europeu de 7 de Março de 2002. Relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas.

- Directiva 2002/21/CE do Parlamento Europeu e do Conselho Europeu de 7 de Março de 2002. Relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas.

- Directiva 2002/20/CE do Parlamento Europeu e do Conselho Europeu de 7 de Março de 2002. Relativa à autorização de redes e serviços de comunicações electrónicas.

- Directiva 2002/19/CE do Parlamento Europeu e do Conselho Europeu de 7 de Março de 2002. Relativa ao acesso e interligação de redes de comunicações electrónicas.

Conteúdos Digitais

A directiva europeia que aborda esta temática estabelece um conjunto mínimo de regras aplicáveis à reutilização e aos meios práticos de facilitar a reutilização de documentos na posse de organismos do sector público dos Estados-Membros. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Directiva 2003/98/CE do Parlamento Europeu e do Conselho Europeu de 17 de Novembro de 2003. Relativa à reutilização de informações do sector público. Jornal Oficial da União Europeia.

Facturação Electrónica

A facturação electrónica é regulamentada por um Decreto Regulamentar e por um Decreto-Lei que visam estabelecer as condições e os requisitos de utilização da factura ou documento equivalente transmitidos por via electrónica pelos sujeitos passivos de relação jurídica de imposto. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Decreto-Lei n.º 196/2007 de 15 de Maio. Regula as condições técnicas para a emissão, conservação e arquivamento das facturas ou documentos equivalentes emitidos por via electrónica, nos termos do Código do Imposto sobre o Valor Acrescentado, aprovado pelo Decreto-Lei n.º 394-B/84, de 26 de Dezembro.

- Resolução do Conselho de Ministros n.º 137/2005 de 17 de Agosto. Determina, a adopção pela Administração Pública do sistema de facturação electrónica e a preferência pelo recebimento das facturas correspondentes às operações realizadas enquanto adquirente de bens e serviços por via electrónica e incumbe a UMIC de promover o respectivo processo de acompanhamento e avaliação da execução.

- Decreto Regulamentar n.º 16/2000, do DR n.º 228, I Série B de 2 de Outubro. Regula o Decreto-Lei nº375/99, de 18 de Setembro. Estabelece a equiparação entre factura emitida em suporte de papel e a factura electrónica.

- Decreto-Lei n.º375/99, do DR n.º 219, I Série A de 18 de Setembro. Estabelece a equiparação entre a factura emitida em suporte papel e a factura electrónica.

Internet

A regulamentação existente relativa à Internet abrange desde a definição jurídica à disponibilização e submissão por via electrónica de formulários, passando pela referenciação dos sítios da Internet do Estado até à avaliação das páginas da Administração Pública na Internet. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Decreto-Lei n. º 51/2002, do DR n.º 52, I Série A de 2 de Março. Atribui relevância jurídica à disponibilização e submissão por via electrónica dos modelos dos formulários dos organismos e serviços públicos integrados na Administração.

- Resolução do Conselho de Ministros n.º 22/2002, do DR n.º 26, I Série B de 31 de Janeiro. Determina a referenciação dos sítios da Internet do Estado e a publicação de publicidade do Estado em sítios da Internet operados por terceiros.

- Resolução do Conselho de Ministros n.º 22/2001, do DR n.º 49, I Série B de 7 de Fevereiro. Sujeita as páginas na Internet de organismos integrados na administração directa ou indirecta do Estado a uma avaliação periódica. Avaliação das páginas da Administração Pública na Internet.

- Decisão n.º 1720/1999/CE do Parlamento Europeu e do Conselho Europeu de 12 de Julho de 1999. Adopta uma série de acções e medidas destinadas a garantir a interoperabilidade das redes transeuropeias para o intercâmbio electrónico de dados entre administrações (IDA) e o acesso a essas redes. Jornal Oficial das Comunidades Europeias.

Sociedade da Informação

Dentro deste tópico pode-se destacar o Plano de Acção para a Sociedade da Informação que estabelece objectivos e metas ambiciosos, tendo em consideração, por um lado, o impacto estruturante do desenvolvimento da sociedade da informação na competitividade do País e das suas empresas, na modernização da Administração Pública e na qualidade de vida dos portugueses e, por outro, o facto de Portugal ocupar uma posição pouco favorável no contexto europeu, no âmbito dos objectivos estabelecidos nos Planos de Acção *e*Europe 2002 e *e*Europe 2005. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Despacho nº 7908/2010 de 5 de Maio. Extingue a Autoridade de Gestão do POSC – Programa Operacional Sociedade do Conhecimento, passando as respectivas atribuições, direitos e obrigações para o Programa Operacional Factores de Competitividade (POFC) e os bens ao serviço para a UMIC, onde estavam inventariados, com excepção do sistema de informação que contem os elementos necessários à gestão do encerramento do programa, o qual passa também para o POFC.

- Resolução do Conselho de Ministros n.º 190/2005, do DR n.º 240, I Série B de 16 de Dezembro. Aprova o plano tecnológico – uma estratégia de crescimento com base no conhecimento, na tecnologia e na inovação.

- Resolução do Conselho de Ministros n.º 109/2003, do DR n.º 185, I Série B de 12 de Agosto. Implementação da Iniciativa Nacional para a Banda Larga.

- Resolução do Conselho de Ministros n.º 107/2003, do DR n.º 185, I Série B de 12 de Agosto. Aprova o Plano de Acção para a Sociedade da Informação, principal instrumento de coordenação estratégica e operacional das políticas do XV Governo Constitucional para o desenvolvimento da sociedade da informação em Portugal.

- Resolução do Conselho de Ministros n.º 135/2002, do DR nº 268, I Série B de 20 de Novembro. Define o novo enquadramento institucional da actividade do governo em matéria de sociedade da informação, da inovação e do governo electrónico.

- Directiva 2001/29/CE do Parlamento Europeu e do Conselho Europeu, de 22 de Maio de 2001. Relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação. Jornal Oficial das Comunidades Europeias.

- Resolução do Conselho de Ministros n.º 24/2001, do DR n.º 51, I Série B de 1 de Março. Determina a constituição de um sítio na Internet onde sejam publicitados os concursos de pessoal por parte de organismos públicos e de um sítio para a

publicitação de oferta de emprego científico e tecnológico, conferindo mandatos a membros do governo para a respectiva implementação.

- Resolução do Conselho Europeu de 3 de Outubro de 2000. Relativa à organização e à gestão da Internet. Jornal Oficial das Comunidades Europeias.

- Resolução do Conselho de Ministros n.º 110/2000, do DR n.º 193 de 22 de Agosto. Aprova a iniciativa Internet e adopta o respectivo plano de acção.

- Resolução do Conselho de Ministros n.º 95/99, do DR n.º 198, I Série B de 25 de Agosto. Determina a disponibilização na Internet de informação detida pela Administração Pública.

- Resolução do Conselho de Ministros n.º 60/98, do DR n.º 104, I Série B de 6 de Maio. Determina a existência de um endereço de correio electrónico nos serviços e organismos integrados na administração directa ou indirecta do estado e regula o valor atribuído aos documentos que circulam por via electrónica, dando cumprimento ao estabelecido no Livro Verde para a Sociedade da Informação.

Verifica-se a existência de um número considerável de documentos normativos aplicável às TSI e que se reflectem sobre a Administração Pública Portuguesa no seu todo. Por consequência, os Municípios também necessitam de levar na devida consideração aqueles regulamentos e uma vez que as Câmaras Municipais lidam com informação de vários Munícipes, a observância do articulado nos diversos normativos legais constitui um elemento essencial na actuação daquelas entidades.

Do percurso legislativo enunciado resulta a constatação do papel fulcral dos Órgãos da União Europeia, os quais, no âmbito da regulamentação relativa às TSI/SI, têm impulsionado a produção, considerável, de normativos jurídicos de enquadramento e disciplina das mesmas.

3.3.3 Programas de Apoio

As Câmaras Municipais são abrangidas por um conjunto de programas, projectos e iniciativas governamentais no âmbito das tecnologias e sistemas de informação, que permitem um melhoramento destes mecanismos, destacam-se dois programas que seguidamente são apresentados individualmente, designadamente o projecto Cidades e Regiões Digitais e o Plano Tecnológico.

O projecto Cidades e Regiões Digitais, financiado pelo POS-Conhecimento pretende desenvolver a Sociedade de Informação e do Conhecimento ao nível regional de forma a criar competências regionais aplicadas que criem valor económico para a região, aumentem a qualidade de vida dos seus cidadãos e promovam a competitividade das suas empresas e o seu desenvolvimento sustentado.

A dinamização da “Cidade e Regiões Digitais" constitui-se como um veículo único de implementação no território dos Projectos mais emblemáticos na área da Sociedade da Informação e do Conhecimento, permitindo através do compromisso entre a competitividade e a coesão social fazer vir ao de cima as dinâmicas de distinção de qualificação que os actores regionais podem levar a cabo.

Os projectos da iniciativa "Cidades e Regiões Digitais" do Programa Operacional para a Sociedade de Informação (POSI) devem gravitar em torno de quatro vertentes de intervenção [POSI/UMIC 2003]:

1. Dinamização Regional (Conteúdos e Serviços Digitais)

   Esta vertente de intervenção pretende abarcar todo o conjunto de conteúdos e serviços digitais relevantes para os Habitantes, Visitantes, Empresas e demais organismos que constituem as "forças vivas" da região, nas múltiplas vertentes sectoriais, designadamente Educação, Saúde, Cultura, Sociedade, etc.

   O acesso a esta base de conteúdos e serviços deverá ser facilitada através de um Portal Regional agregador, que disponibiliza sob a forma de um directório regional devidamente indexado e categorizado.

2. Governo Electrónico Local em Banda Larga

   A modernização da administração pública é um tema central no desenvolvimento da Sociedade da Informação. Neste contexto de mudança, as tecnologias de informação e comunicação, que inclui em todos os aspectos relacionados com a gestão e o processamento do conhecimento, surgem como os principais elementos facilitadores e aceleradores desta modernização.

   A implementação destas novas tecnologias ao nível das instituições públicas locais deverá, no entanto, ser sempre acompanhada por programas de gestão da mudança e redesenho de procedimentos administrativos para facilitar a sua adopção e difusão em todos os níveis organizacionais. A nova visão integral e transversal baseada nos perfis e nos eventos da vida de um cidadão deu origem a um novo conceito de relacionamento entre a administração pública local e o cidadão. Este conceito tem como objectivo identificar os vários momentos nos quais cada cidadão deve interagir com a administração pública local, que por seu lado deve passar a acompanhar o cidadão de uma forma personalizada e pro-activa ao longo da sua vida.

   Esta vertente deverá estar integrada com a estratégia de Governo Electrónico que define como principal ponto de acesso aos serviços da administração pública, um Portal do Cidadão, desenvolvido a nível central, presentemente a cargo da Unidade Missão Inovação e Conhecimento (UMIC).

3. Acessibilidades

   A realização da "Sociedade da Informação para Todos" passa, em primeiro lugar, pela aposta na generalização do acesso e da utilização das tecnologias de informação e comunicação a todos os portugueses. Neste sentido, os projectos de "Cidades e Regiões Digitais" devem promover o acesso à Internet em Banda Larga através de espaços públicos e a adesão do público em geral à Banda Larga.

4. Infra-estruturas

   A infra-estrutura tecnológica que dará suporte ao portal regional e ao governo electrónico local é um dos componentes básicos da candidatura. No âmbito das

"Cidades e Regiões Digitais", esta infra-estrutura deve ser considerada na perspectiva da sua usabilidade, percepção e utilização efectiva. Outros aspectos complementares relacionados com a gestão da mudança e o nível de qualidade do serviço prestado aos utilizadores devem também ser considerados.

Esta abordagem sócio-técnica é compatível com a filosofia de implementação de serviços "do exterior para o interior das organizações (*edge to core*)", ou seja, o factor mais importante não é a tecnologia ou a estrutura orgânica interna das instituições, mas sim as interacções com a envolvente. Os pontos de contacto com os utilizadores são a origem (e o destino final) do desenho da plataforma tecnológica, os quais determinam também os fluxos de informação e, principalmente, as condições de implementação e exploração dos sistemas de informação.

A "Rede Cidade e Regiões Digitais" é presentemente composta por 28 Projectos [Portal Cidades Digitais 2008]:

- Açores Digital
- Algarve Digital
- Almada Digital
- ALO Digital
- Aveiro Digital
- Beira Baixa Digital
- Beja Digital
- Braga Digital
- Entre Douro e Vouga Digital
- Évora Digital
- Gaia Global
- Leiria Digital
- Litoral Alentejano Digital
- Madeira Digital
- Maia Digital
- Médio Tejo Digital
- Oeste Digital
- Portalegre Digital
- Porto Digital
- Ribatejo Digital
- Seixal Digital
- Setúbal Digital
- Trás-os-Montes Digital
- Vale do Minho Digital
- Vale do Ave Digital
- Vale do Sousa Digital
- Valimar Digital
- Viseu Digital

Cada uma das Cidades Digitais é constituída por um conjunto mais ou menos significativo de instituições locais, sendo as Câmaras Municipais uma das entidades participantes. As Cidades Digitais têm em cada uma das regiões onde estão

implementadas desenvolvido um conjunto de acções e iniciativas com o objectivo de massificar e modernizar a acessibilidade dos cidadãos, empresas e a sociedade em geral ao uso das tecnologias e sistemas de informação e consequentemente tornar a administração pública mais próxima das pessoas.

O XVII e XVIII Governos Constitucionais tinham no seu programa governamental e implementaram o denominado Plano Tecnológico, que inclui também a Administração Pública na sua abrangência.

Segundo o Portal do Governo [2008], as TI são um instrumento fundamental para a reforma dos organismos públicos, contribuindo para uma maior aproximação e melhor relação do cidadão com a administração, o aumento da eficácia dos serviços prestados e a racionalização das ferramentas de gestão pessoal e institucional. No entanto, a generalização das TI terá sempre menor impacto se não for acompanhada por iniciativas que visem a reforma dos próprios processos da administração, reorganizando serviços, promovendo a evolução das atitudes e racionalizando os recursos existentes.

Segundo a informação disponível no Portal do Governo relativamente a este tema, é considerado inegável o esforço feito nos últimos anos visando a modernização da administração pública, conseguindo-se, por exemplo, a ligação à Internet de todos os organismos públicos, o acesso a informação básica dos serviços, a informatização de alguns sectores chave na administração pública, e a interligação e cruzamento de algumas bases de dados. Apesar de muitos destes serviços serem já virados para as reais necessidades dos cidadãos, outros são apenas serviços informativos, sendo relativamente reduzida a interacção com os seus utilizadores.

A procura de serviços públicos por parte dos cidadãos e empresas tem sido cada vez mais exigente, o que tem obrigado a administração pública a uma reorganização e reformulação de processos, de modo a que os serviços disponibilizados satisfaçam, de forma simples e eficaz, as suas necessidades.

Uma administração pública ao serviço dos cidadãos, empresas e de toda a sociedade, implica a utilização do conhecimento como verdadeira alavanca para a competitividade do país. O aumento do número de serviços transaccionais, a possibilidade de aceder aos serviços a qualquer hora, em qualquer lugar e a partir de vários dispositivos, a interligação das diferentes bases de dados existentes de forma a criar um verdadeiro "banco de dados de conhecimento da administração pública" ao serviço dos cidadãos e empresas, a disponibilização de serviços de estímulo à cidadania e à participação dos cidadãos na "causa pública" – são essenciais para a passagem do Governo Electrónico (e-Gov) para o patamar do Governo do Conhecimento (k-Gov) [Portal do Governo 2008].

Neste sentido, apontam-se alguns objectivos propostos pelo Estado que poderão originar impactos significativos na capacidade de inovação, tanto a nível dos cidadãos como das empresas levando à prosperidade da economia [Portal do Governo 2008]:

1 Potenciar o conhecimento existente nos vários organismos da administração pública;

2 Promover a mobilidade de funcionários da administração pública;

3 Reestruturar, concentrar e desmaterializar os processos e actos da administração pública;

4 Simplificar os documentos de identificação do cidadão;

5 Estimular a participação democrática dos cidadãos, promovendo uma maior interacção dos cidadãos com os eleitos e serviços públicos.

No final deste trabalho de investigação foi eleito o XIX Governo Constitucional, que embora com uma conjuntura económica menos favorável pretende "desenvolver um Estado ágil e inovador, adaptado aos desafios da sociedade da informação, que preste serviços de qualidade e individualizados aos cidadãos, segundo novos paradigmas de organização e funcionamento em rede, suportados pelas tecnologias de informação e comunicação" [Portal do Governo 2011].

A execução de projectos locais e regionais de SI, impulsionados pela Administração Central do Estado, estimulou a apetência de cidadãos e Municípios pelo acesso às funcionalidades e vantagens oferecidas pelas TSI, contribuindo para o alargamento da utilização destas ferramentas tecnológicas por parte dos particulares, mas também por parte dos serviços públicos, mesmo em territórios mais distantes dos grandes centros.

O paradigma de relacionamento dos cidadãos com a administração local foi-se progressivamente alterando, na medida em que se tornou possível o acesso a um conjunto de serviços públicos, de forma não presencial, bem como a uma desmaterialização de processos e procedimentos administrativos no seio dos órgãos autárquicos. As novas funcionalidades das TSI permitiram, ainda, um reforço do controlo democrático da actividade autárquica na medida em que facilitaram o acesso a informação administrativa e normativa dos Municípios, facilitaram a divulgação das respectivas actividades e, ainda, permitiram o surgimento de novas formas de participação no processo de formação das decisões administrativas, por parte dos particulares.

3.4 Segurança de Sistemas de Informação nas Câmaras Municipais

Após as secções anteriores, em que se apresentou a caracterização geral das Câmaras Municipais e se apresentaram aspectos da utilização das tecnologias e dos sistemas de informação, esta secção abrange a segurança dos sistemas de informação nessas edilidades, mediante a apresentação de dados resultantes de estudos realizados e com a apresentação da legislação existente sobre esta temática.

3.4.1 Dados de Estudos Realizados

Da pesquisa efectuada verificou-se a ausência de estudos que tivessem visado directamente a temática da SSI. Contudo, encontraram-se referências a alguns aspectos dessa temática. Pretende-se que esta lacuna possa ser mitigada com o trabalho de investigação que agora se propõe.

Abrangência da Estratégia das TIC

A abrangência da estratégia das TIC é evidenciada na Tabela 15, onde se observa e se destaca que em 85% dos inquiridos as políticas de segurança na utilização das TIC são alvo de atenção por parte da estratégia das TIC. Este valor é positivo pois indica que 125

Câmaras Municipais (85% de entre as 60% que têm estratégia para o desenvolvimento das TIC) têm essa estratégia na utilização das TIC.[4]

Abrangência da Estratégia das TIC	(%)
Infra-estrutura das TIC	94
Serviços ao cidadão via Internet	89
Política de segurança na utilização das TIC	85
Formulação e/ou certificação em TIC	50
Compras via Internet	26

Tabela 15: Abrangência da Estratégia das TIC
Fonte: OSIC e UMIC [2006]

Tecnologias de Segurança Utilizadas

Quanto às tecnologias de segurança utilizadas, verifica-se que só por um ponto percentual o uso de anti-vírus não é utilizado em 100% das Câmaras Municipais. O uso de *firewalls* e filtros *anti-spam* merecem também ser destacados pela elevada percentagem de utilização, tal como se constata da Tabela 16.

Tecnologias de Segurança	(%)
Software anti-vírus	99
Firewall	86
Filtros *anti-spam*	66
Servidores seguros (ex: recorrendo a protocolos s-http)	27
Backup de informação numa localização externa à Câmara Municipal	22

Tabela 16: Tecnologias de Segurança
Fonte: OSIC e UMIC [2006]

Problemas de Segurança

Inquiridos sobre se já encontraram problemas de segurança, a resposta foi em termos percentuais dada por 11% das Câmaras Municipais. Quanto ao tipo de problemas de segurança e como se visualiza na Tabela 17, 71% referem-se a ataques de vírus informáticos e em 18% ocorreu acesso não autorizado à rede. Nos casos mencionados a ameaça ou perda de informação está sempre eminente.

Problemas de Segurança Encontrados	(%)
Ataque de vírus informático resultando na perda de informação ou de horas de trabalho	71
Acesso não autorizado à rede de computadores ou a dados do organismo	18
Chantagem ou ameaças aos dados ou ao software do organismo	4

Tabela 17: Problemas de Segurança Encontrados
Fonte: OSIC e UMIC [2006]

[4] No Capítulo seguinte apresentar-se-á um estudo cujos resultados contrapõem outros valores para este montante.

Importará colocar em relevo a escassez de dados relativos à SSI nas Câmaras Municipais, confirmando a pouca atenção que a investigação tem dedicado às políticas de SSI no âmbito do Poder Local, pese embora o reconhecimento operado em torno da sua importância.

3.4.2 Legislação Aplicável à Segurança dos Sistemas de Informação

Após levantamento da regulamentação existente é apresentada nesta subsecção a documentação aplicável à Segurança de Sistemas de Informação, aquela que diz respeito directamente a esta temática e outras que indirectamente condicionam também a segurança dos Sistemas de Informação. A legislação é apresentada em diferentes tópicos conforme o seu enquadramento em: Criminalidade Informática, Protecção de Dados Pessoais, Segurança em Redes e Segurança Informática. Seguidamente são apresentados os principais regulamentos constituintes de cada uma das vertentes.

Criminalidade Informática

No âmbito da Criminalidade Informática existe uma Recomendação do Conselho Europeu que recomenda que os Estados-Membros garantam que a unidade investida como ponto de contacto naquela matéria mantenha um serviço de 24 horas por dia e que essa unidade seja realmente um organismo especializado que aplique as boas práticas estabelecidas de investigação de crimes relacionados com as TI. Para além disso, a unidade referida também deverá estar apta a tomar medidas operacionais. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Lei n.º 109/09 de 15 de Setembro. Relativa a ataques contra sistemas de informação, e o direito interno à Convenção sobre Cibercrime do Conselho da Europa.
- Proposta de Decisão – Quadro do Conselho relativa a ataques contra os sistemas de informação/*COM/2002/0173final-CNS2002/0086*/.
- Recomendação do Conselho Europeu de 25 de Junho de 2001 – Relativo a um serviço de 24 horas por dia de combate ao crime de alta tecnologia. Jornal Oficial das Comunidades Europeias.

Protecção de Dados Pessoais

O tópico Protecção de Dados Pessoais tem uma série de regulamentação adjacente que aborda em concreto a protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Outro tema abordado é a protecção da privacidade no sector das telecomunicações. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Lei n.º 41/04 de 18 de Agosto. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Transpõe para

a ordem jurídica nacional a Directiva n.o 2002/58/CE,do Parlamento Europeu e do Conselho, de 12 de Julho).

- Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho Europeu, de 18 de Dezembro de 2000. Relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias.

- Lei n.º 69/98 de 28 de Outubro. Regula o tratamento dos dados pessoais e a protecção da privacidade no sector das telecomunicações (transpõe a Directiva 97/66/CE, do parlamento Europeu e do Conselho, de 15 de Dezembro de 1997).

- Lei n.º 67/98 de 26 de Outubro. Lei da protecção de dados pessoais (transpõe para a ordem jurídica Portuguesa a Directiva nº45/46/CE, do Parlamento Europeu e do Conselho Europeu, de 24 de Outubro de 1995 relativa à protecção de pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados).

- Resolução da Assembleia da República n.º 53/94, do DR n.º 191, I Série A de 12 de Agosto. Regulamento da Comissão Nacional da Protecção de Dados Pessoais Informatizados.

- Lei n.º 109/91 de 17 de Agosto (Lei da criminalidade informática) – Protecção de dados pessoais.

<u>Segurança de Redes</u>

Dentro da temática da Segurança de Redes destaca-se o Regulamento do Parlamento Europeu e do Conselho que cria a Agência Europeia para a Segurança das Redes e da Informação, a fim de garantir na Comunidade um nível de segurança das redes e da informação elevado e eficaz e com vista a desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das organizações do sector público da União Europeia, contribuindo assim para o normal funcionamento do mercado interno. Dentro deste tópico pode-se referenciar a seguinte regulamentação e parecer:

- Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho Europeu de 10 de Março de 2004. Cria a Agência Europeia para a Segurança das Redes e da Informação. Jornal Oficial da União Europeia.

- Lei n.º 5/04, do DR n.º 34, I Série A de 10 de Fevereiro. Estabelece o regime jurídico aplicável à redes e serviços de comunicação electrónicas e aos recursos e serviços conexos e define as competências da autoridade reguladora nacional neste domínio.

- Parecer do Comité Económico e Social sobre a "Comunicação da Comissão ao Conselho, Parlamento Europeu, Comité económico e Social e Comité das Regiões – Segurança das redes e da informação: proposta de abordagem de uma política Europeia" (2002/C 48/07). Jornal Oficial das Comunidades Europeias.

- Resolução do Conselho Europeu de 28 de Janeiro de 2002. Sobre uma abordagem comum e acções específicas no domínio da segurança das redes e da informação. Jornal Oficial das Comunidades Europeias.

Segurança Informática

A segurança dos sistemas informáticos é regulamentada pela Resolução do Conselho de Ministros que estabelece normas para a segurança nacional, salvaguarda e defesa das matérias classificadas e segurança informática. A diversidade e evolução dos equipamentos e programas dos sistemas informáticos não se coadunam com o estabelecimento de normas rígidas que prevejam todas as situações pelo que foram estabelecidas um conjunto de regras suficientemente flexível, de forma a deixar à Autoridade Nacional de Segurança a possibilidade de, caso a caso, apreciar a oportunidade das medidas a aplicar. Dentro deste tópico pode-se referenciar a seguinte regulamentação:

- Decreto-Lei n.º 176/07 de 08 de Maio. Primeira alteração à Lei n.º 5/2004, de 10 de Fevereiro (Lei das Comunicações Electrónicas), estabelecendo o regime sancionatório da aquisição, propriedade e utilização de dispositivos ilícitos para fins privados no domínio de comunicações electrónicas.

- Resolução do Conselho de Ministros n.º 5/90, do DR n.º 49, I Série de 28 de Fevereiro. Normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança informática.

- SEGNAC’s 1,2,3 e 4. As normas compiladas em quatro distintos volumes respeitantes a quatro áreas específicas são conhecidas pela designação SEGNAC's.1,2,3 e 4 sendo que o SEGNAC 1 aborda as regras relativas a Matérias Classificadas, o SEGNAC 2 a Segurança Industrial, o SEGNAC 3 Segurança das Comunicações e o SEGNAC 4 a Segurança Informática.

Tal como anteriormente, verifica-se a existência de um leque de documentos normativos aplicável à SSI ao qual a Administração Pública Portuguesa como um todo, e os Municípios em particular, têm de devotar a devida atenção. Instanciando os normativos legais para as áreas de actuação das Câmaras Municipais, observa-se a necessidade destas entidades adoptarem e aplicarem os mecanismos de segurança decorrentes daqueles normativos com vista à promoção da segurança da informação respeitante quer aos seus funcionários e quer aos seus Munícipes.

3.5 Conclusão

Nas três décadas em que o País vive em regime democrático assistiu-se ao florescimento e afirmação de um poder Autárquico consolidado que pauta a sua acção pela lógica da proximidade da Administração com os administrados. Tal facto, aliado a uma forte tradição comunitária, ajudará a explicar a existência actual de 308 Municípios.

A quantidade de municípios existente pode ser categorizada pela sua dimensão em Municípios muito grandes, grandes, médios e pequenos. Esta divisão é feita em função do número de eleitores por Município.

Em termos de tecnologias e sistemas de informação verifica-se uma grande adesão das Câmaras Municipais, nomeadamente em termos de ligação à Internet e da presença com *websites* neste meio de comunicação.

Verifica-se a existência de variada regulamentação aplicável às Tecnologias e Sistemas de Informação e à Segurança dos Sistemas de Informação, abrangendo tópicos como: Acessibilidades, Aquisição de bens e serviços, Assinatura digital, Correio e Comercio Electrónico, Comunicações Electrónicas, Conteúdos Digitais, Facturação electrónica e Internet, Sociedade da Informação, Criminalidade Informática, Protecção de Dados Pessoais, Segurança de Redes e Segurança Informática. A regulamentação é feita de várias formas destacando-se as Resoluções do Conselho de Ministros, Directivas do Parlamento Europeu, Leis, Regulamentos do Parlamento Europeu e do Conselho Europeu, Recomendações, Decretos-Lei e Decretos Regulamentares. Esta regulamentação é em número considerável proveniente da União Europeia, o que reflecte as preocupações em regulamentar estas áreas por parte daquela entidade.

Sob o ponto de vista orçamental verifica-se um acréscimo em termos de investimento no que diz respeito à aquisição de hardware e software. No que diz respeito à Segurança de Sistemas de Informação, os estudos são praticamente inexistentes e abordam sempre de forma muito superficial a temática da SSI, não se conhecendo dados concretos e quantitativos que permitam ter uma visão e entendimento consolidados sobre segurança dos sistemas de informação na Administração Pública Local em Portugal.

Capítulo 4

Levantamento sobre Políticas de SSI nas Câmaras Municipais em Portugal

4.1 Introdução

No capítulo anterior caracterizaram-se as Câmaras Municipais Portuguesas segundo um conjunto de perspectivas que se julgaram pertinentes para este estudo. No presente capítulo, que precede a apresentação da abordagem de investigação que se aplicou neste trabalho, apresenta-se o levantamento realizado sobre políticas de SSI nas Câmaras Municipais em Portugal.

No decurso da redacção deste trabalho de investigação e previamente à definição dos métodos e técnicas de investigação a utilizar para a prossecução do estudo, surge como dificuldade primeira o desconhecimento e ausência de qualquer trabalho de investigação precursores da demonstração da realidade das Câmaras Municipais Portuguesas no que tange à adopção de políticas de SSI.

Tendo por finalidade constituir uma base de reflexão acerca das opções de investigação a desenvolver em torno da temática da "Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal", foi realizado um inquérito à totalidade das Câmaras Municipais Portuguesas.

O presente capítulo tem por objectivo a explanação dos resultados obtidos com o levantamento sobre políticas de SSI nas Câmaras Municipais em Portugal, bem como a afirmação do percurso investigatório empreendido, designadamente o planeamento e estrutura do inquérito que consubstanciou o levantamento e o relato das dificuldades e obstáculos encontrados, ao que acresce a referência a outros elementos e aspectos tidos por pertinentes para a concretização do presente estudo.

4.2 Inquérito

4.2.1 Planeamento

Atentando-se na dificuldade encontrada, e observada a inexistência de estudos neste domínio, promoveu-se a realização de um levantamento junto das Câmaras Municipais através de um inquérito que compreendeu um conjunto de questões conexas com políticas de SSI, indagando-se através de contactos directos, junto dos serviços das 308 edilidades municipais Portuguesas.

Assim, o principal objectivo do levantamento foi a obtenção de resposta à seguinte questão:

> As Câmaras Municipais Portuguesas têm implementadas políticas de SSI?

O levantamento corporizou-se num inquérito para aferir a realidade das Câmaras Municipais em matéria de segurança dos seus sistemas de informação e quantificar as que realmente têm políticas de segurança (incluindo-se neste conceito as políticas de privacidade) de sistemas de informação.

Laborando em torno da problemática das políticas de SSI, assumiu importância crucial a adopção de uma definição de política de SSI susceptível de transmissão e apreensão por parte dos inquiridos. Assim, e tendo em vista a estabilização de conceitos base, para uma resposta objectiva por parte de todos os inquiridos, optou-se pela adopção da definição preconizada por de Sá-Soares [2005, p. 56], que compreende as políticas de SSI como "documentos que orientam ou regulam as acções das pessoas ou sistemas no domínio da SSI".

Para a execução do inquérito consideraram-se três meios de concretização possíveis: o correio tradicional (suporte físico em papel), correio electrónico ou contacto telefónico. Procurando-se alcançar o maior número de respostas possíveis, no mais curto espaço de tempo, com um grau de fiabilidade elevado, aliada à circunstância de a extensão do questionário não implicar um elevado dispêndio de tempo, optou-se prioritariamente pelo contacto telefónico, sem prejuízo de os inquiridos que assim o desejassem poderem responder através de correio electrónico ou mesmo via correio tradicional.

O desenvolvimento do levantamento compreendeu quatro fases distintas:

1. Identificação dos objectivos e público-alvo;
2. Concepção e desenvolvimento do questionário;
3. Planeamento e logística dos meios necessários para a sua realização;
4. Interpretação dos resultados e elaboração do presente capítulo.

4.2.2 Estrutura

A estrutura do inquérito resultou directa e necessariamente da associação da revisão de literatura, subordinada à temática das políticas de SSI, efectuada no âmbito deste trabalho, e do próprio objectivo do levantamento.

Assim, foram formuladas as questões do inquérito, de resposta individual e de natureza confidencial, tendo sido organizadas em três quadros, conforme se ilustra no Apêndice F. As questões do inquérito surgem após uma breve caracterização da Câmara Municipal e do inquirido, seguindo-se as questões atinentes às características gerais de políticas de SSI, as quais são antecedidas pela questão fundamental: "A Câmara possui uma política de SSI?".

Após a pergunta principal, e caso a resposta fosse negativa, passava-se para o Quadro 3, onde se questionava os inquiridos se estavam a pensar formular uma política de segurança ou não, uma vez que ainda não possuíam nenhuma, e caso

estivessem a pensar formular alguma, se já estava ou não em processo de elaboração. Se não estivessem a pensar formular uma política de segurança, eram questionados se essa opção seria por não considerarem a segurança da informação importante. Uma última questão formulada aos inquiridos relacionava-se com a existência ou não de outros mecanismos de protecção da informação e sua descrição.

Caso a resposta à questão principal fosse positiva, passava-se aos Quadros 1 e 2, que se diferenciam pelo facto do Quadro 1 focar as políticas de segurança enquanto produto e pelo Quadro 2 se centrar nos processos de formulação, implementação e revisão das políticas de segurança de sistemas de informação.

Relativamente às políticas enquanto produto, as questões colocadas foram: a forma como é apresentada (escrita ou verbal); o que aborda; a sua dimensão (em número de páginas); quem tem conhecimento da política; onde se encontra disponível; se estão definidos os papéis, as responsabilidades e as sanções para o não cumprimento da política e se os utilizadores assinaram um termo de aceitação da política.

Em relação aos processos, ou seja, no que concerne à formulação, implementação e revisão das políticas, as questões colocadas relacionavam-se com o tempo de vida das políticas, por quem foi desencadeado o processo de formulação, por quem foi desenvolvida, se foi aprovada superiormente, quem a implementou e quem supervisiona o seu cumprimento, se foi bem aceite pelos utilizadores, se está em vigor, se é revista, se existe uma única política ou várias, e a quem se destina.

Estas questões, consideradas paralelamente à questão principal, permitiam em certa medida verificar se os inquiridos responderam validamente à primeira questão, uma vez que ter uma política de segurança é por vezes entendido por se dispor de anti-vírus ou *firewall* o que, de acordo com o entendimento adoptado neste trabalho, não configura uma política de segurança.

4.3 População

O presente estudo tem por âmbito a Administração Pública Local em Portugal. A divisão territorial em Portugal é feita através de distritos e de regiões autónomas, sendo o número de distritos dezoito e as regiões autónomas duas (os Açores e a Madeira). Em relação aos municípios, o território está dividido em 308 entidades.

A realização do inquérito compreendeu a inquirição das 308 Câmaras Municipais existentes no país, compreendendo, assim, as 278 sitas no território continental, as 11 compreendidas na jurisdição da Região Autónoma da Madeira e as 19 compreendidas no território da Região Autónoma dos Açores. O levantamento configurou, assim, um censo sobre políticas de SSI na Administração Pública Local em Portugal.

Os dados foram recolhidos através de um inquérito, efectuado aos responsáveis da informática das Câmaras Municipais, no período de 15 de Novembro a 6 de Dezembro de 2007.

Das 308 Câmaras Municipais, que constituíam o alvo do levantamento, obtiveram-se respostas das 308 edilidades, o que corresponde a uma taxa de resposta de 100%.

4.4 Condução do Estudo

4.4.1 Ajustamentos ao Estudo Planeado

A execução do inquérito não envolveu a realização prévia de testes exaustivos, tendo-se, no entanto, procurado aferir, durante a realização dos cinco primeiros contactos telefónicos, acerca da inteligibilidade das questões propostas e da apropriação da interpelação efectuada aos inquiridos.

Assim, não mereceram reparo ou ajustamento de linguagem ou formulação as questões propostas no inquérito, não obstante foi objecto de ajuste a introdução realizada. Efectivamente, sem prescindir das necessárias referências à identificação da autora, do objectivo e universo do inquérito, bem como à sua natureza confidencial e tratamento agregado de dados, o tempo dispendido para o efeito mereceu substancial redução.

A redução do tempo de inquérito referente à introdução e apresentação do inquérito resultou da crítica e resistência que o mesmo mereceu junto dos inquiridos e que poderia importar para a realização do trabalho dificuldades e obstáculos acrescidos e indesejáveis.

4.4.2 Dificuldades e Particularidades

No que respeita às dificuldades experimentadas ao longo do levantamento, não se pode deixar de mencionar a frequente confusão dos inquiridos que reiteradamente associavam políticas de segurança à reserva e discrição de funcionários ou mesmo à confidencialidade do conteúdo de bases de dados. Apenas a insistência e a repetição da explicação do que se pretendia com a realização do inquérito permitiu vencer e ultrapassar as resistências dos inquiridos. Outra dificuldade que se pode mencionar é o tempo de espera até falar com a pessoa responsável pelo sector da informática, por vezes a chamada passava de pessoa em pessoa até chegar ao Director. A falta de disponibilidade naquele momento, uma vez que o primeiro contacto foi sempre realizado via telefone, era constante, só com muita persistência se conseguiu ultrapassar este obstáculo.

Porém, é também da mais elementar justiça o reconhecimento da disponibilidade e abertura de alguns serviços de Câmaras Municipais na divulgação e explicação das suas políticas de segurança de sistemas de informação, que com grande abertura e espírito de colaboração, além dos esclarecimentos prestados, remeteram à autora a base normativa de tais políticas.

Sem prejuízo do que já anteriormente se referiu quanto à importância da opção conceptual de política de SSI, designadamente para a compreensão do inquérito que esteve na base do levantamento realizado, constata-se um claro desconhecimento dos inquiridos do conceito e respectivo preenchimento substantivo. Assim, foi com

grande dificuldade que os inquiridos associaram a política de segurança de sistemas de informação ao conjunto de normas que estabelecem o regime de utilização dos aludidos sistemas. Para tanto poderá contribuir a enorme profusão de "roupagens" formais de tais normas e regras de procedimento, em virtude das mesmas se acharem vertidas em regulamentos internos, normas, despachos e até mesmo sob a forma de avisos no espaço de trabalho.

Constatou-se, ainda, que apesar do grande número de Câmaras Municipais que não possuem uma política de segurança de sistemas de informação, na verdade muitas foram aquelas que em resposta ao inquérito afirmaram ponderar a formulação de uma política de segurança de sistemas de informação. Tal facto ficar-se-á a dever à necessidade que actualmente surge de certificação de serviços, no âmbito da certificação da qualidade (ISO 9001), que inclui também a certificação do Departamento de Informática e consequente elaboração de políticas de segurança.

A adesão a projectos de redes de cidades digitais, por parte das Câmaras Municipais, facto que se verifica em alguns Distritos, está também a levar à ponderação e elaboração conjunta de políticas de segurança e outros mecanismos de protecção dos sistemas de informação, para os Municípios pertencentes a essa rede digital.

4.5 Resultados

4.5.1 Caracterização do Levantamento

A caracterização do levantamento é apresentada de uma forma sintética, mas abrangendo todos os itens considerados necessários para a mesma, no quadro seguinte:

Universo de Referência:	Câmaras Municipais (308)
Âmbito geográfico:	Continente e Regiões Autónomas
Realização do trabalho de campo:	15 de Novembro a 6 de Dezembro de 2007
Técnica de recolha de informação:	Inquérito Via Correio Electrónico - 9 Via Contacto Telefónico - 299
Número de respostas obtidas:	308
Taxa de resposta:	100%
Âmbito do estudo:	Doutoramento em Sistemas de Informação

4.5.2 Caracterização dos Respondentes

O perfil dos respondentes ao inquérito pode ser diferenciado em termos da categoria profissional que ocupam na Câmara Municipal e anos de serviço em que estão no cargo.

Relativamente aos cargos, e tal como se observa no Gráfico 4, 167 dos inquiridos são técnicos superiores de informática, seguindo-se os especialistas de informática, coordenadores, chefes de divisão (informática, administrativa e financeira),

administradores de sistemas, vereadores responsáveis pela informática, administrativos e outros (chefe de gabinete, economista, adjunto do presidente, engenheiro civil, director de departamento e consultor informático). Embora as categorias sejam diferentes é de destacar que se tratam dos responsáveis pela informática na autarquia, e que foi sempre com essa premissa que se norteou a condução do levantamento.

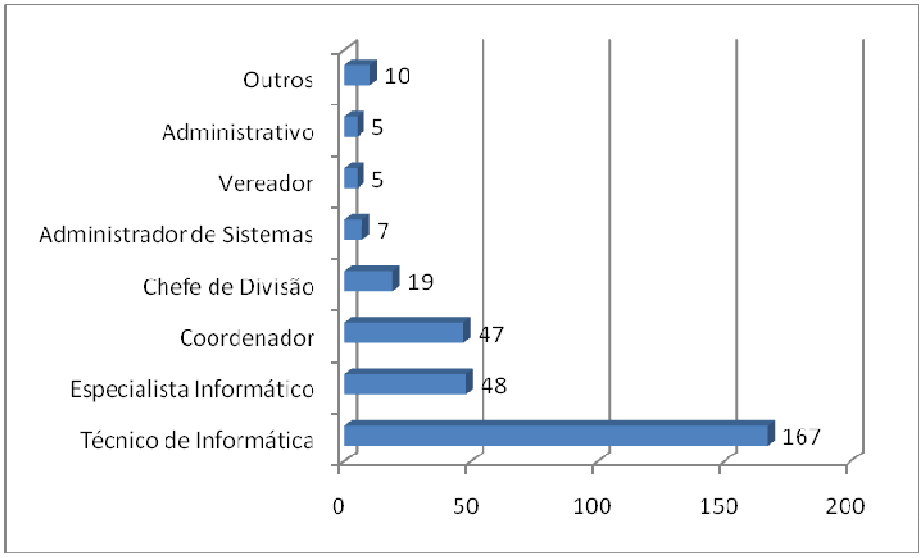


Gráfico 4: Categoria Profissional dos Inquiridos

O número de anos de serviço que os inquiridos possuem nesse cargo pode ser observado no Gráfico 5 (sublinha-se que os valores não são dos anos de serviço que os inquiridos estão na Câmara Municipal, mas sim na categoria que ocupam à altura do levantamento). Destaca-se que 36% (111) dos inquiridos está naquela categoria profissional há 6 a 10 anos, 23% (70) estão nessa categoria há 2 a 5 anos, seguindo-se 14% (44) que só estão nessa categoria há menos de 2 anos, por seu lado 13 % (39) dos inquiridos estão nessa categoria há 11 a 15 anos.

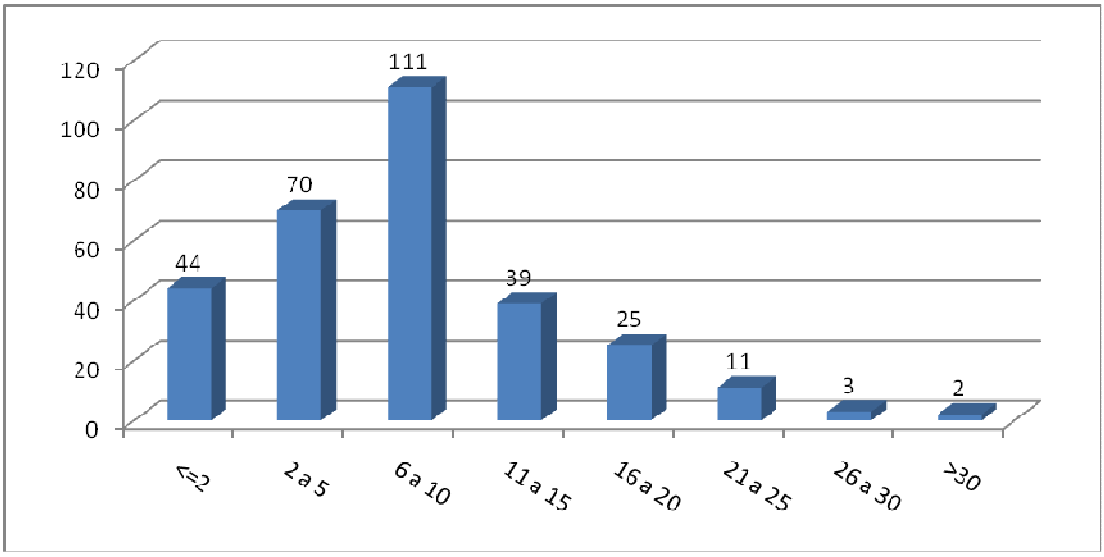


Gráfico 5: Anos de Serviço dos Inquiridos

Note-se que existem três Câmaras que não estão mencionadas no que diz respeito aos anos de serviço, porque os inquiridos que eram os responsáveis pela informática não eram funcionários da Câmara, sendo um deles destacado e os restantes dois trabalharem por avença.

4.5.3 Análise das Respostas

Nesta subsecção serão analisadas as respostas obtidas em cada questão do inquérito. Essa análise resulta do agrupamento de todos os dados e posterior ponderação conjunta. Por vezes e sempre que se entende como conveniente e esclarecedor, os dados são apresentados por Distrito. Por compromissos de anonimato não se apresentarão dados por Concelho.

Posse de Política de SSI

A questão principal do inquérito, como já foi referido neste capítulo, prende-se com a existência de políticas de SSI nas Câmaras Municipais em Portugal. Dada a sua importância e pelo facto de ser a base para as restantes questões, a posse de uma política foi a primeira pergunta formulada. As respostas obtidas encontram-se no Gráfico 6.

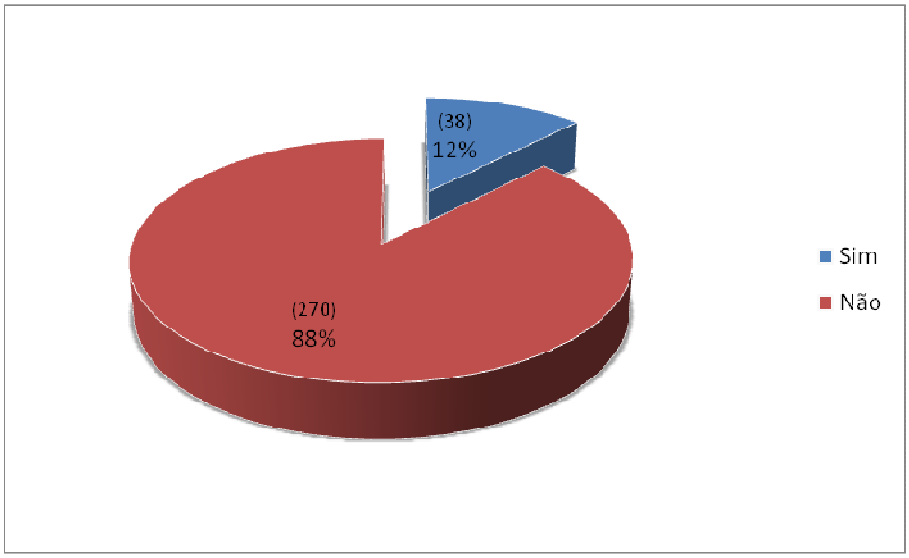


Gráfico 6: Posse de uma Política de Segurança

Como se observa no gráfico anterior, 12% das Câmaras Municipais indicaram possuir políticas de SSI, ou seja, das 308 Câmaras Municipais, 38 (12%) informaram dispor de políticas de segurança e 270 (88%) não têm ou ainda estão a formular uma política para posterior implementação. Esta constatação é apresentada no Gráfico 7, com a distribuição por Distrito.

Outra leitura que se pode apresentar é a sua distribuição por dimensão eleitoral da respectiva Câmara Municipal. O Gráfico 8 apresenta essa distribuição. Das 38 Câmaras com políticas de SSI, 20 (52,6%) são da Classe C (Autarquias Médias), 9 (23,7%) são da Classe D (Autarquias Pequenas), 6 (15,8%) pertencem à Classe B (Autarquias Grandes) e 3 (7,9%) à Classe A (Autarquias Muitos Grandes). Estas

percentagens devem ser cruzadas com o número de Câmaras que compõem cada uma daquelas quatro classes. Assim no cômputo geral constata-se que das 20 Câmaras pertencentes à Classe A, 3 possuem política de segurança o que corresponde a 15% dessa classe. Das 21 Câmaras da Classe B, 6 possuem uma política de segurança o que corresponde a 29% dessa classe. Das 150 Câmaras da Classe C, 20 possuem uma política de segurança o que corresponde a 13% dessa classe. Das 117 Câmaras da Classe D, 9 possuem uma política de segurança o que corresponde a 8% das Câmaras incluídas nessa classe.

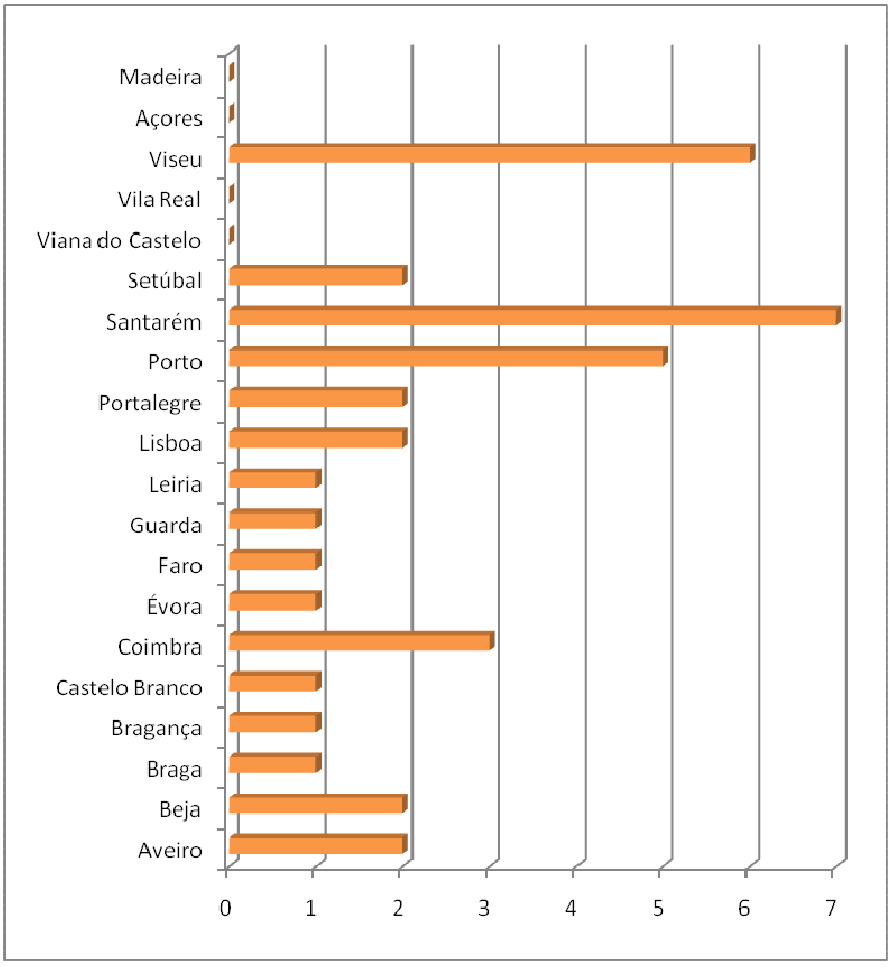


Gráfico 7: Posse de Políticas de Segurança por Distrito

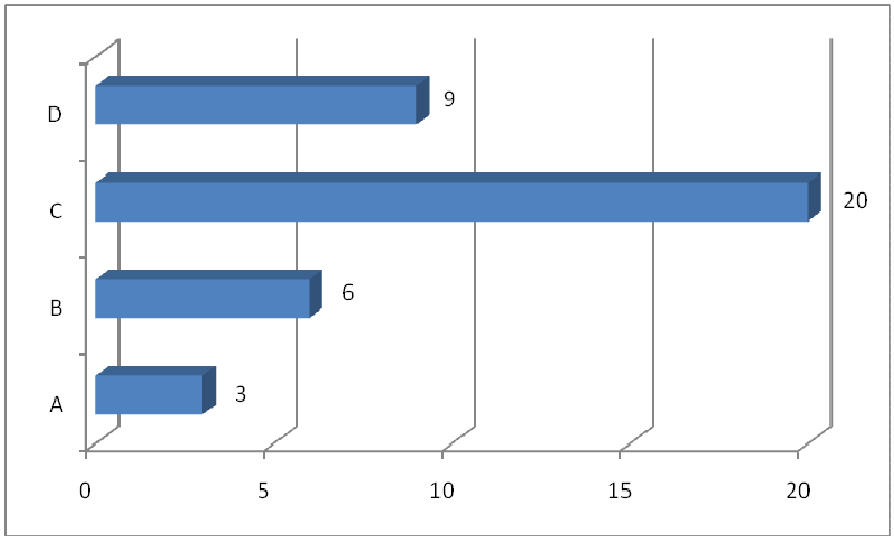


Gráfico 8: Posse de uma Política por Dimensão da Autarquia

Política como Documento Escrito

Esta questão é a primeira do Quadro 1 do inquérito, que aborda aspectos das políticas enquanto produto. As respostas obtidas que indicavam que as políticas de SSI são um documento escrito foram 38, número coincidente com o total de políticas de segurança existente nas Câmaras Municipais. Obtiveram-se seis respostas relativas a Câmaras que responderam afirmativamente à questão da existência de uma política, mas que responderam seguidamente que o documento não era escrito. Destas, quatro disseram ter políticas verbais e duas terem software e hardware. Dada a definição de política de SSI da qual tiveram conhecimento, considerou-se que estas seis respostas não configuravam uma verdadeira política de segurança, pelo que foram retiradas do número total de políticas existentes (cf. esta decisão no Gráfico 9).

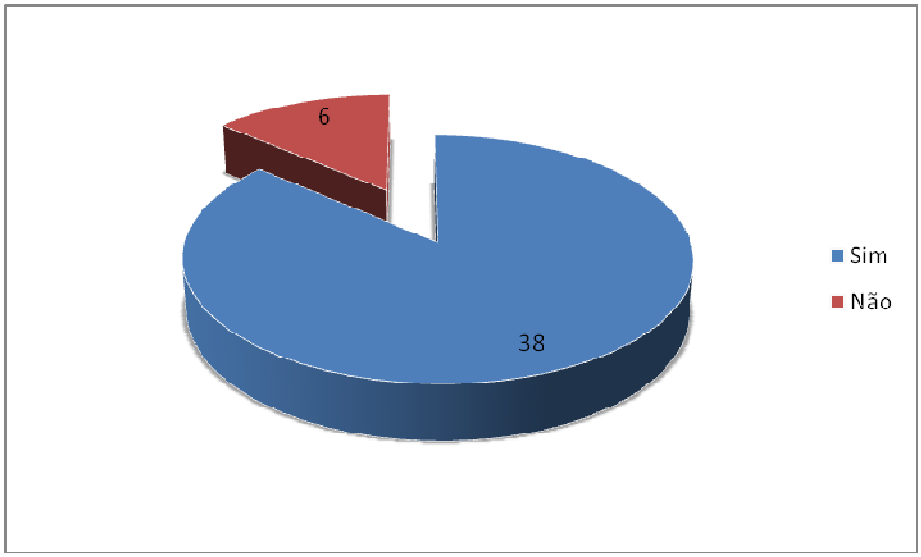


Gráfico 9: Política como Documento Escrito

Temas Abordados pelas Políticas

Dentro do universo das 38 respostas afirmativas, o conteúdo das políticas de segurança aborda: tecnologias (30), comportamentos[5] (38) e outros (3). Tratando-se de uma questão com possibilidade de escolha múltipla o total não tem que somar 38. O agrupamento dos dados é apresentado no Gráfico 10. Relativamente ao ponto "outros", as três respostas que o mencionaram dizem respeito a políticas de segurança que se encontram dentro de um regulamento interno mais abrangente e que podem abordar, a título de exemplo, as instalações onde se encontra o equipamento.

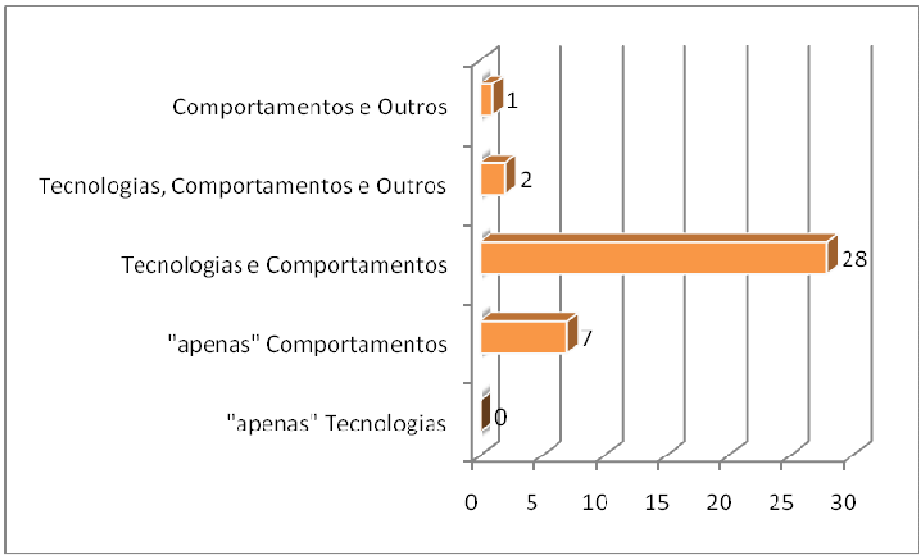


Gráfico 10: Temas Abordados pelas Políticas

Dimensão do Documento da Política

A dimensão das políticas, em termos de número de páginas, varia muito no universo das 38 Câmaras, sendo a média de oito páginas por documento, com o máximo de 30 páginas e o mínimo de uma página, como se pode observar no Gráfico 11.

Conhecimento da Política

Questionados sobre quem tem conhecimento da política, as respostas foram iguais nos 38 casos: as políticas são do conhecimento do Executivo Municipal, das Chefias e dos Funcionários. A opção Munícipes não obteve qualquer resposta. Por norma, as políticas são aprovadas pelo executivo ou por um dos seus elementos, posteriormente essas orientações são comunicadas às chefias de cada departamento que as fazem chegar a todos os funcionários que utilizam os sistemas e tecnologias de informação da Câmara Municipal.

[5] Por 'comportamentos' entende-se o modo de actuação dos funcionários, ou seja, as suas acções concretas.

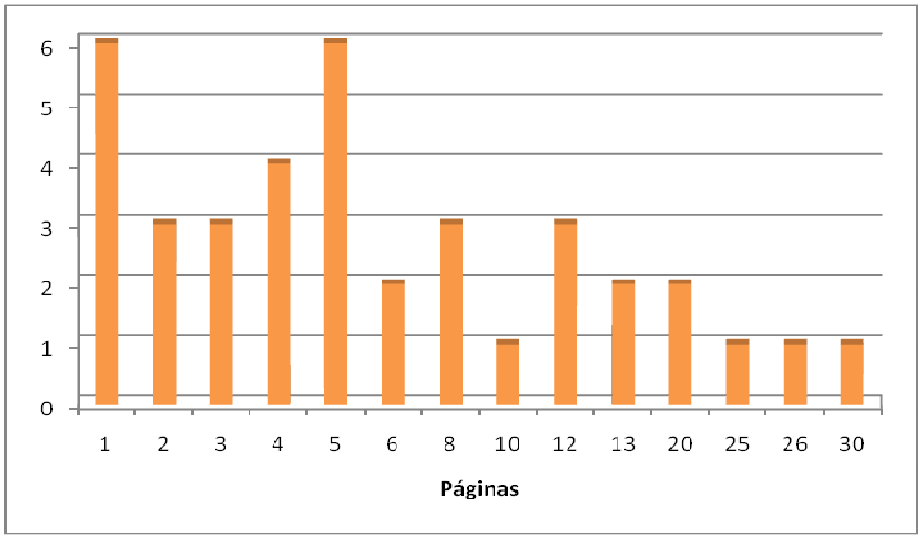


Gráfico 11: Dimensão do Documento da Política

Meio de Disponibilização da Política

Das 38 respostas, 34 têm a política de segurança em documento disponível internamente (*email*, *intranet* ou papel), quatro em documento interno reservado (no departamento de informática) e como a questão é de escolha múltipla uma Câmara Municipal respondeu que o documento estava disponível internamente (via correio electrónico) e em documento disponível ao público (no *website* da Câmara Municipal). Os dados recolhidos encontram-se resumidos no Gráfico 12.

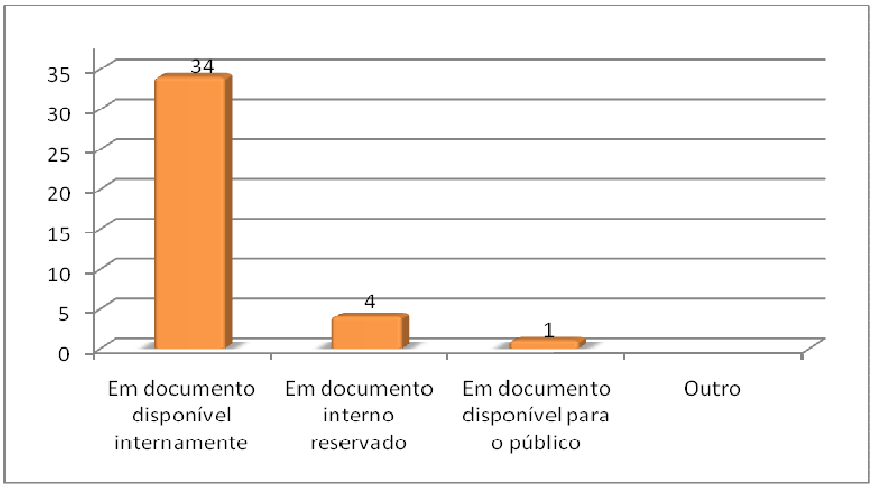


Gráfico 12: Meio de Disponibilização da Política

Definição de Papéis e Responsabilidades na Política

Das 38 Câmaras, em 92% (35) as políticas têm definidos os papéis e as responsabilidades dos utilizadores, em 8% (3) essa definição não está feita. Estes valores e respectivas percentagens estão representados no Gráfico 13.

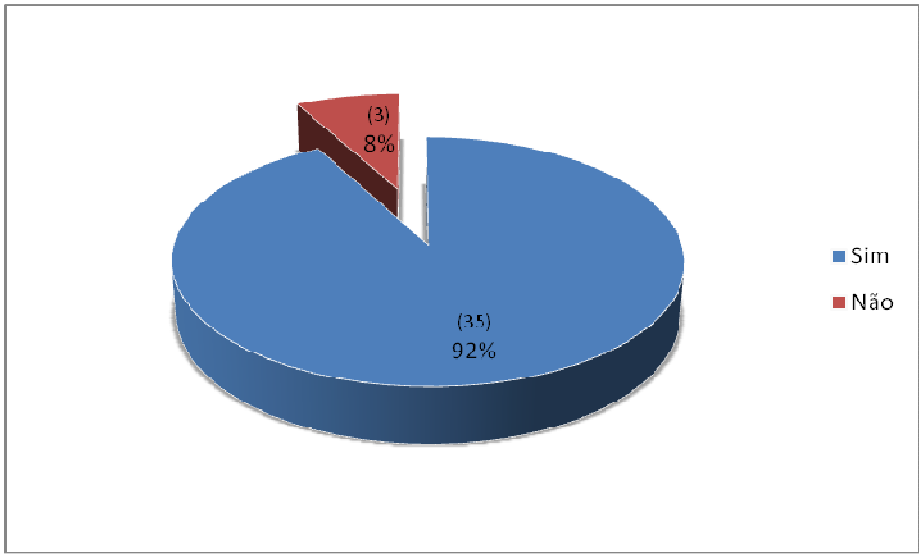


Gráfico 13: Definição de Papéis e Responsabilidades na Política

Definição de Sanções na Política

Questionados sobre a definição de sanções para o não cumprimento da política, 63% (24) não têm essa definição na política. Os inquiridos justificaram esta ausência pelo facto de se regerem pela lei da função pública e os funcionários poderem ser alvo de processo disciplinar independentemente de estar ou não alguma sanção definida na política, embora compreendam que as sanções possam ser de outro nível. Um número inferior – 37% (14) – tem essa definição no próprio documento (Ver Gráfico 14).

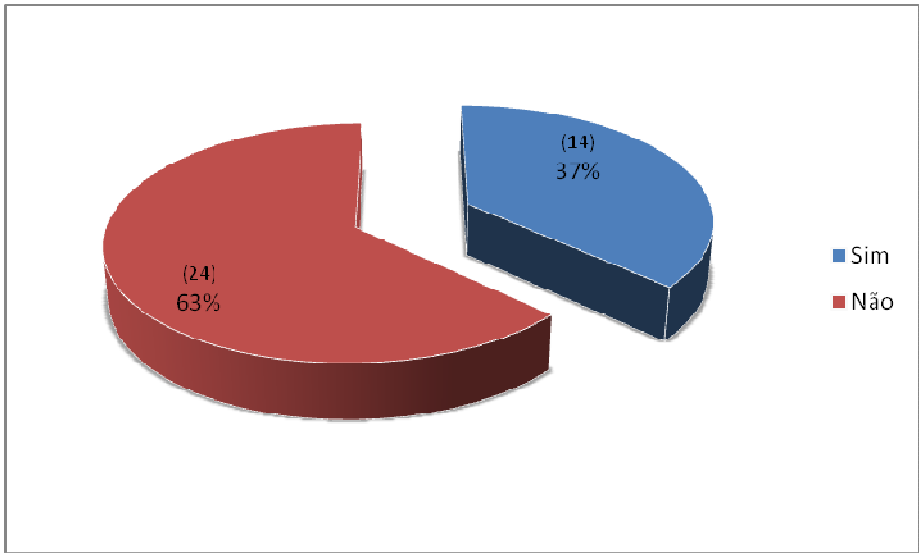


Gráfico 14: Definição de Sanções na Política

Termo de Aceitação da Política

Relativamente à questão de os utilizadores assinarem ou não um termo de aceitação da política de SSI, nas situações de comunicação da política ou de revisão da mesma, 45% (17) responderam positivamente e os restantes 55% (21) negativamente. Normalmente, a comunicação é feita da seguinte forma: o documento é entregue às chefias de cada departamento ou o documento circula via

intranet e neste caso os utilizadores não assinam qualquer termo de aceitação. O Gráfico 15 ilustra estes dados.

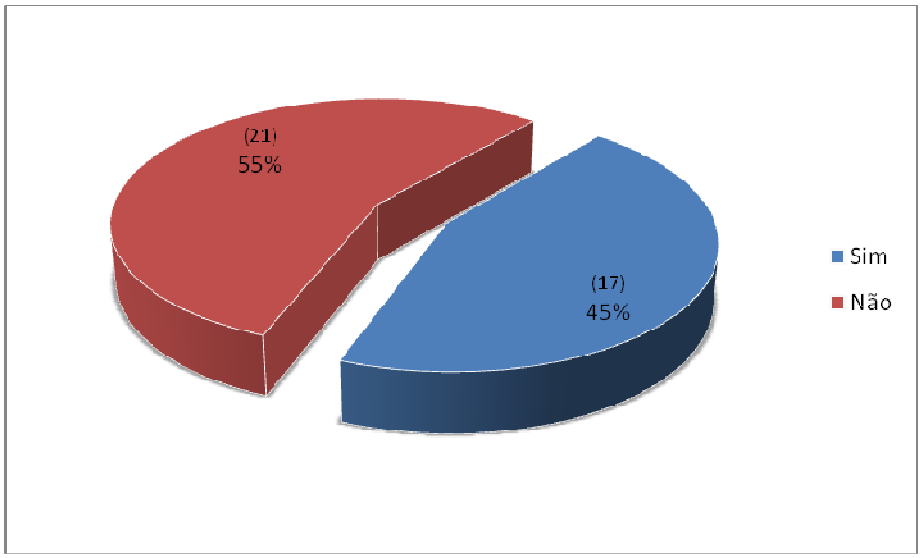


Gráfico 15: Termo de Aceitação da Política

Anos de Existência da Política

Esta questão inicia o Quadro 2 do inquérito, que aborda os processos conexos às políticas. Questionados sobre há quantos anos foi elaborada a política de SSI, a média das respostas obtidas situa-se em três anos, a política mais antiga foi elaborada há 15 anos e a mais recente há um ano.

Face à exactidão das respostas a esta questão, com alguns inquiridos a indicarem o tempo de existência das políticas em meses, optou-se por tratar os dados de forma aproximada, tendo-se arredondado a idade das políticas para números inteiros, ou seja, para anos, apresentando-se os resultados no Gráfico 16.

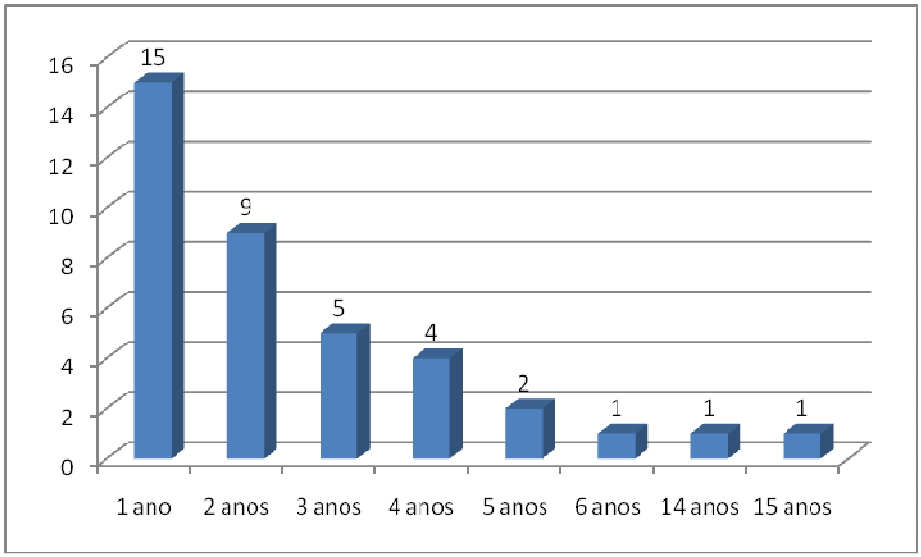


Gráfico 16: Anos de Existência da Política

Uma vez que a média dos anos de existência das políticas de SSI é de três anos, o que se traduz num número relativamente baixo, conclui-se que há três anos só nove Câmaras tinham políticas de segurança.

Destaca-se neste gráfico a quantidade de políticas elaboradas no último ano, sendo esse número de 15. Este despertar para a formulação das políticas com base nas respostas dadas pelos inquiridos deve-se em grande parte a imperativos legais impostos, nomeadamente pela certificação da qualidade dos serviços.

Quem Desencadeou o Processo de Formulação

A resposta a esta questão foi unânime: nos 38 casos o departamento/divisão/sector de informática esteve envolvido no desencadear do processo de formulação da política de SSI.

Justificação para o Desencadeamento do Processo de Formulação

Questionados sobre a razão que levou ao desencadeamento do processo de formulação das políticas, e como se pode observar no Gráfico 17, 31 inquiridos responderam que foi por iniciativa dos técnicos de informática, seis por ordem do executivo, um por imperativo legal (certificação da qualidade), embora as Câmaras estejam a certificar os seus serviços só em um caso é que está já certificado o departamento de informática e um por outro motivo (no âmbito da estruturação de todo o serviço de informática). O total de respostas é diferente de 38 pelo facto de se poder escolher mais do que uma resposta e uma Câmara respondeu que foi por ordem do Executivo e por iniciativa dos técnicos de informática.

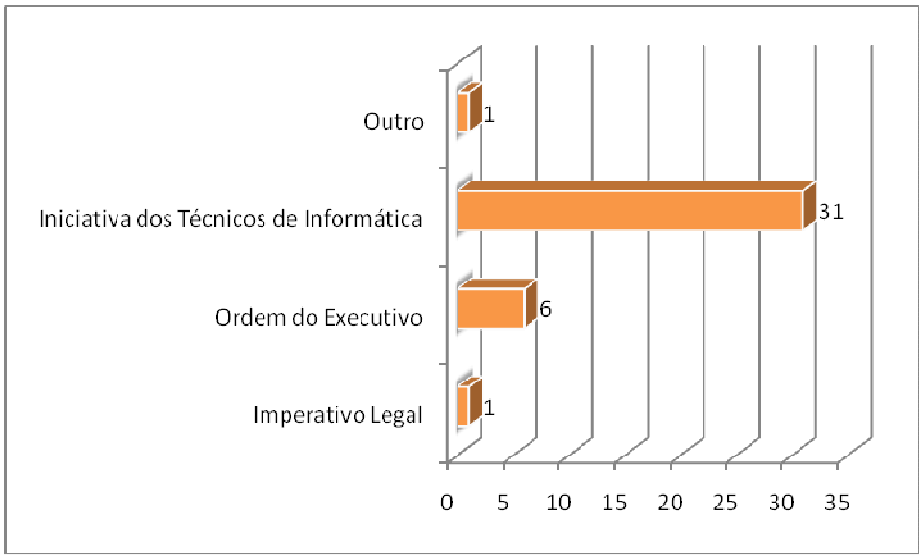


Gráfico 17: Justificação para o Desencadeamento do Processo de Formulação

Quem Elaborou a Política

Quanto a quem elaborou a política de SSI, com excepção de uma resposta, em todas as outras a elaboração da política recaiu sobre o pessoal interno da Câmara, mais especificamente, sobre os especialistas/técnicos de informática, em alguns casos com

a colaboração do gabinete jurídico da Câmara. Os resultados da análise desta questão encontram-se resumidos no Gráfico 18.

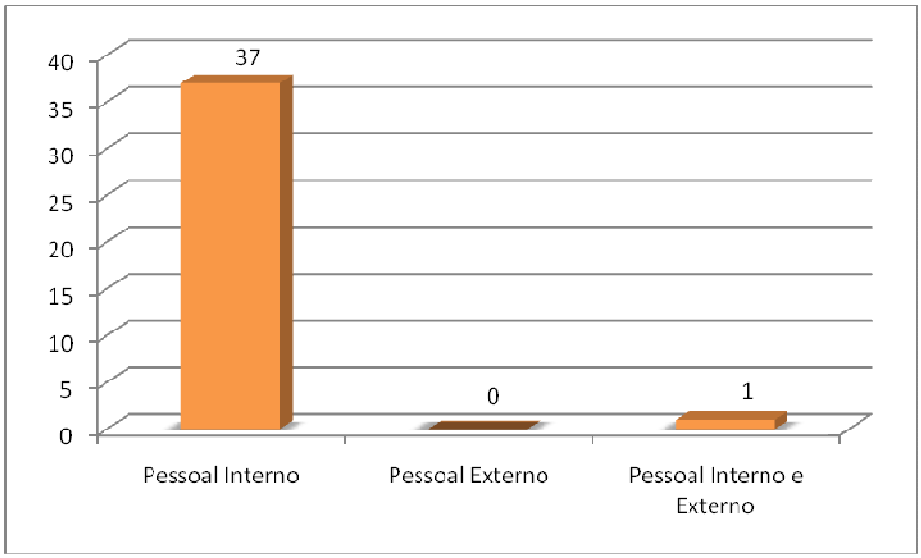


Gráfico 18: Quem Elaborou a Política

Aprovação Superior da Política

Nas 38 respostas a política foi aprovada superiormente, em maior número pelo Executivo, seguindo-se a aprovação por Vereadores e em alguns casos foi aprovada na Assembleia Municipal, pelo facto de estar incluída em regulamentos, carecendo dessa forma a sua aprovação por este órgão. Os resultados são apresentados no Gráfico 19.

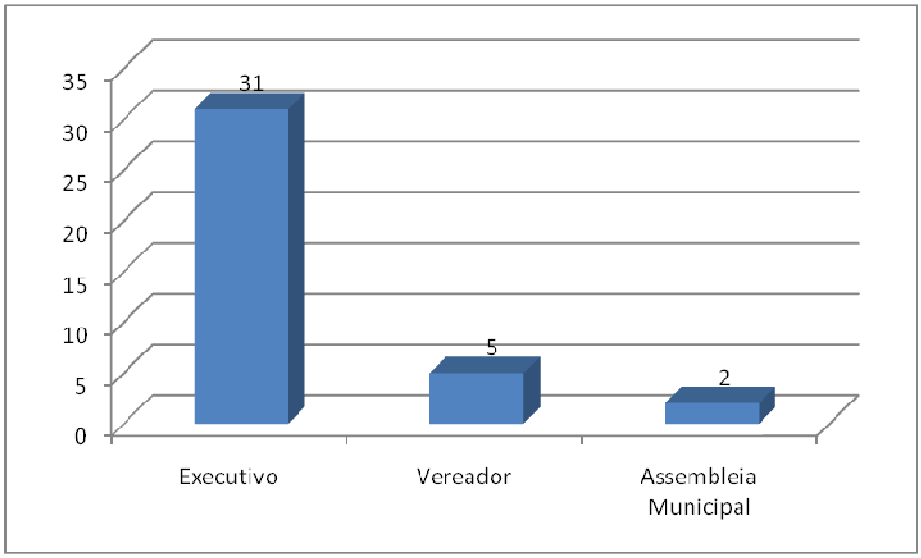


Gráfico 19: Quem Aprovou a Política

Responsabilidade de Implementação da Política

A responsabilidade de implementação da política de segurança da informação recaiu nos 38 casos sobre o departamento/divisão/sector de informática.

Políticas em Vigor

Nas 38 Câmaras que responderam possuir uma política de SSI, a mesma está implementada, ou seja, encontra-se em vigor.

Aceitação da Política

A implementação da política foi bem aceite pelos utilizadores em 79% (30) dos casos e mal aceite em 21% (8) dos casos. As oito Câmaras que responderam que a política foi mal aceite mencionaram sempre que não existiu qualquer má reacção por parte dos utilizadores, mas apenas algum desconforto natural de ter de se passar a cumprir regras. No Gráfico 20 apresentam-se os valores agregados das respostas a esta questão.

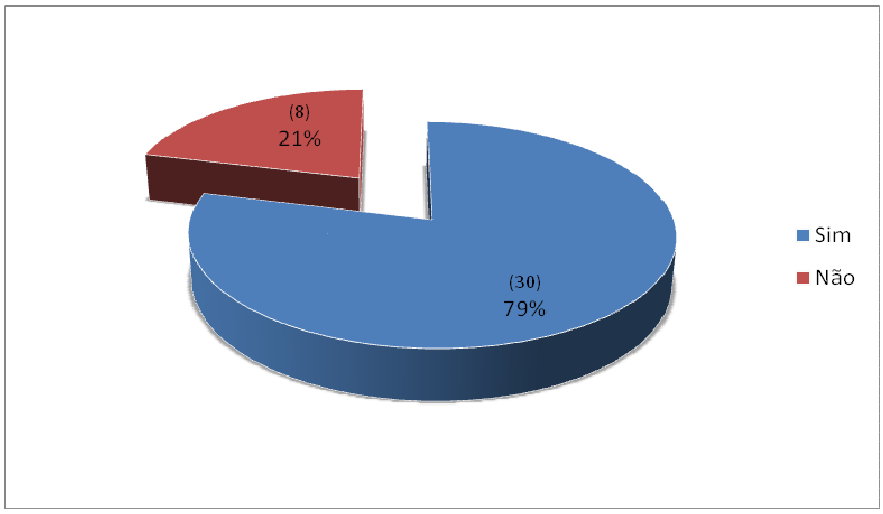


Gráfico 20: Aceitação da Política

Responsável pela Observância do Cumprimento da Política

Quanto há existência de alguém responsável pela observância ou cumprimento da política de segurança, 95% (36) responderam afirmativamente, contudo mencionando o facto de ser o departamento/divisão/sector da informática a realizar essa tarefa, não havendo nenhuma pessoa específica responsável por essa função. Os restantes 5% (2) não têm ninguém responsável. O Gráfico 21 apresenta os valores resultantes da análise das respostas a esta questão do inquérito.

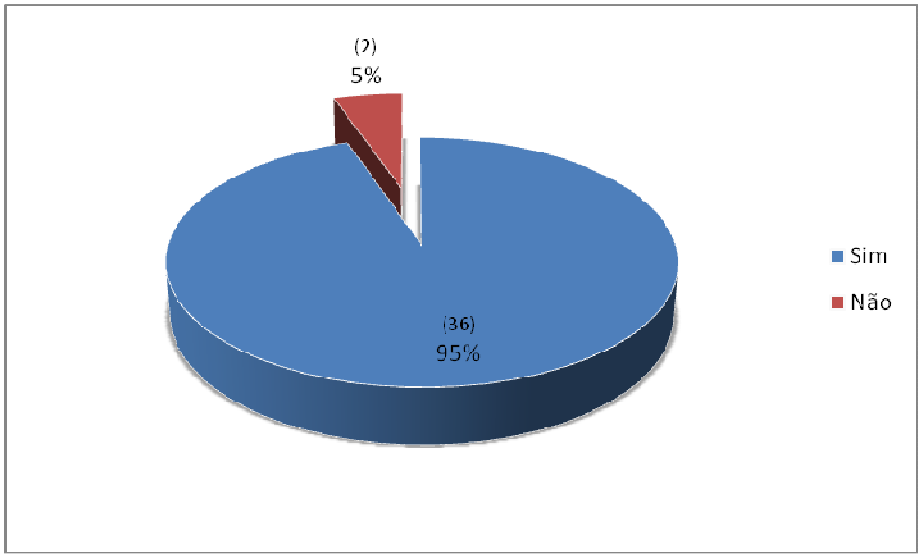


Gráfico 21: Responsável pela Observância do Cumprimento da Política

Revisão da Política

Das 38 Câmaras Municipais que indicaram ter implementado uma política de SSI, 87% (33) nunca fizeram qualquer revisão à política, 5% (2) fizeram uma vez uma revisão, 5% (2) têm previsto fazer a revisão anualmente e 3% (1) fazer a revisão de dois em dois anos. A reacção a esta questão foi praticamente unânime, na opinião de que é difícil definir um período específico, por considerarem que a revisão deve ser feita conforme as necessidades e esse período poder ser influenciado por diversas variáveis e factores, nomeadamente a aquisição de novo hardware e software, os serviços da Autarquia serem instalados em novos edifícios e a disponibilização de serviços *online* aos munícipes, entre outros.

Políticas Globais ou Parciais

Questionados sobre a existência de uma ou várias políticas de segurança de sistemas de informação, e como se pode observar no Gráfico 22, 89% (34) dos inquiridos responderam ter uma única política global e 11% (4) terem várias políticas parciais. Relativamente às respostas da existência de políticas parciais, nas 4 situações isso verifica-se devido à elaboração posterior de uma determinada norma e a sua não anexação à política anteriormente elaborada, tais como a elaboração de normas para o correio electrónico e para novos serviços.

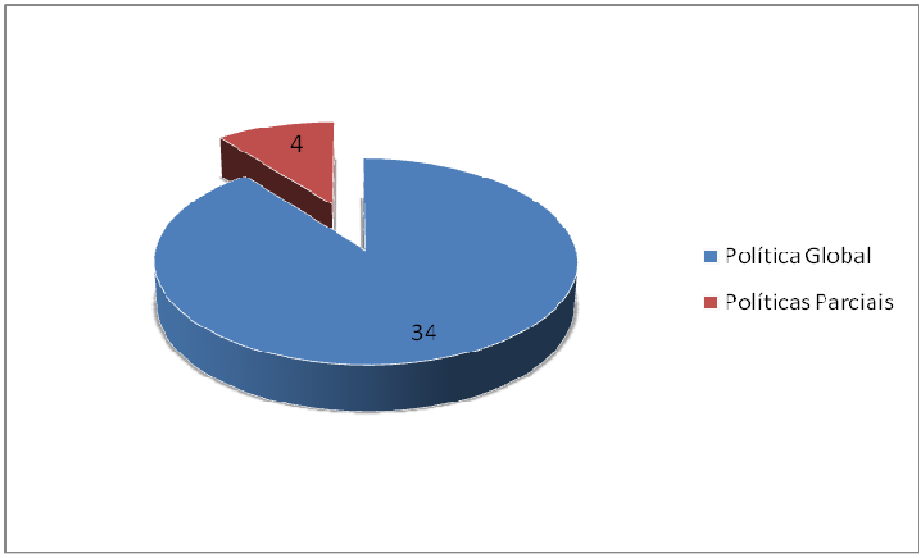


Gráfico 22: Política Global e Políticas Parciais

Aplicação da Política

A política de SSI aplica-se em 58% (22) dos casos às pessoas, em 37% (14) dos casos às pessoas e tecnologias, em 3% (1) dos casos às pessoas e outro e em igual número às tecnologias. Como cada resposta pode ter mais que uma opção, a sua soma não tem de dar 38. Os dados agregados por categorias podem ser visualizados no Gráfico 23 que se segue.

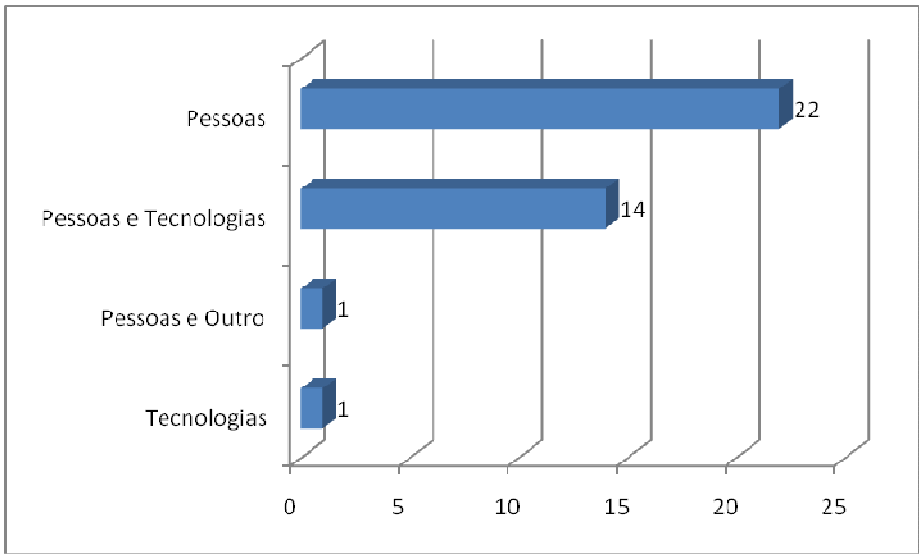


Gráfico 23: Aplicação da Política

Seguidamente serão apresentados os resultados dos dados do Quadro 3, que foi preenchido em caso de não existência de uma política.

Intenção de Formular uma Política

Das 270 Câmaras que indicaram não ter políticas de segurança, questionados sobre a intenção de formular uma política de SSI responderam afirmativamente 66% (177)

dos inquiridos, contra os 34% (93) que neste momento não pensam em formular qualquer política, conforme se observa no Gráfico 24.

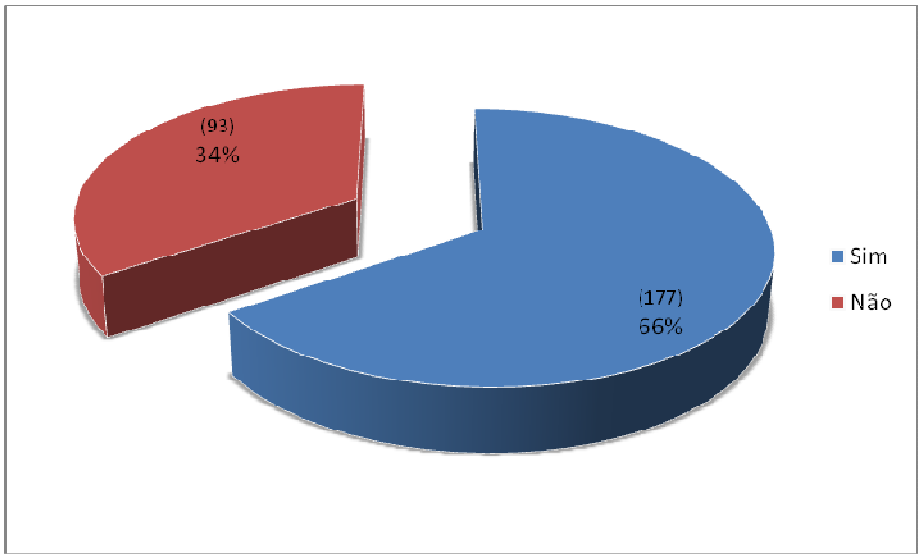


Gráfico 24: Intenção de Formular uma Política

Início do Processo de Formulação

Das 177 Câmaras que têm intenção de formular uma política de SSI, 42% (75) já estão em processo de elaboração da política e em 58% (102) a intenção existe, mas ainda não se iniciou o processo de formulação, como se pode observar no Gráfico 25.

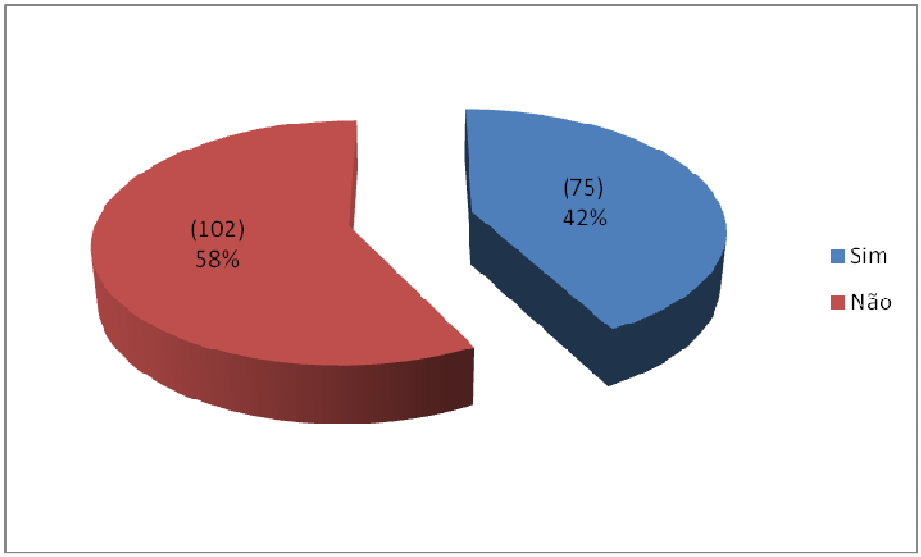


Gráfico 25: Início do Processo de Formulação

Segurança da Informação como Preocupação

Como se observa no Gráfico 24, 34% dos inquiridos, que corresponde a 93 Municípios, responderam que não têm intenção de formular uma política de SSI, contudo tendo-se colocado posteriormente a questão "A segurança da informação não é uma preocupação?", obtiveram-se 100% de respostas positivas. Verifica-se

assim uma potencial incongruência: apesar de não estarem a pensar formular uma política, consideram a segurança da informação uma preocupação, justificada pelo valor que reconhecem à informação. Alguns inquiridos defendem que não se trata de nenhuma incongruência, na medida em que não estão a pensar formular nenhuma política porque os mecanismos de software que têm implementados são suficientes para manter a segurança da informação.

Mecanismos de Protecção da Informação e dos Sistemas Informáticos

Questionados sobre a existência de mecanismos de protecção da informação e dos sistemas informáticos, a resposta foi unânime e todas as Câmaras possuem em maior ou menor número estes mecanismos, embora não se tenha procedido à sua quantificação no âmbito deste estudo. O mecanismo de protecção mais comum é a existência de software anti-vírus, as *firewalls* são dispositivos igualmente existentes em grande número, os filtros *anti-spam* e os *backups* diários da informação são também muito utilizados, assim como, *active directory* e *anti-malware*. Entende-se neste ponto por "anti-vírus" um programa projectado para detectar e eliminar vírus informáticos, enquanto que por "*anti-malware*" se entende os programas que para além de anti-vírus incluem funcionalidades de *anti-spyware*.

As Câmaras Municipais, em termos de dispositivos e aplicações de segurança, estão relativamente bem equipadas, verificando-se também que nas regiões pertencentes aos projectos de redes de cidades digitais este esforço é conjunto e superior, com a utilização de servidores conjuntos para a rede onde serão feitos, por exemplo, *backups* de informação numa localização externa.

4.6 Conclusões

O levantamento compreendeu a inquirição das 308 Câmaras Municipais existentes no país, compreendendo, assim, as 278 sitas no território continental, as 11 localizadas na Região Autónoma da Madeira e as 19 compreendidas na Região Autónoma dos Açores.

Das 308 Câmaras Municipais de Portugal, 12% (38) indicaram dispor de políticas de SSI e 88% (270) afirmaram não ter ou ainda se encontram em processo de formulação da política para posterior implementação.

A iniciativa de desenvolver a política de SSI é claramente dos Directores/Especialistas/Técnicos de informática, bem como a responsabilidade pela sua formulação, implementação e observância do seu cumprimento por parte dos utilizadores.

Constatou-se, ainda, que apesar do grande número de Câmaras Municipais que não possuem uma política de SSI, na verdade muitas foram aquelas que em resposta ao inquérito afirmaram ponderar a formulação de uma política de SSI. Tal facto ficar-se-á a dever à necessidade que actualmente surge de certificação de serviços, no âmbito da certificação da qualidade (ISO 9001) e da adesão a projectos de redes de cidades digitais.

Estão a ponderar formular uma política de SSI 66% (177) dos inquiridos, contra os 34% (93) que neste momento não pensam em formular nenhuma política, apesar destes últimos entenderem a segurança da informação como uma preocupação.

Dos inquiridos que responderam que estão a ponderar formular uma política de SSI, 42% já estão em processo de elaboração e nos restantes 58% a intenção de formular uma política existe, mas ainda não foi iniciado o processo de formulação.

Nas 38 Câmaras Municipais que indicaram ter políticas de SSI, estas encontram-se em vigor. A média dos anos de existência da política no total das 38 Câmaras que responderam afirmativamente à existência de política é de 3 anos, o que indica que a sensibilidade para a formulação e implementação de políticas é muito recente e que é um assunto que talvez não tenha sido tratado com a seriedade que lhe é devida.

Por outro lado, a existência de mecanismos de protecção da informação e dos sistemas informáticos é uma realidade na totalidade das Câmaras, e todas possuem em maior ou menor número estes mecanismos. O mecanismo de protecção mais comum é a existência de software anti-vírus, as *firewalls* são dispositivos igualmente existentes em grande número, os filtros *anti-spam* e os *backups* diários da informação são também muito utilizados.

Constatou-se ao longo da realização deste estudo que as Câmaras Municipais, em termos de dispositivos e aplicações de segurança, estão relativamente bem equipadas, verificando-se também que nas regiões pertencentes aos projectos de redes de cidades digitais, este esforço é conjunto e superior, com a utilização de servidores conjuntos para a rede onde serão feitos por exemplo *backups* de informação numa localização externa.

Capítulo 5

Descrição do Estudo

5.1 Introdução

No capítulo anterior apresentaram-se as principais conclusões do levantamento efectuado sobre políticas de SSI às Câmaras Municipais de todo o país. Face a essas conclusões, e atendendo-se à motivação com que se desencadeou o presente estudo, julga-se estarem reunidas as condições para enunciar o problema de investigação que irá ser alvo de atenção, bem como as questões a que este trabalho procurará responder. Posteriormente, o método, técnicas de investigação e fundamentos teóricos a utilizar neste estudo são apresentados, discutindo-se as razões que levaram à sua selecção, as suas principais características e os aspectos relacionados com o rigor, a validade e a generalidade das conclusões que permitem obter.

Com base nos dados recolhidos no levantamento efectuado junto das Câmaras Municipais, e que foi descrito no Capítulo anterior, obteve-se uma melhor consciência e conhecimento do contexto e realidade portuguesa, no que concerne a políticas de SSI, por parte das Câmaras Municipais, pelo que, se procedeu à concepção do estudo. Este capítulo apresenta essa concepção e descreve os trabalhos realizados.

A adopção de um particular método de investigação, e respectivas técnicas associadas, está condicionada pela perspectiva filosófica adoptada pelo investigador, pelo objecto do estudo e, principalmente, pelos objectivos da investigação [Caldeira e Romão 2002]. Neste sentido, este capítulo apresenta o método e técnicas a utilizar no estudo, bem como as perspectivas filosóficas em que assenta.

Tal como há várias perspectivas filosóficas que podem informar a pesquisa, assim há também vários métodos de investigação. Para Myers [2007], um método de investigação é uma estratégia de pesquisa que vai das suposições filosóficas subjacentes ao projecto de investigação até ao levantamento de dados. Estruturalmente, o presente capítulo aborda de forma geral as perspectivas filosóficas, seguindo-se a identificação do problema de investigação, bem como os objectivos e questões inerentes à investigação, definindo-se, por fim, a estratégia de investigação.

O enquadramento teórico para a interpretação dos resultados é feito com base na teoria institucional. Neste capítulo é abordada a teoria institucional onde se explicitam os principais conceitos, com destaque para a sua aplicabilidade.

5.2 Posicionamento Filosófico na Investigação

5.2.1 Perspectivas Filosóficas

De entre as várias correntes filosóficas existentes destacam-se a corrente Positivista e a Interpretivista. A posição positivista assume que a realidade é objectiva e independente do observador, enquanto a posição interpretivista defende que a realidade é o resultado da interpretação do observador. Os positivistas advogam que a forma correcta de gerar conhecimento é através da construção de teorias que são posteriormente validadas recorrendo-se a testes estruturados. Os interpretivistas defendem que o conhecimento sobre a realidade só pode ser construído através da compreensão e interpretação dos fenómenos em estudo. Os métodos de investigação na corrente interpretivista baseiam-se na inserção do investigador no meio da realidade em estudo, enquanto os métodos positivistas assentam na formulação e verificação de hipóteses através de testes [Macedo et al. 2006].

No que respeita à corrente filosófica Crítica, segundo Myers [2007] os investigadores críticos reconhecem que a sua capacidade está confinada por vários factores do domínio social, cultural e político. A pesquisa crítica focaliza-se nas oposições, nos conflitos e nas contradições da sociedade contemporânea.

Na Figura 12 identificam-se as perspectivas paradigmáticas que estão subjacentes às abordagens de investigação, anteriormente expostas.

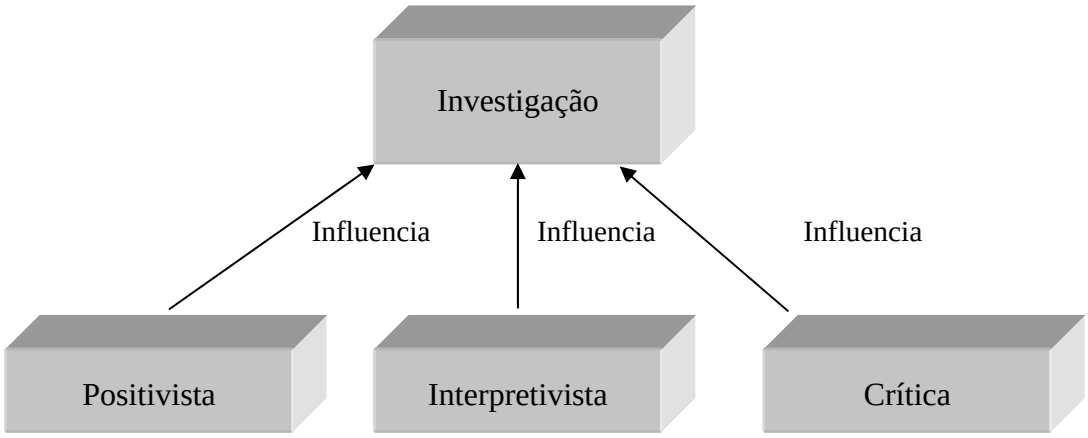


Figura 12: Perspectivas Paradigmáticas na Investigação
Adaptado de Myers [2007]

À medida que se planeiam e desenvolvem projectos de investigação, devem imediatamente confrontar-se dois assuntos: a concepção da investigação e a escolha da estratégia de investigação [Denzin e Lincoln 2000]. Para estes autores, "os paradigmas positivista, pós-positivista, construcionista e crítico ditam com varáveis graus de liberdade o *design* de uma investigação qualitativa" [p. 368]. As estratégias de pesquisa "ligam os investigadores a abordagens específicas e métodos para recolher e analisar materiais empíricos" [p. 371].

5.2.2 Métodos Qualitativos

Uma vez determinado o objectivo do estudo, é necessário escolher o tipo de abordagem que melhor se adequa a cada tipo de investigação. As abordagens de investigação podem ser classificadas de diversos modos, mas é amplamente aceite que se podem dividir em métodos quantitativos, qualitativos e mistos. Os métodos dedutivos e empíricos podem enquadrar-se dentro do que se denomina por abordagens de investigação quantitativas e são especialmente apropriados para o estudo de fenómenos ou objectos naturais. Por outro lado, o estudo de fenómenos culturais e sociais requer outro tipo de métodos, que não se baseiam em experimentação e teorias formais, mas sim em entrevistas, questionários, documentos, impressões e relações do investigador, os quais recebem o nome de métodos qualitativos [Marcos 2006].

Os métodos qualitativos nasceram no contexto das Ciências Sociais e aí se impuseram por melhor se adaptarem à subjectividade intrínseca da razão e do comportamento humano. No final da década de oitenta e início da década de noventa assistiu-se a um crescimento da investigação no domínio dos SI. Os estudos dessa época resultaram no desenvolvimento de diferentes abordagens metodológicas de investigação, que normalmente eram utilizadas noutros domínios científicos, nomeadamente na psicologia social, sociologia, psicologia, estudos organizacionais e na educação. Essas diferentes abordagens estão a impor-se cada vez mais, no domínio da concepção e desenvolvimento de SI [Marcos 2006]. Ainda segundo a autor anteriormente referido, neste domínio, a aplicação da abordagem qualitativa tem-se centrado fundamentalmente nos seguintes métodos:

- Estudo de Casos
- Estudos Etnográficos
- *Grounded Theory*
- Investigação-Acção

As características inerentes à investigação qualitativa são apresentadas e discutidas por diferentes autores. Neste trabalho, não se pretendendo abordar exaustivamente este tema, apresentam-se as propostas de Rossman e Rallis [1998], por se entenderem bastante abrangentes e completas. Para estes autores as características da investigação qualitativa são as seguintes:

- A pesquisa qualitativa ocorre em ambiente natural. O investigador geralmente vai para o local do participante para conduzir a investigação. Isto permite ao investigador desenvolver um nível de detalhe sobre o indivíduo ou local e envolver-se bastante nas experiências actuais dos participantes.

- A investigação qualitativa emprega métodos múltiplos que são interactivos e humanísticos. Os métodos de recolha de dados estão a aumentar e envolvem cada vez mais a participação activa dos participantes e a sensibilidade dos participantes no estudo. Os investigadores qualitativos procuram o envolvimento dos participantes na recolha de dados e elaboração de relatórios. Adicionalmente, os métodos actuais de recolha de dados

tradicionalmente baseados em observações abertas, entrevistas e documentos, incluem agora uma vasta gama de materiais, tais como sons, *email*, *scrapbooks* e outras formas emergentes.

- A investigação qualitativa é mais emergente que prefigurada. Vários aspectos surgem durante o estudo qualitativo. As questões de investigação podem surgir e ser refinadas à medida que o investigador aprende a formulá-las e a quem as deve dirigir. O processo de recolha de dados pode alterar-se à medida que se vão abrindo portas à recolha de dados e o investigador aprende os melhores locais para estudar acerca do principal ponto de interesse. Estes aspectos de um modelo de investigação aberta tornam difícil definir fortemente a investigação qualitativa na fase de proposta ou estádio de pesquisa inicial.

- A investigação qualitativa é fundamentalmente interpretativa, isto significa que o investigador interpreta os dados desenvolvendo uma determinada descrição e analisa os dados por temas ou categorias e finalmente faz uma interpretação ou delineia conclusões acerca dos seus significados pessoais e teóricos, estabelecendo o que se aprendeu e fornecendo questões posteriores. Em suma, não se pode escapar à interpretação pessoal da análise de dados qualitativa.

- O investigador qualitativo vê os fenómenos sociais holisticamente. Isto explica porque é que as investigações qualitativas aparecem mais como visões panorâmicas do que como micro-análises.

- Quanto mais complexa, interactiva e fechada for a narrativa, melhor é o estudo qualitativo. Modelos visuais de muitas facetas de um processo ou fenómeno central ajudam no estabelecimento da imagem holística.

- O investigador qualitativo sistematicamente reflecte sobre quem ele é no inquérito e é sensível à sua biografia pessoal e como isso desenha o estudo. Esta introspecção e aceitação de preconceitos, valores e interesses tipificam hoje a investigação qualitativa. O ser pessoal do participante torna-se inseparável do ser do investigador.

- O investigador qualitativo utiliza raciocínios complexos que são multifacetados, iterativos e simultâneos. Embora o raciocínio seja grandemente indutivo, utilizam-se tanto processos indutivos como dedutivos. Este processo de pensamento é também iterativo, com um vaivém cíclico de recolha e análise de dados e reformulação do problema e vice-versa. Adicionalmente, há as actividades simultâneas de recolha, análise e escrita de dados.

- O investigador qualitativo adopta e utiliza uma ou mais estratégias de inquirir como um guia para os procedimentos no estudo qualitativo.

O presente trabalho de investigação é de cariz qualitativo uma vez que as características inerentes à investigação qualitativa estão presentes no mesmo,

nomeadamente a utilização do método “estudo de casos”, a técnica de investigação “entrevistas” e ocorrer num ambiente natural.

5.3 Problema de Investigação

Como foi referido no Capítulo 1, na secção “Motivação da Investigação”, observa-se a existência de um número considerável de estudos que se debruçaram sobre a temática das políticas de segurança [de Sá-Soares 2005]. Estes estudos abordam tópicos diversificados, que vão desde a importância e factores a considerar para o sucesso dessa política até aos tipos e elementos constituintes de uma política de SSI. Contudo, verifica-se um número reduzido de estudos acerca das questões da implementação de políticas de segurança. Esta constatação aplica-se também à falta de investigação substanciada acerca dos factores que afectam ou condicionam a adopção de políticas de SSI.

No âmbito do interesse deste trabalho – as Câmaras Municipais – esses estudos são mesmo inexistentes. Embora haja estudos sobre a utilização das TI nas Câmaras Municipais [OSIC e UMIC 2006] e sobre o montante orçamental para o investimento em TIC [Meneses 2008], constata-se que o domínio da SSI não tem sido alvo privilegiado dos levantamentos. A título de exemplo, no primeiro estudo referido encontram-se menções às preocupações com a segurança, mas de uma forma superficial, continuando a adopção de políticas de segurança nas Câmaras Municipais a ser uma questão em aberto, não se conhecendo qualquer estudo nesta área.

Esta observação levou à realização do levantamento sobre políticas de SSI nas Câmaras Municipais em Portugal, para desta forma se conhecer a realidade do país neste sector da Administração Pública no que diz respeito à existência ou não de políticas de SSI, para posteriormente se poder estudar mais a fundo esta questão.

Das 308 Câmaras Municipais de Portugal, 12% (38) indicam possuir políticas de SSI e 88% (270) não possuem ou ainda se encontram em processo de formulação da política para posterior implementação.

Apesar do grande número de Câmaras Municipais que não possuem uma política de SSI, muitas foram aquelas que em resposta ao inquérito afirmaram ponderar a formulação de uma política de SSI. Concretamente, ponderam formular uma política de SSI 66% (177) dos inquiridos, contra os 34% (93) que neste momento não pensam formular nenhuma política. Dos inquiridos que responderam que estão a ponderar formular uma política de SSI, 42% (75) já estão em processo de elaboração e nos restantes 58% (102) a intenção de formular uma política existe, mas ainda não foi iniciado o processo de formulação.

Nas 38 Câmaras Municipais que têm políticas de segurança de sistemas de informação, estas encontram-se em vigor. O conteúdo das políticas engloba tecnologias e comportamentos em 28 casos, comportamentos em 7 dos casos sendo que nos restantes 3 casos a política acrescenta considerações de outra ordem. A média dos anos de existência da política no total das 38 Câmaras que responderam afirmativamente à existência de política é de 3 anos, o que indica que a sensibilidade

para a formulação e implementação de políticas é recente e que é um assunto que talvez não tenha sido alvo da devida atenção.

Estes resultados levaram à definição do problema de investigação que anima a realização deste trabalho e que consiste na reduzida expressão da adopção de políticas de SSI por parte das Câmaras Municipais Portuguesas.

O exposto anteriormente constitui a base de trabalho para as duas secções seguintes, que identificam os objectivos e questões da investigação a que este trabalho se propõe dar resposta.

5.4 Objectivos da Investigação

Conforme se referiu na secção anterior, o presente trabalho de investigação foi motivado pela constatação da inexistência de estudos sobre a adopção de políticas de SSI nas Câmaras Municipais em Portugal. Esta constatação deu origem ao problema de investigação, que de forma a ser diluído implica satisfazer os seguintes objectivos:

- Estabelecimento de um quadro teórico inicial para o estudo das práticas de SSI na Administração Pública Local em Portugal, com especial incidência no que respeita à adopção de políticas de segurança;
- Identificação das componentes e características das políticas de SSI existentes na Administração Pública Local;
- Identificação de factores que condicionam a adopção de políticas de SSI por parte das Câmaras Municipais;
- Classificação dos factores condicionadores da adopção de políticas de SSI por parte das Câmaras Municipais e
- Proposta de um enquadramento para auxiliar na compreensão da adopção de políticas de SSI na Administração Pública Local em Portugal.

Com vista a atingir estes objectivos, uma série de questões de investigação têm de ser tidas em conta. Essas questões são apresentadas na secção que se segue.

5.5 Questões de Investigação

A ênfase principal deste trabalho é identificar quais são os factores que condicionam, positiva e negativamente, a adopção das políticas de SSI. Para atenuar esse problema de investigação e tendo em conta os objectivos do presente trabalho de investigação, avançam-se quatro questões de investigação:

> **Questão 1 -** Que factores condicionam (facilitando ou inibindo) a adopção de políticas de SSI nas Câmaras Municipais Portuguesas?

Questão 2 - Quais são as características e componentes das políticas de SSI existentes nas Câmaras Municipais Portuguesas?

Questão 3 - De que forma se articulam os factores condicionantes da adopção de uma política de SSI no âmbito das Câmaras Municipais Portuguesas?

Questão 4 - Que recomendações poderão ser avançadas de forma a potenciar a adopção de políticas de SSI nas Câmaras Municipais Portuguesas?

Com vista a uma melhor estruturação e articulação do trabalho, recorreu-se ao enquadramento para a análise da mudança proposto por Walsham [1993]. Este enquadramento é composto por três dimensões fundamentais: conteúdo, processo e contexto.[6] A Figura 13 apresenta as dimensões do enquadramento da investigação.

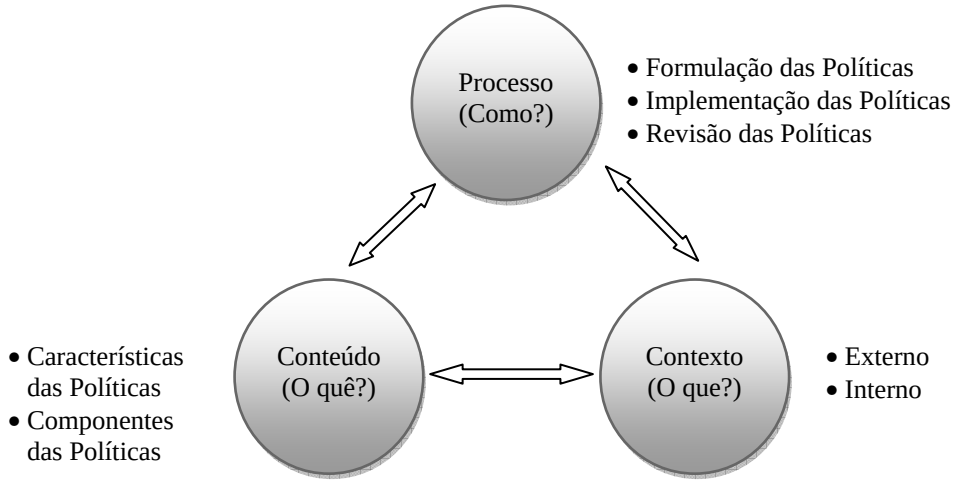


Figura 13: Enquadramento da Investigação

O trabalho que se propõe pretende dar resposta aos pontos de cada uma das três grandes dimensões de investigação, ou seja, ao Processo, ao Conteúdo e ao Contexto de uma política de SSI. Ao se responder a essas três dimensões julga-se que se conseguirá dar resposta às questões de investigação propostas neste trabalho de investigação.

Tendo por base as três dimensões do enquadramento de Walsham, os dados serão analisados de acordo com os seguintes parâmetros: no que se refere à dimensão "Conteúdo" focar-se-ão os aspectos relacionados com "o quê" das políticas de SSI, ou seja, as suas características e componentes; relativamente à dimensão "Processo", tentar-se-á dar resposta ao "como", ou seja, ao modo como as políticas são formuladas, implementadas e revistas e, por fim, na dimensão "Contexto" centrar-se-á a atenção em "o que" afecta as políticas de SSI, ou seja, nos factores pertencentes ao contexto externo e ao contexto interno das Câmaras Municipais – no contexto externo serão tidos em conta aspectos pertencentes às esferas política, legal, social e económica e no contexto interno os elementos a ter em conta serão os referentes às esferas política, social e cultural dentro das Câmaras Municipais.

[6] O enquadramento é ainda composto por um quarto componente, designadamente a ligação.

5.6 Estratégia de Investigação

Nesta secção será discutida a estratégia de investigação a seguir neste trabalho. Para tal, apresentar-se-ão o método de investigação, as técnicas de geração de dados a utilizar, bem como a forma como se analisaram os dados recolhidos.

5.6.1 Método de Investigação

Dado o problema de investigação, os objectivos enunciados para o presente estudo, as questões de investigação formuladas e a matriz filosófica da investigadora, o método de investigação seleccionado para o presente trabalho foi o "Estudo de Caso". Nesta secção será abordado esse método, iniciando-se com uma breve definição do método, apresentando-se de seguida a sua caracterização e objectivos, a sua aplicação na investigação na área dos SI, bem como, as suas limitações e vantagens.

5.6.1.1 Definições de Estudo de Casos

O termo "Estudo de Caso" assume diversas denotações. Pode ser usado para descrever uma unidade de análise, como o fazem os autores Denzin e Lincoln [2000, p. 372] onde afirmam que o Estudo de Casos "não é uma escolha metodológica mas uma escolha do objecto a ser estudado, como por exemplo uma criança ou uma sala de aula", ou para descrever métodos de investigação. A discussão nesta secção concerne o uso do Estudo de Casos como um método de investigação.

Embora haja numerosas definições, Yin [1994, p. 23] define o método de Estudo de Casos como uma "pesquisa empírica que investiga um fenómeno contemporâneo dentro de um contexto real de vida, no qual as fronteiras entre fenómeno e contexto não são claramente evidentes e no qual múltiplas fontes de evidência são usadas".

Numa linha similar, Benbasat et al. [1987] definiram este método como uma estratégia de investigação que examina um fenómeno no seu estado natural, empregando múltiplos métodos de recolha de dados e tratamento de dados sobre uma ou algumas entidades (pessoas, grupos ou organizações).

5.6.1.2 Caracterização e Objectivos

Yin [1989] afirma que a decisão por uma pesquisa qualitativa do tipo exploratório não define obrigatoriamente a preferência pelo método do Estudo de Casos, uma vez que esse método pode ser utilizado também com outros objectivos, tais como o descritivo e o explanatório, não havendo, segundo aquele autor, uma "hierarquia para os métodos de pesquisa". Para Yin, essa escolha deve ser realizada com base em três factores:

- O tipo de questão a que a investigação pretende dar resposta;
- A contemporaneidade do fenómeno que se pretende estudar e

- A possibilidade de controlo sobre esse fenómeno.

O método de Estudo de Caso é um dos mais adequados quando se procura responder a questões do tipo como? e porquê?, quando o fenómeno estudado é contemporâneo (isto é, ainda está ocorrendo) e quando há pouca ou nenhuma possibilidade de controlar os factores envolvidos. Quando o foco é em fenómenos ou eventos não contemporâneos (isto é, já ocorreram) a análise histórica será o método mais adequado. Quando se procura responder a questões do tipo quem?, onde?, quantos?, o que?, os levantamentos (*surveys*) podem revelar-se mais adequados. Quando o foco é em questões do tipo porquê? e como?, mas existe controlo sobre os factores relevantes envolvidos, o método experimental poderá ser o mais adequado. Questões do tipo o que? (ou quais?) também podem ser respondidas pelo método do Estudo de Caso quando a pesquisa é do tipo exploratório, isto é, quando se busca identificar aspectos presentes e não quantificá-los ou descrever a sua incidência estatística.

Para Yin [1989], as questões do tipo como? e porquê? são questões explicativas e tratam de relações operacionais que ocorrem ao longo do tempo mais do que frequências ou incidências, pelo que o método de Estudo de Caso será mais adequado para lhes dar resposta. Este autor apresenta quatro aplicações para o método de investigação Estudo de Casos:

1. Para explicar ligações causais nas intervenções na vida real que são muito complexas para serem abordadas pelos levantamentos ou pelos estudos laboratoriais;

2. Para descrever o contexto da vida real no qual a intervenção ocorreu;

3. Para fazer uma avaliação, ainda que de forma descritiva, da intervenção realizada;

4. Para explorar aquelas situações onde as intervenções avaliadas não possuem resultados claros e específicos.

Quanto aos objectivos do método de investigação Estudo de Casos, McClintock et al. [1979, p. 612], enumeram os seguintes:

1. Capturar o esquema de referência e a definição da situação de um dado participante;

2. Permitir um exame detalhado do processo organizacional;

3. Esclarecer aqueles factores particulares ao caso que podem levar a um maior entendimento da causalidade.

Outro autor, Bonoma [1985, p. 207], considera este método útil “quando um fenómeno é amplo e complexo, onde o corpo de conhecimento existente é insuficiente para permitir a proposição de questões causais e quando um fenómeno não pode ser estudado fora do contexto no qual ele naturalmente ocorre”. Este mesmo autor identifica como objectivos na recolha de dados do método de Estudo de Casos, os seguintes [Bonoma 1985, p. 206]:

1. Descrição

2. Classificação

3. Desenvolvimento teórico

4. Teste limitado da teoria

Normalmente, o método de investigação Estudo de Casos consiste em cinco fases sequenciais [MacNealy 1997; Stake 2000, Yin 1994], que se apresentam na Figura 14. Esta figura é detalhada por Pereira [2002].

- Durante a selecção e definição do problema a ser investigado, estabelece-se a problemática do estudo proposto, justificando-se a motivação da investigação. Adicionalmente, especificam-se os aspectos relacionados com o estudo, os quais se podem caracterizar por uma reconstrução histórica onde a sua natureza e configuração podem ser descritas.

- No planeamento da investigação define-se a evolução de um tópico, clarificando-se o tema chave para o estudo. Para além disso, determina-se o procedimento de recolha de dados que pode ser feito através de diferentes técnicas, tais como entrevistas, questionários e análise de documentos.

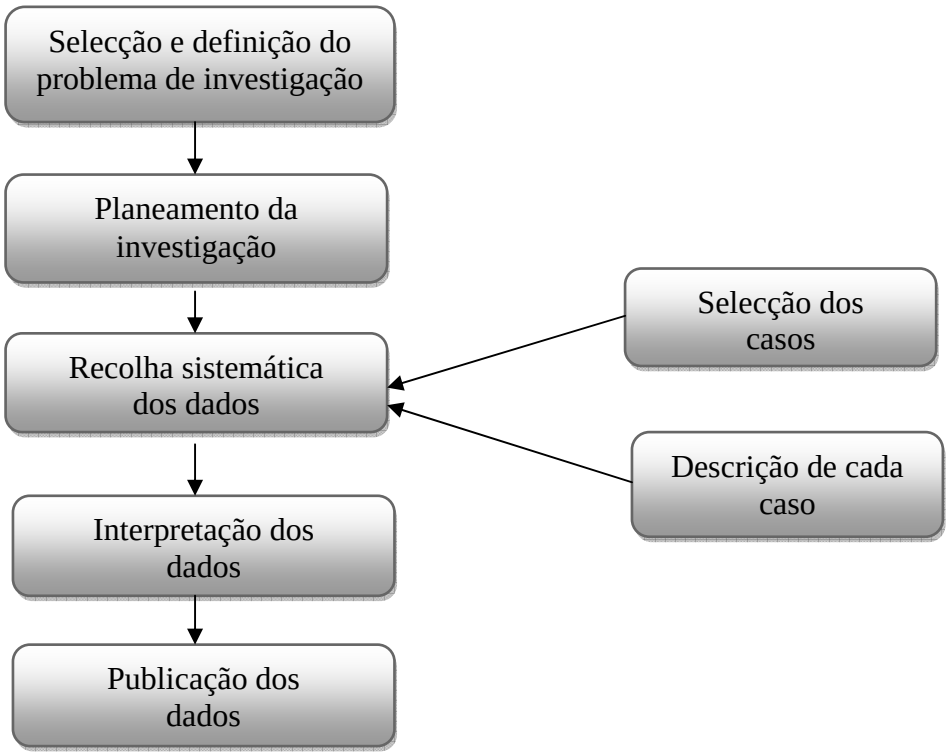


Figura 14: Etapas da Investigação com o Método Estudo de Casos

- Segundo Stake [2000], os investigadores têm de ter em linha de conta cinco aspectos durante a selecção da recolha de dados:
    - Seleccionar os métodos que produzem os dados necessários.
    - Seleccionar os métodos que produzem os dados que podem ser examinados por outros investigadores.
    - Usar a triangulação para garantir a precisão dos resultados.
    - Provar os procedimentos durante a recolha de dados.
    - Descrever os métodos usados e teorias/informações encontradas para a evolução de outros investigadores.

- A interpretação dos dados deve considerar os padrões e categorias identificados nos dados. Os restantes processos realizam-se com a verificação, interpretação e respectivas conclusões através da análise por outros investigadores ou pelos próprios participantes do estudo.

- Finalmente, são publicados os resultados da investigação, em diferentes formatos, conforme seja para a organização onde se realizou o estudo ou para a sua publicação em livro, revista ou conferência.

5.6.1.3 Estudo de Casos Aplicado a Sistemas de Informação

O método de investigação Estudo de Casos é considerado por muitos investigadores um dos métodos mais adequados para a realização de investigação na área dos SI [Benbasat et al. 1987; Darke et al. 1998; Klein e Myers 1999; Lee 1989; Orlikowski e Baroudi 1991; Walsham 1995].

Não será pois de estranhar que a investigação por Estudo de Casos seja o método mais comum usado em SI [Alavi e Carlson 1992; Caldeira e Romão 2002; Orlikowski e Baroudi 1991]. Segundo Caldeira e Romão [2002, p. 77], o Estudo de Casos, "desde que devidamente desenhado e executado, é uma estratégia de investigação (método) que permite captar de uma forma poderosa os mais diferentes aspectos inerentes à complexa realidade social que envolve as organizações e respectivos Sistemas de Informação".

Para Hartley [1994], o Estudo de Casos adequa-se particularmente a investigações onde seja necessário estudar comportamentos organizacionais, nomeadamente processos de conflito e fenómenos ligados à reacção do factor humano à implementação das TI. Aquele autor considera ainda que o Estudo de Casos representa um meio de investigação adequado para o estudo de campos sociais emergentes ou em áreas em constante mutação, como é o caso dos SI.

5.6.1.4 Limitações e Vantagens do Estudo de Casos

O método de investigação Estudo de Casos é um método das Ciências Sociais e, como outras abordagens, tem as suas vantagens e desvantagens.

Um dos principais problemas normalmente apontados aos estudos de casos segundo Cunha [2000, p. 37] é a "subjectividade introduzida pelo investigador, sendo uma das suas fontes a interpretação que o investigador faz da situação. No entanto, a subjectividade é um problema recorrente nas várias abordagens de comparação".

De acordo com Lee [1989], identificam-se quatro problemas na realização de investigação em SI, quando é usado o método Estudo de Casos:

1. Como controlar as observações

   Sem controlos de laboratório ou controlos estatísticos, deve-se tentar utilizar controlos naturais de forma que um factor seja constante e os outros, variáveis.

2. Como controlar as deduções

   A dedução controlada ou lógica não necessita de análise matemática para comprovar a sua validade. A matemática é um subconjunto da lógica formal, e não o contrário. As deduções lógicas por meio de proposições verbais são tão válidas quanto aquelas derivadas de proposições matemáticas.

3. Como permitir a replicação

   Outro investigador pode utilizar as mesmas teorias testadas no Estudo de Caso original em que um conjunto diferente de condições iniciais, em outra população, e chegará a resultados diferentes, porém testando a mesma teoria. Embora as observações de um caso em particular não possam ser replicadas, os resultados do Estudo de Casos, confirmando ou não uma determinada teoria, podem ser replicados.

4. Como permitir a generalização

   A capacidade de generalização é uma qualidade da teoria quando esta é testada e confirmada em diversas situações, seja através de Estudo de Casos, experiências de laboratório ou experiências estatísticas. Portanto, é um problema de qualquer tipo de pesquisa. A capacidade de generalização de uma teoria só pode ser confirmada a partir da execução de testes sucessivos em contextos diferentes, seja por meio de estudos de casos, seja por meio de experiências de laboratório ou de outros métodos que viabilizem o teste de teorias.

Neste sentido, MacNealy [1997, p. 183] afirma que o método Estudo de Casos "é uma ferramenta qualitativa, como tal, o seu principal objectivo é proporcionar uma descrição contundente de um evento ou de um pequeno grupo de pessoas ou objectos. Dado que o âmbito de um Estudo de Casos é tão estreito, as descobertas raramente podem ser generalizadas, mas um Estudo de Casos pode oferecer ideias sobre eventos e comportamentos e pode proporcionar hipóteses para serem testadas".

Apesar das limitações apontadas anteriormente, o método de investigação Estudo de Caso apresenta diversas vantagens. Benbasat et al. [1987] enumeram as seguintes vantagens:

- O investigador pode estudar o sistema de informação no seu estado natural, aprende sobre o estado-de-arte e gera teorias com base nas práticas verificadas;
- Este método leva o investigador a perceber a natureza e a complexidade do problema;
- Conhecimentos válidos podem ser retirados nas áreas que se encontram em constante mutação.

Hartley [1994] apresenta como vantagem e ponto forte do Estudo de Casos a capacidade de explorar processos sociais à medida que esses processos ocorrem nas organizações, permitindo uma análise processual, contextual e longitudinal das várias acções e significados que ocorrem e são construídos nas organizações. A natureza mais aberta da recolha de dados em estudos de casos permite analisar em profundidade os processos e as relações entre eles.

5.6.2 Técnicas de Geração de Dados

Face aos objectivos estipulados para este estudo, às questões de investigação formuladas e em articulação com o método de investigação seleccionado, identifica-se a existência de duas formas geradoras de dados: a recolha de documentos e as entrevistas.

Em relação aos documentos, as técnicas de geração de dados circunscrevem-se à obtenção de políticas de SSI. O sucesso deste passo dependeu muito da abertura dos responsáveis autárquicos, uma vez que existe algum "receio" ao abordar e muito mais em disponibilizar este tipo de documentos, por serem frequentemente considerados como documentos muito reservados.

A técnica enunciada no parágrafo anterior é importante para a recolha de dados e condução do estudo, contudo, há questões que ficariam em aberto só com esta observância. Logo, é necessária a utilização de mais uma técnica de geração de dados e que dada a natureza deste estudo consistiu na realização de entrevistas.

Assim, entrevistaram-se 44 responsáveis autárquicos, distribuídos pelos 308 municípios pertencentes aos 18 distritos e às duas regiões autónomas de Portugal, tendo por base dois factores: a dimensão eleitoral e quatro *clusters*[7] que classificam as Câmaras.

As 308 Câmaras Municipais Portuguesas foram assim subdivididas em quatro *clusters*, dependendo a sua posição de quatro factores distintos. Os factores de diferenciação são: Câmaras Municipais que têm uma política de SSI (*Cluster* 1); Câmaras que não têm uma política de SSI, mas estão em processo de formulação ou

[7] Porter (1998) define *Cluster* como concentrações geográficas de empresas interligadas, fornecedores especializados, provedores de serviços, empresas em indústrias afins e as instituições que lhes estão associadas – universidades, agências públicas de certificação e normalização, associações empresariais – em áreas específicas que competem e cooperam entre si. No âmbito deste estudo, o termo *cluster* será empregue para designar um grupo de entidades que verificam determinados critérios classificativos.

adopção (*Cluster* 2); Câmaras que não têm uma política de SSI, mas têm intenção de a formular (*Cluster* 3) e Câmaras que não têm uma política de SSI, não tendo intenção de adoptar qualquer política (*Cluster* 4).

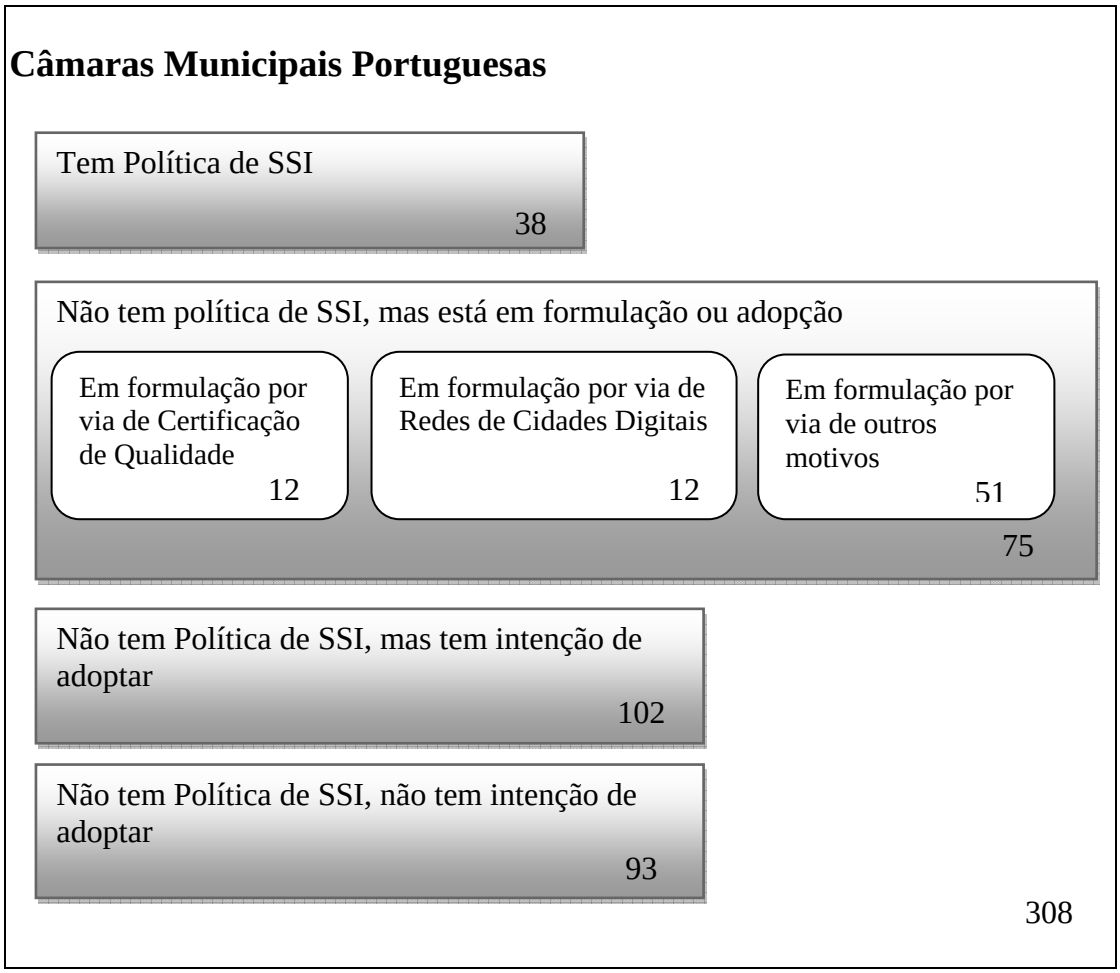


Figura 15: *Clusters* em Estudo

Outro factor de selecção foi a dimensão eleitoral. Outras variáveis ou indicadores poderiam servir para a diferenciação dos municípios, como por exemplo a área, o montante de impostos, o número de freguesias, população residente, mas o mais unanimemente utilizado é a dimensão por número de eleitores. Desta forma, a selecção dos municípios vai ser em relação à sua dimensão eleitoral, tendo por base os seguintes intervalos populacionais:

	Classes de Dimensão Eleitoral
A	Mais de 100.000 eleitores (autarquias muito grandes)
B	50.000 a 100.000 eleitores (autarquias grandes)
C	10.000 a 50.000 eleitores (autarquias médias)
D	Até 10.000 eleitores (autarquias pequenas)

As entrevistas foram assim condicionadas por estes intervalos e pelos quatro *clusters*, tendo-se entrevistado responsáveis autárquicos de Câmaras com diferentes dimensões, permitindo assim que o estudo fosse mais abrangente e completo.

Está-se, assim, como observa Stake [2000, p.436], mais interessado no estudo "de uma população de casos do que num caso individual". Ainda recorrendo ao trabalho citado de Stake, pode concluir-se do exposto que este projecto envolveu a realização de um "estudo de caso colectivo"[8], no pressuposto de que o seu exame levará a uma melhor compreensão acerca de uma colecção de casos ainda mais abrangente, nomeadamente as Câmaras Municipais Portuguesas.

As entrevistas foram objecto de gravação áudio, depois de obtida a devida autorização dos entrevistados ou dos seus superiores hierárquicos.

Quanto ao tipo de entrevistas a realizar, a escolha recaiu nas entrevistas semi-estruturadas, por se considerarem as mais adequadas ao presente estudo, uma vez que as questões base são de fácil identificação, mas existe sempre alguma subjectividade que só poderá ser resolvida com este tipo de entrevista.

De forma a melhor orientar as entrevistas elaboraram-se guiões com questões previamente preparadas para serem colocadas aos participantes, mas com a abertura suficiente para que sempre que a entrevistadora achasse pertinente, poder fazer outras questões adicionais com vista a uma melhor compreensão dos temas versados ou a uma exploração mais detalhada de alguns aspectos referidos pelos participantes.

Antes de se iniciar a entrevista propriamente dita, ou seja, previamente à colocação das questões foi necessário esclarecer um conjunto de pontos que não são mais que a abertura da entrevista com o entrevistado em causa:

- Informar o âmbito da realização do trabalho de investigação;
- Informar sobre o tema do trabalho de investigação;
- Informar acerca dos objectivos da investigação e a necessidade de realizar a entrevista;
- Informar como será utilizada e tratada a informação recolhida;
- Informar como serão difundidos os resultados obtidos.

Para além destes pontos, ao entrevistado foi solicitada a autorização para a gravação da entrevista, bem como a recolha de informação acerca da sua pessoa, nomeadamente, a identificação pessoal, a formação académica, o seu cargo na Câmara Municipal e os anos de serviço que acumula nesse cargo.

Realizados estes procedimentos prévios, dava-se início à entrevista propriamente dita. As questões concretas colocadas aos entrevistados encontravam-se divididas em quatro guiões, ou seja, tantos quantos os *clusters*. Por sua vez, cada um dos guiões foi organizado tendo em conta a sua aplicabilidade a esse *Cluster* segundo as três dimensões anteriormente definidos:

- Conteúdo das políticas de SSI;

[8] Stake [2000] identifica três tipos de estudo de caso: estudo de caso intrínseco (foco na melhor compreensão de um caso particular), estudo de caso instrumental (se examina um caso particular com vista a obter melhor entendimento de um dado fenómeno ou para rever uma generalização) e estudo de caso colectivo (um estudo instrumental estendido a vários casos).

- Processo associado às políticas de SSI;
- Contexto relativo às políticas de SSI.

Na primeira dimensão, que está relacionada com o conteúdo das políticas de SSI, pretendeu-se saber as características e as componentes das políticas. Dada esta especificidade, esta dimensão só está presente no guião relacionado com o *Cluster* que abrange as Câmaras que não tem uma política de SSI, mas que se encontram em processo de formulação da mesma.

A segunda dimensão diz respeito ao processo associado às políticas, ou seja, aos processos de formulação, implementação e revisão das políticas. Este domínio só está presente no *Cluster* 1 e parcialmente no *Cluster* 2, porque só estavam capacitadas para responder a este tipo de perguntas as Câmaras que já têm uma política e as Câmaras que estão em processo de formulação.

Na terceira e última dimensão, que está relacionada com o contexto relativo às políticas de SSI, as questões incidiram sobre os factores facilitadores e inibidores da adopção das políticas de SSI pelas Câmaras Municipais Portuguesas. Este domínio está presente em todos os guiões pois abrangia os quatro *Clusters*.

Seguidamente apresentam-se os guiões elaborados para aplicação em cada um dos quatro *clusters*.

Guião 1 – Câmaras que têm uma política de SSI

Q1: Esta Câmara Municipal adoptou uma política de SSI, como é que foi formulada?

Q2: Quem elaborou a Política de SSI?

Q3: Quem detectou a falta de uma política?

Q4: Porque foi adoptada a política de SSI?

Q5: Como é que foi implementada a política de SSI?

Q6: A política é revista periodicamente? Se sim, como é que tal é feito? Se não, porquê?

Q7: Durante os processos de implementação, formulação e revisão, surgiram dificuldades ou problemas? Se sim, quais e em que processo? Esses problemas foram superados? Se sim, como? Se não, porquê?

Q8: Quais eram os benefícios/utilidade esperados da política de SSI aquando da sua adopção/formulação?

Q9: Os benefícios/utilidade esperados concretizaram-se. Se não, porquê?

Q10: Aquando da adopção da política debateram-se com alguns problemas? Quais?

Q11: Existiu resistência relativamente à adopção da política?

Q12: Foram superados esses problemas de adopção? Se sim, como? Se não, porquê?

Q13: Ocorrem problemas na aplicação da política no dia-a-dia?

Q14: Os utilizadores cumprem a política no dia-a-dia? Se não, porquê?

Q15: Há alguém responsável pela observância ou cumprimento da política? Se não, acha que faria falta alguém com essa responsabilidade?

Q16: Está satisfeito com a política de SSI? E os utilizadores, estão satisfeitos? Que razões o levam a ter essa visão?

Q17: Que factores acha fundamentais para que uma política de SSI tenha sucesso no âmbito de uma Câmara Municipal Portuguesa?

Guião 2 – Câmaras que não têm uma política de SSI, mas estão em processo de formulação

Q1: Esta Câmara Municipal está em processo de formulação e adopção de uma política de SSI, como está a ser formulada?

Q2: Como vai ser implementada a política de SSI?

Q3: Considera que a adopção de uma política de SSI pela Câmara trará benefícios/será útil? Porquê? Quais? Os outros elementos da Câmara partilham da sua opinião?

Q4: Quem detectou a falta de uma política? Que razões levaram à formulação da política? Essas razões já se faziam sentir há algum tempo ou não?

Q5: Que factores condicionaram o início do processo de adopção da política de SSI?

Q6: Quem está a elaborar a Política de SSI?

Q7: Vai existir uma única política global ou vão existir várias políticas parciais? Porquê?

Q8: Que métodos estão a ser usados na sua formulação?

Q9: Sobre quem vai recair a responsabilidade da sua implementação?

Q10: Onde vai ficar a política?

Q11: Quem vai ter conhecimento da política de SSI? Porquê?

Q12: Vão estar definidos os papéis e responsabilidades no documento da política? Porquê?

Q13: Vão estar definidas as sanções para o não cumprimento da política? Porquê?

Q14: A política de SSI vai ser superiormente aprovada? Em que órgão? Porquê?

Q15: Que factores acha fundamentais para que uma política de SSI tenha sucesso no âmbito de uma Câmara Municipal Portuguesa?

Guião 3 – Câmaras que não têm uma política de SSI, mas têm intenção de adoptar uma política de SSI

Q1: Esta Câmara Municipal não tem uma política de segurança, mas tem intenção de adoptar uma, porquê? Há quanto tempo têm essa intenção? Se for há pouco tempo, o que explica o aparecimento dessa intenção? Se for há muito tempo, porque é que ainda não existe uma política?

Q2: Quem detectou a falta de uma política?

Q3: Considera que a adopção de uma política de SSI será útil/trará benefícios? Porquê? Quais? Os outros elementos da Câmara partilham da sua opinião?

Q4: Porque não foi ainda iniciado o processo de formulação? Quais os condicionantes que estão a afectar o início do processo? Que soluções preconiza para superar os eventuais problemas?

Q5: Que factores acha fundamentais para que uma política de SSI tenha sucesso no âmbito de uma Câmara Municipal Portuguesa?

Guião 4 – Câmaras que não têm uma política de SSI e não têm intenção de adoptar uma política de SSI

Q1: Esta Câmara Municipal não tem uma política de segurança, nem tem intenção de adoptar uma, porquê?

Q2: Não considera uma política de SSI útil para esta Câmara Municipal? Caso considere que não, porquê? Caso considere que sim, o que seria necessário para desbloquear a situação corrente? Os outros elementos da Câmara partilham da sua opinião?

Q3: Considera que existem outros mecanismos de protecção que podem substituir os benefícios geralmente apontados para a existência de uma política de SSI?

Q4: Que medidas tecnológicas e não tecnológicas, pode uma Câmara Municipal implementar com vista à protecção do seu sistema de informação?

Q5: Que factores lhe parecem críticos para uma Câmara Municipal seja bem sucedida nos seus esforços de protecção do seu Sistema de Informação?

Os quatro guiões apresentados com as respectivas questões foram elaborados para serem utilizados conforme a inclusão da Câmara nos diferentes *Clusters*. É de referir que há questões que estão simultaneamente em mais do que um guião, pelo facto de existirem *clusters* para os quais se partilharam questões com outros *clusters*, e o tema ser para os quatro o mesmo, logo, existirem questões que devem constar de todos os guiões.

5.6.3 Análise de Dados

No que concerne às técnicas de investigação propostas, a análise de documentos foi fundamental para um melhor conhecimento das políticas de SSI existentes. Para tal, após recolha, leram-se e analisaram-se os documentos organizacionais considerados como políticas de SSI.

Essa análise documental identifica as características, as componentes e o conteúdo das políticas de SSI em estudo. Para tal, orientou-se a análise dos documentos alicerçando-a na revisão da literatura efectuada sobre políticas de SSI. Ou seja, atentou-se em aspectos como a sua dimensão, forma como está escrita, itens focados, profundidade e abrangência.

Para o caso das entrevistas, o primeiro passo para a análise dos dados foi a transcrição total e literal do seu conteúdo. Seguidamente, procedeu-se à sua codificação e posterior análise do conteúdo.

Para facilitar as tarefas de análise dos dados das entrevistas e dos documentos das políticas de SSI recorreu-se a uma aplicação de apoio à análise qualitativa de dados.

Hoje em dia, a oferta deste tipo de programas, conhecidos com o nome genérico de CAQDAS (*Computer Assisted Qualitative Data Analysis Software*), é ampla, oferecendo praticamente todos eles, as ferramentas suficientes para facilitar o trabalho do analista. Justicia [2005] defende que a selecção do programa a utilizar depende mais das preferências pessoais do analista do que das suas funcionalidades, dada a grande proximidades entre eles.

Dois exemplos são o ATLAS.ti e o NVivo (versão mais actual do Nudist). A escolha de uma destas aplicações informáticas nem sempre é fácil. Barry [1998] realizou um estudo comparativo destas duas aplicações, tendo identificado as características e diferenças entre as mesmas, com vista a auxiliar os investigadores interessados a seleccionar a aplicação adequada.

Para Barry, o Nudist tende a ganhar na estrutura sequencial, gestão de projectos e busca sofisticada, enquanto o ponto forte do ATLAS.ti reside na sua inter-conectividade e interface criativa.

O processo de análise dos dados das entrevistas e dos documentos foi feito com o programa ATLAS.ti. Este programa é vocacionado para a análise de dados qualitativos de informação escrita. Quer a informação escrita se apresente sob a forma de texto literário, entrevistas ou discursos, a aplicação ATLAS.ti revela-se útil como apoio às tarefas de análise de dados qualitativos. Embora esta aplicação possa

prestar um serviço relevante ao investigador, é forçoso ter-se presente que não substitui o trabalho que só o investigador pode realizar, nomeadamente no que concerne à codificação, relacionamento e interpretação de conceitos.

A quantidade de dados resultantes da realização de entrevistas e dos documentos foi normalmente elevada, o que tornou o processo de análise demorado e difícil. O ATLAS.ti auxiliou a organizar e analisar esses dados de uma forma mais operacional, sistemática e eficiente. Estes aspectos podem ser considerados a maior mais-valia na utilização deste tipo de software de análise qualitativa, facilitando e agilizando o trabalho mecânico do investigador.

Com vista à operacionalidade dos dados e melhor análise dos mesmos, utilizando o ATLAS.ti, utilizou-se para codificar os dados tanto das entrevistas como dos documentos das políticas um *codebook* e um *coding instructions* distintos para cada uma das situações.

A leitura dos conteúdos e tendo em conta a revisão da literatura efectuada possibilitou a identificação de distintos e significativos aspectos referentes ao conteúdo. Os referidos aspectos é que vão dando o compasso na confecção de um determinado aglomerado de códigos que no seu conjunto dá origem ao *codebook*. Na codificação das políticas de SSI aplicar-se-á o *codebook* desenvolvido por de Sá-Soares [2010], bem como as respectivas *coding instructions*. Relativamente à codificação das entrevistas elaborou-se para o efeito um *codebook* para este trabalho (cf. Apêndice G).

O principal objectivo da utilização de *codebooks* para a codificação, para além de facilitar o trabalho e o tornar mais eficaz e eficiente, ajuda a que os códigos se mantenham homogéneos ao longo de todo o estudo.

As *codings instructions* contêm um conjunto de instruções para a codificação onde são descritos os principais procedimentos com vista a uma melhor operacionalidade do trabalho de codificação. Estes documentos enunciam o que fazer como trabalho preparatório para a codificação e o trabalho de codificação propriamente dito.

Para além dos aspectos anteriormente referidos e de modo a se proceder à análise das entrevistas, e para além do apoio que a aplicação ATLAS.ti prestou na sistematização dos dados recolhidos, organizou-se a análise dos casos em estudo através da execução sucessiva das três fases seguintes:

- Análise de cada caso individual
- Análise intra-*cluster*
- Análise inter-*clusters*

A apresentação dos resultados será feita caso a caso, *intra-clusters* e *inter-clusters*, ou seja, um caso de *per si*, o caso dentro do *cluster* em que se inseria e a comparação entre os vários *clusters* existentes. Esta forma de análise vai permitir ter a percepção da realidade das Câmaras que têm políticas de SSI, das que não têm, mas que estão em fase de adopção de uma, das que não têm nenhuma política, mas que têm intenção de um dia adoptarem uma e das que não têm política e que não querem

adoptar nenhuma. A comparação e interligação entre cada realidade serão igualmente efectuadas.

Esta forma de análise permite um termo de comparação, conforme as diferentes perspectivas existentes em cada um dos *clusters*, tornando assim o estudo mais completo.

Com vista a uma melhor estruturação e articulação do trabalho, e tal como se avançou anteriormente, de modo a potenciar a obtenção de resultados mais frutíferos recorreu-se ao enquadramento para a análise da mudança proposto por Walsham [1993]. Conforme se explanou, este enquadramento é composto por três dimensões fundamentais: conteúdo, processo e contexto. A Tabela 18 apresenta as dimensões do enquadramento da investigação, assim como os aspectos inerentes a cada uma dessas dimensões.

Dimensão	Descrição
Conteúdo	**Características das Políticas de SSI** • Dimensão do documento, nível de abstracção, durabilidade, linguagem, formato, suporte, etc. **Componentes das Políticas de SSI** • Objectivos, declarações gerais de metas, responsabilidades, sanções, contactos, data, proibições, permissões, etc.
Processo	**Formulação das Políticas de SSI** • Caracterização do processo de formulação de uma política de SSI. • Factores condicionadores da formulação de uma política de SSI. **Implementação das Políticas de SSI** • Caracterização do processo de implementação de uma política de SSI. • Factores condicionadores da implementação de uma política de SSI. **Revisão das Políticas de SSI** • Caracterização do processo de revisão de uma política de SSI. • Factores condicionadores da revisão de uma política de SSI.
Contexto	**Externo** • Factores económicos, políticos e legais no âmbito das Câmaras Municipais que influenciam a adopção das políticas de SSI. **Interno** • Factores de gestão estrutural, político, social e cultural dentro das Câmaras Municipais que influenciam a adopção das políticas de SSI.

Tabela 18: Componentes de Enquadramento Contextual

5.6.4 Análise de Conteúdo

Face aos objectivos estipulados para este estudo e dado o grande volume de dados para análise, o método de análise de conteúdo foi o escolhido para a analisar esses dados.

A "análise de conteúdo" é para Ghiglione e Matalon [1997] e Stemler [2001] um método que permite aos investigadores filtrarem grandes volumes de dados com relativa facilidade de maneira sistemática.

A "análise de conteúdo" é um método de análise de texto estabelecido há mais tempo no conjunto dos métodos empíricos de investigação social [Herkner 1974, Holsti 1968, Silbermann 1974].

A literatura sobre análise de conteúdo é rica e variada, não sendo fácil apresentar-se uma compreensão homogénea e integrada deste método. Contudo algumas definições podem ser enunciadas, nomeadamente a proposta por Weber [1990] que define a "análise de conteúdo" como um método de pesquisa que utiliza um conjunto de procedimentos que permitem inferências válidas a partir de texto. Para Babbie [2010], a "análise de conteúdo" é um conjunto de técnicas de análise das comunicações, considerada como a mais comummente utilizada por investigadores em ciências sociais para analisar as transcrições de entrevistas gravadas com os participantes. Babbie [1999, p.71] expressa que "análise de conteúdo tem a vantagem de fornecer um exame sistemático de materiais em geral avaliados de forma mais impressionista". E ainda, a análise de conteúdo é uma técnica que visa a uma descrição objectiva, sistemática e quantitativa do comportamento simbólico, tendo o objecto o conteúdo da comunicação.

Outra autora, Bardin [2009], define a "análise de conteúdo" como um conjunto de instrumentos metodológicos cada vez mais subtis e em constante aperfeiçoamento, que se aplicam a "discursos" extremamente diversificados. O factor comum destas técnicas múltiplas e multiplicadas é uma hermenêutica controlada, baseada na dedução: a inferência. Enquanto esforço de interpretação, a análise de conteúdo oscila entre os dois pólos do rigor da objectividade e da fecundidade da subjectividade.

A análise de conteúdo segundo a tão citada definição de Berelson [1952] é uma técnica de investigação para a descrição objectiva, sistemática e quantitativa do conteúdo manifesto da comunicação. Para que seja objectiva, tal descrição exige uma definição precisa das categorias de análise, de modo a permitir que diferentes pesquisadores possam utilizá-las, obtendo os mesmos resultados; para ser sistemática, é necessário que a totalidade de conteúdo relevante seja analisada com relação a todas as categorias significativas; a quantificação permite obter informações mais precisas e objectivas sobre a frequência da ocorrência das características do conteúdo.

Para Merten [1983, p. 46] "a variedade de procedimentos de análise de conteúdo é enorme, quer a nível de objectivos analíticos quer dos meios ou processos

desenvolvidos para atingi-los", que segundo Titscher et al. [2000], a análise de conteúdo é, por isso, mais uma questão de uma estratégia de investigação do que de um método único de análise de texto.

A análise de conteúdo é um método diferente dos demais métodos de pesquisa porque, ao invés de entrevistar ou observar pessoas, o pesquisador lida com registos que já existem e faz inferências a partir dos mesmos.

O processo da "análise de conteúdo" inicia-se com a elaboração de um esquema de categorias constituído pelas várias unidades de análise (componentes mais pequenos de texto nos quais a ocorrência e caracterização de variáveis são examinadas) ou seja, os documentos em análise tem de ser transformada em algo passível de ser interpretável, que tenha significado para os investigadores que são, as já referidas categorias de análise. Segundo Berelson [1952] os estudos serão produtivos na medida em que as categorias sejam claramente formuladas e bem adaptadas ao problema e ao conteúdo (a analisar). Seguidamente, ao sistema de categorias estar estabelecido, pode-se iniciar a codificação.

De forma a garantir o rigor e a qualidade dos dados analisados e das conclusões da investigação, é necessário que esta possua duas características de relevo: a validade e a fiabilidade.

A validade pode ser definida como a adequação entre os objectivos e os fins sem distorção dos factos. Refere-se a qualidade dos resultados da investigação no sentido de os podermos aceitar como "factos indiscutíveis". Yin [1994] refere dois tipos de validade: Validade Interna e Validade Externa. A validade interna depende da capacidade do estudo realmente responder às questões propostas inicialmente. Ela mede até que ponto os resultados do estudo são o produto das variáveis que foram seleccionadas, observadas e medidas e não o fruto de outras variáveis que não foram tratadas. A validade externa mede até que ponto os resultados obtidos pelo estudo, podem ser generalizados para outras situações com outros indivíduos. Um estudo pode ter validade interna mas não ter validade externa. Já um estudo que não tenha validade interna nunca poder a ter validade externa.

A fiabilidade dos resultados refere o grau de confiança ou exactidão que podemos ter na informação obtida. Os resultados devem ser independentes daqueles que os produzem. Assim, os testes de fiabilidade serão para testar a fidelidade do codificador e das categorias de análise. Um conjunto de codificadores, operando sobre um mesmo texto, deve reproduzir a mesma análise. A fiabilidade é completa quando a categoria de análise não é ambígua, ou seja, permite classificar sem dificuldade a unidade de registo.

Segundo Weber [1990, p. 12] "para se fazerem inferências válidas a partir do texto, é importante que o processo de classificação seja confiável no sentido de ser coerente: Diferentes pessoas devem codificar o mesmo texto da mesma maneira".

5.7 Enquadramento Teórico para a Interpretação dos Resultados

A necessidade neste trabalho de investigação de um enquadramento teórico para a interpretação dos resultados decorrentes da análise de dados levou à selecção da teoria institucional como lente interpretativa, atendendo à natureza dessa teoria e às conexões que se crêem existir com este trabalho de investigação.

Assim, nesta secção delinear-se-á sobre os principais conceitos da teoria institucional, com destaque para a sua aplicabilidade. Sinteticamente será descrito o percurso desta teoria desde o seu aparecimento, serão definidos conceitos indissociáveis da perspectiva institucional, identificados os seus pilares e transportadores, discutidas a agência e a estruturação e por fim a sua aplicabilidade nas diferentes áreas, seguindo-se a sua aplicação potencial na área da SSI e a discussão da sua relevância para este estudo.

5.7.1 Introdução à Teoria Institucional

O institucionalismo da primeira metade do século XIX tinha uma orientação descritiva e utilizava a razão indutiva. O antigo institucionalismo de Commons [1950] considera que as instituições existentes em um tempo determinado representam soluções imperfeitas e pragmáticas dos conflitos passados. Assim, a história institucional é um processo de selecção de um conjunto de práticas institucionais sobre um conjunto de alternativas, num processo de tomada de decisão que implica o descobrimento através da investigação e a negociação do que é a melhor prática nas circunstâncias actuais de interesses organizados em conflito, para impor a sua vontade colectiva entre os grupos e sobre os indivíduos.

Foi mais tarde, em 1977, que se poderá considerar que apareceu o novo institucionalismo, com o artigo de Meyer e Rowan [1977] que desafiou as tradições teóricas e empíricas então dominantes na investigação organizacional. A análise destes investigadores foi guiada por uma ideia-chave em que as estruturas formais têm propriedades simbólicas assim como as propriedades geradoras de acção. Ou seja, as estruturas podem ser revestidas de significados socialmente partilhados, pelo que, além das funções "objectivas", como as relacionadas com a eficiência económica, podem servir para informar um público tanto interno quanto externo sobre a organização [Kamens 1977].

O papel dos valores é central ao antigo institucionalismo, mas o novo institucionalismo orienta-se mais pelos processos cognitivos. Greenwood e Hinings [1996] resumem esta alteração assinalando que o antigo institucionalismo enfatiza os termos de influência, coligação e os valores de competência, juntamente com o poder e as estruturas informais e o novo institucionalismo enfatiza a legitimidade, o envolvimento dos campos organizacionais e a centralidade da classificação, rotinas, guiões e esquemas. O novo institucionalismo presta atenção aos campos organizacionais como unidades de análise. Os processos institucionais podem dar uma certa estabilidade aos campos organizacionais, ainda que estes estejam sempre em evolução. Segundo DiMaggio e Powell [1983, p. 148], o campo organizacional refere-se àquelas organizações que, em geral, constituem uma área reconhecida da vida institucional: fornecedores chaves, recursos e consumidores de produtos,

agências reguladoras e outras organizações que desenvolvem produtos e serviços similares. A virtude dessa unidade de análise é a atenção dada a todos os actores relevantes, compreendendo a importância das conexões e da equivalência estrutural.

O novo institucionalismo segundo Powell e DiMaggio [1991, p. 8] centrado na "teoria da organização e na sociologia compreende uma rejeição dos modelos do actor-racional, reforçando, pelo contrário, um interesse pelas instituições enquanto variáveis independentes, uma viragem em direcção às explicações cognitivas e culturais e ainda uma atenção particular às propriedades das unidades supra-individuais de análise, as quais não podem ser reduzidas a agregações ou a consequências directas dos atributos ou dos motivos dos indivíduos".

Segundo Scott [2008] observa-se a maturidade alcançada pelo neo-institucionalismo, que se reflecte, para o autor, em aspectos como:

- A maior coerência do conceito de instituições nos estudos neo-institucionalistas recentes;
- A mudança de explicações dos fenómenos como produto de mecanismos deterministas em prol de explicações que incluem a capacidade de agência das organizações em relação ao ambiente institucional;
- O foco no campo organizacional como nível analítico, em contraste com a ênfase no nível organizacional;
- Ênfase na mudança institucional, em comparação com a concepção de estruturas estáticas e
- A mudança de entendimento das instituições como contraponto à racionalidade instrumental, para a sua concepção enquanto pano de fundo para a acção racional.

5.7.2 Definições

Após esta breve revisão histórica sobre a Teoria Institucional, define-se seguidamente o que se depreende por "instituição". Diversos autores avançam distintas definições, como se ilustra nas explanações subsequentes.

> As instituições são esquemas, normas e regulamentos humanamente compartimentados que permitem e constrangem a conduta dos actores sociais e tornam previsível e significativa a vida social [DiMaggio e Powell 1991; North 1990; Scott 2001].

> Instituições são as regras do jogo numa sociedade ou, mais formalmente, as restrições criadas para moldar a interacção humana e, assim, estruturar incentivos para acções de natureza política, social ou económica, na definição de Douglass North, Prêmio Nobel de Economia de 1993. As instituições podem ser formais (leis e constituições formalizadas e escritas, em geral impostas por um governo ou agente com poder de coerção) [North 1990, p. 46] e informais (normas ou códigos de conduta, formados em geral no seio da própria sociedade) [North 1990, p. 36].

> O desenvolvimento das organizações (políticas, económicas, sociais, educacionais e outras) decorre das instituições.
>
> Instituição é uma "estrutura social que tenha atingido um alto nível de elasticidade. São compostas de elementos reguladores, cognitivo-culturais e normativos que, juntamente com actividades e recursos associados, dão estabilidade e significado à vida social. As instituições são transmitidas por vários tipos de transportadores incluindo sistemas simbólicos, sistemas relacionais, rotinas e artefactos. As instituições operam em diferentes níveis de jurisdição, desde o sistema mundial até a relações interpessoais localizadas. As instituições por definição, conotam estabilidade, mas estão sujeitas a processos de mudança, quer incrementais quer descontínuos" [Scott 1995, p. 48].
>
> Uma instituição é um conjunto de hábitos estabelecidos de pensamento que são comuns à generalidade dos indivíduos [Veblen 1994].
>
> As instituições "consistem em esquemas e actividades cognitivas, normativas e reguladoras que dão estabilidade e sentido ao comportamento social" [Scott 1995, p. 33].
>
> As instituições são regras colectivas dando significado colectivo e valor a entidades particulares e actividades, integrando-as dentro de esquemas maiores [Meyer et al. 1994].

Das várias definições de "Instituição" anteriormente citadas, a que vai ser adoptada neste trabalho por se entender como a que apresenta um nível de abstracção mais baixo é a proposta por DiMaggio e Powell e North e Scott, que a definem como esquemas, normas e regulamentos humanamente compartimentados que permitem e constrangem a conduta dos actores sociais e tornam previsível e significativa a vida social.

Após esta breve súmula de traços definidores de "instituição", serão apresentadas as perspectivas de dois autores sobre o que se entende por "teoria institucional".

Segundo Scott [2004], a teoria institucional trata dos mais profundos aspectos da estrutura social, considerando os processos pelos quais as estruturas (tais como, esquemas, regras, normas e rotinas) se estabelecem como linhas orientadoras e confiáveis para o comportamento social e investigando a forma como estes elementos são criados, difundidos, adoptados e adaptados ao longo do tempo e do espaço; e a forma como eles caem em declínio e desuso.

Para o investigador Prates [2000, p. 90], a perspectiva institucional para o estudo das organizações pode ser tipificada como uma abordagem simbólico-interpretativa da realidade organizacional, apresentando uma posição epistemológica predominantemente subjectivista, na qual é salientada a construção social da realidade organizacional.

5.7.3 Pilares da Teoria Institucional

As estruturas institucionais consistem nas pressões de natureza regulativa, normativa e cognitiva, aceites no campo organizacional e que são definidas e redefinidas a partir da interpretação e interacção entre os actores, estabelecendo critérios para a legitimidade das acções. A Tabela 19 tem como principal objectivo sintetizar os três principais pilares da nova escola institucional.

Elemento Teórico	Regulador	Normativo	Cultural – Cognitivo
Base de submissão	Diligência	Obrigação social	Pressuposto Compreensão partilhada
Base da ordem	Regras reguladoras	Expectativas associadas	Esquemas constitutivos
Mecanismos	Coercivo	Normativo	Mimético
Lógica	Instrumentalidade	Adequação	Ortodoxia
Indicadores	Regras Leis Sanções	Certificação Acreditação	Crenças comuns Lógicas de acção partilhadas Isomorfismo
Afecto	Medo/Culpa/ Inocência	Vergonha/Honra	Certeza/Confusão
Base de legitimidade	Sancionado legalmente	Governada moralmente	Compreensível Reconhecível Sustentada culturalmente

Tabela 19: Três Pilares das Instituições
Adaptado de Scott [2008, p. 51]

O pilar regulador constrange e regula o comportamento por meio de regras, sanções e punições de maneira formal. Assim sendo, a legitimidade das acções dos actores está associada ao cumprimento destes requerimentos [Scott 1995].

No pilar normativo a ênfase é colocada numa base moral, mais profunda de legitimação. São enfatizados os valores e normas, como elementos capazes de pressionar a acção organizacional, transformando-se, pela utilização quotidiana, em uma obrigação social. A acreditação, dessa forma, é um mecanismo de funcionamento da organização. A lógica, então, é a da adequação, pois os valores e normas são interiorizados [Scott 1995].

As estruturas culturais-cognitivas também sustentam significados que são partilhados entre os actores acerca das estruturas regulativas e normativas, ou seja, da realidade que cerca os actores, que constroem e continuamente negoceiam a realidade social, num contexto que contempla estruturas simbólicas, objectivas e externas que oferecem orientação. As estruturas culturais-cognitivas representam modelos de comportamento individual com base na subjectividade e em compreensões internalizadas, frutos da interpretação da realidade social em que se actua, servindo como categorias aplicadas para o pensar e para o agir, bem como de base para a construção da identidade dos actores [Scott 1995].

Este terceiro pilar, segundo Berger e Luckmann [2001], é onde se ancora o Novo Institucionalismo, dado realçar a importância das interpretações subjectivas das acções, ou seja, são valorizados os símbolos e significados, a dimensão subjectiva da realidade social. A legitimidade é evidenciada como advinda da adopção de uma estrutura comum de referência ou definição da situação. Os adeptos dessa abordagem entendem as organizações, então, como uma realidade socialmente construída.

5.7.4 Transportadores

As instituições definem-se como sistemas compostos por elementos reguladores, normativos e cognitivo-culturais que actuam para dar sentido, significado, estabilidade e ordem. Os elementos institucionais mudam de lugar para lugar e de tempos a tempos com o auxílio de "transportadores". Distinguem-se quatro tipos de transportadores – sistemas simbólicos, sistemas relacionais, rotinas e artefactos. Segundo Scott os transportadores não são veículos neutros, mas têm efeitos importantes nos elementos transmitidos [Scott 2003, p. 879].

Os quatro tipos de transportadores identificados são transversais aos três pilares, o que permite a sua comparação, conforme se ilustra na Tabela 20. As teorias variam não apenas de acordo com os elementos que favorecem, mas também de acordo com o tipo de transportadores que enfatizam. Os enquadramentos institucionais diferem em relação aos tipos de elementos centrais e aos tipos de transportadores a utilizar. Eles apontam um conjunto de mecanismos fundamentais que permitem determinar como as ideias evoluem através do espaço e do tempo e quem, ou o quê, os transporta [Scott 2008, p. 79].

	Pilares		
	Regulador	**Normativo**	**Cultural-Cognitivo**
Sistemas Simbólicos	Regras Leis	Valores Expectativas	Categorias Tipificação Esquemas
Sistemas Relacionais	Sistemas de governação Sistemas de poder	Regimes Sistemas de autoridade	Isomorfismo estrutural Identidades
Rotinas	Protocolos Procedimentos operacionais normalizados	Profissões Papeis Obediência no dever	Guiões
Artefactos	Objectos concordantes com especificações dadas	Objectos que vão de encontro a convenções e normas	Objectos que possuem valor simbólico

Tabela 20: Transportadores e Pilares Institucionais
Adaptado de Scott [2008, p. 79]

5.7.5 Isomorfismo

Embora existam diversas escolas do pensamento dentro da perspectiva institucional, muita literatura utiliza o conceito de isomorfismo para explicar a forma como as características organizacionais são modificadas para aumentar a competitividade com as características ambientais [DiMaggio e Powell 1983; Rowan 1982]. O isomorfismo pressupõe que as organizações respondam de maneira similar a outras que estão de alguma forma ajustadas ao ambiente. Através do isomorfismo, as organizações assimilam regras institucionais, tornando-se mais homogéneas dentro do seu campo organizacional.

Segundo DiMaggio e Powell [1983], o isomorfismo institucional é a razão dominante pela qual as organizações assumem determinadas formas. O isomorfismo é um conjunto de restrições que forçam uma unidade de uma população a parecer-se com outras unidades que se colocam num mesmo conjunto de condições ambientais. Tal abordagem sugere que as características organizacionais são modificadas na direcção do aumento de compatibilidade com as características ambientais, o número de organizações numa população, em função da capacidade ambiental projectada e a diversidade das formas organizacionais é isomórfica à diversidade ambiental.

Os investigadores DiMaggio e Powell [1983] asseveram que existem dois tipos de isomorfismo entre as organizações: o competitivo e o institucional, conforme identificado na Figura 16.

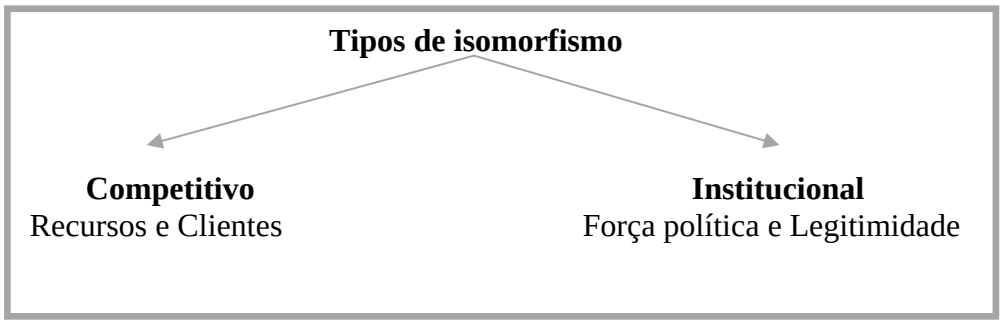


Figura 16: Tipos de Isomorfismo nas Organizações
Adaptado de DiMaggio e Powell [1983]

O isomorfismo competitivo explica a busca por um lugar no mercado, por recursos e por clientes; mas não é suficiente, na visão dos autores, para explicar o moderno mundo das organizações. Nesse sentido, é o estudo do isomorfismo institucional que deve ser aprofundado, pois as “organizações competem não somente por recursos e clientes, mas por força política e legitimidade institucional, por conveniência social como económica” [DiMaggio e Powell 1983, p. 150].

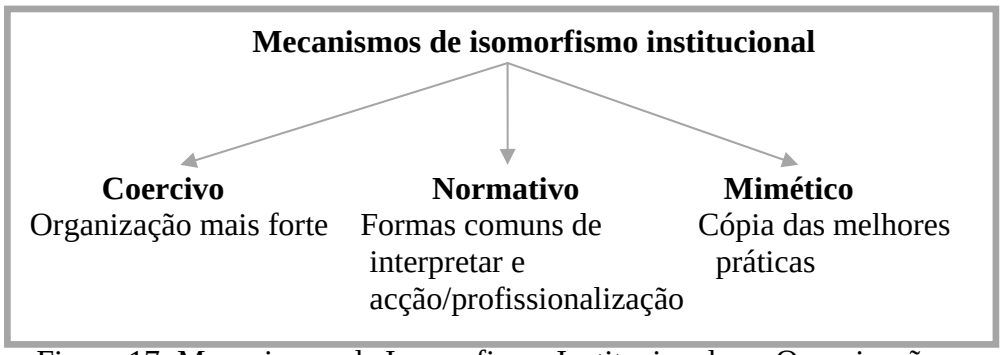


Figura 17: Mecanismos de Isomorfismo Institucional nas Organizações
Adaptado de DiMaggio e Powell [1983]

Assim, conforme se ilustra na Figura 17, os autores identificam três mecanismos por meio dos quais ocorrem as mudanças visando à homogeneidade nas organizações, cada qual com seus próprios antecedentes:

- Isomorfismo coercivo – Consiste nas pressões para a conformidade, exercidas através de padrões, regulamentos e semelhantes, como em empresas aéreas que operam sobre rigorosas regras de segurança, facto que causa certas uniformidades na estrutura estratégica [Mintzberg et al. 2000].

  De acordo com DiMaggio e Powell [1983] o isomorfismo coercivo é o resultado de pressões formais e informais exercidas por uma organização sobre outra que se encontra em condições de dependência, bem como autoridade. Por exemplo, são as regulamentações governamentais e as leis capazes de impor uniformidade às organizações.

- Isomorfismo normativo – Resulta da forte influência da perícia profissional. As organizações contemporâneas são, muitas vezes, dominadas por especialistas que incorporam as suas próprias normas profissionais às tomadas de decisões [Mintzberg et al. 2000].

  Reportando-se ao isomorfismo normativo, DiMaggio e Powell [1983] apontam que o grau de profissionalização é possivelmente o factor mais importante como mecanismo normativo a ser considerado para o entendimento das pressões normativas do ambiente, podendo ser resultante da educação formal ou da formação e manutenção de redes de trabalho.

  O isomorfismo por mecanismo normativo refere-se, principalmente, a formas comuns de interpretação e de acção frente aos problemas que se põem em evidência na vida organizacional.

- Isomorfismo mimético – Consiste em copiar as melhores práticas dos concorrentes, pois com essa prática as organizações buscam mostrar aos outros de que também estão na vanguarda das melhores práticas [Mintzberg et al. 2000].

> Este mecanismo de isomorfismo ocorre quando uma organização, por razões diversas, adopta os procedimentos e práticas que já foram desenvolvidos e provados em outras organizações que pertencem ao seu ambiente específico. Assemelha-se, em certa medida, à prática conhecida no mercado como *benchmarking*.

5.7.6 Agência e Estruturação

Ao longo da história das ciências sociais, segundo Scott [2008, p. 76], "houve uma tensão entre aqueles teóricos que defendem impedimentos estruturais e culturais na acção e aqueles que defendem a capacidade de actores individuais para 'marcar a diferença' no fluxo dos acontecimentos. Esta é uma versão da antiga antinomia entre liberdade e controlo". A teoria institucional tem privilegiado a continuidade e a restrição na estrutura social, mas isso não impede de ter em atenção as formas pelas quais os actores individuais agem para criar, conservar e transformar instituições.

Os primeiros teóricos neo-institucionais, tais como Meyer e Rowan [1977], DiMaggio e Powell [1983] e Meyer e Scott [1983], tinham tendência a dar ênfase à forma como os mecanismos institucionais restringiam as estruturas e as actividades organizacionais. No entanto, trabalhos mais recentes, como por exemplo o trabalho de DiMaggio [1991], Powell [1991] e Scott [Scott et al. 2000], dão mais atenção à forma como tanto os indivíduos como as organizações inovam, agem estrategicamente e contribuem para a mudança institucional [Christensen et al. 1997; Oliver 1991].

Ainda segundo Scott [2008] muitos enquadramentos teóricos tratam a liberdade e a restrição como ideias opostas, obrigando a que se "tome partido" – privilegiar um valor social ou outro. Todavia, desenvolvimentos recentes na teoria sociológica permitem ver estes dois elementos chave como processos interligados e compatíveis. Em concreto, o trabalho de Giddens [1979, 1984] sobre a "estruturação" forneceu um enquadramento produtivo para examinar a inter-relação entre estas duas fontes.

Embora "estruturação" seja uma palavra bastante inadequada, o termo, definido por Giddens [1984], relembra que a estrutura social envolve a padronização das actividades e relações sociais através do tempo e do espaço. As estruturas sociais só existem enquanto actividades sociais padronizadas, englobando regras, relações e recursos reproduzidos ao longo do tempo. Giddens [1984, p. 25] visionou o que denominou de "dualidade da estrutura social", reconhecendo-a como sendo tanto o resultado como a plataforma da acção social. As estruturas sociais mostram um duplo papel na medida em que são "tanto o meio como o resultado das políticas que organizam de modo repetitivo". Os actores individuais desempenham acções que são simultaneamente restringidas (nalgumas direcções) e encorajadas (noutras) pelas estruturas sociais existentes. No modelo de Giddens [1984, p. 21], as estruturas sociais são feitas de regras – "procedimentos generalizados, aplicados na acção/reprodução da vida social" – e recursos – tanto humanos como não humanos, "que podem ser usados para dar e conservar poderes" [Sewell 1992, p. 9]. As instituições são o tipo de estrutura social que envolve regras mais sólidas apoiadas por relações mais fortes e recursos mais fortemente estabilizados. As práticas

institucionais são “aquelas profundamente entranhadas no tempo e no espaço” [Giddnes 1984, p. 13].

Na Teoria da Estruturação de Giddens [1984] são evitadas posições extremas, argumentando que embora as pessoas não sejam inteiramente livres de escolher as suas próprias acções, e o seu conhecimento seja limitado, no entanto, são a agência que reproduz a estrutura social e conduz a mudança social. Este investigador define que a conexão entre a estrutura e a acção é um elemento fundamental da teoria social, a estrutura e a agência são uma dualidade que não pode ser concebida para além de uma ou outra e seu principal argumento é contido na sua expressão "dualidade da estrutura".

Segundo Giddens, a acção e a estrutura não podem ser analisadas separadamente. Na realidade, uma vez que as estruturas são criadas, mantidas e alteradas por meio de acções, a atribuição de forma e significado às acções acontece tendo como pano de fundo a estrutura, pelo que a linha de nexo causal evolui nos dois sentidos, tornando impossível determinar o que está mudando o quê.

Estruturação significa, para Giddens [1984], que as relações que se formaram na estrutura podem existir “fora do tempo e do lugar”, por outras palavras, independentemente do contexto em que são criadas. Um exemplo é a relação entre professor e aluno: quando se cruzam num outro contexto, por exemplo na rua, a hierarquia entre eles mantém-se.

Segundo Scott [2008], a teoria da estruturação vê os actores como criadores e seguidores de regras e utilizadores de recursos na medida em que eles estão envolvidos na constante produção e reprodução de estruturas sociais. Os actores são vistos como conhecedores e reflexivos capazes de entender situações diárias e de monitorizar de forma rotineira os resultados das suas próprias acções e das dos outros.

As relações e as tensões que constituem agência e estrutura configuram o problema básico da moderna teoria social [Archer 1988; Giddens 1979; Ortner 1997]. A teoria social contemporânea estuda as condições na organização de sistemas sociais que governam as interconexões entre ambas – estrutura e agência.

Agência refere-se à capacidade de um actor ter algum efeito do mundo social – alterando as regras, os laços relacionais ou a distribuição de recursos. A presença de agência permite uma teoria de acção não determinante, “voluntária”: “ser capaz de agir de “outra forma” significa ser capaz de intervir no mundo, ou recusar tal intervenção, com o efeito de influenciar o processo específico ou o estado das coisas” [Giddens 1984, p. 14]. A agência permite a consideração do papel do poder nos processos institucionais.

Os actores, sob condições institucionais estáveis ou instáveis, não são capturadas apenas por significados partilhados nos seus campos “… em vez disso, operam com uma certa competência social para reproduzir ou contestar sistemas de poder e privilégio” [Fligstein 2001, p. 111].

Tais actores podem ser concebidos tanto a partir de um modelo de escolha racional, seguindo preferências definidas, como enquanto indivíduos cujos interesses e gostos vão mudando ou vão sendo descobertos à medida que a acção decorre. Em qualquer dos casos existe a possibilidade de mudança dos compromissos institucionais [Scott 2008].

A premissa teórica básica que suporta o conceito de agência está fortemente alinhada com os "pressupostos" fenomenológicos que envolvem as versões sociológicas do pensamento neo-institucional. Entre o contexto e a reacção está a interpretação do actor. A agência reside "nos processos interpretativos pelos quais as escolhas são imaginadas, avaliadas e contingentemente reestruturadas pelos actores num constante diálogo com as situações em desenvolvimento" [Emirbayer e Mische 1998, p. 966].

Os investigadores Emirbayer e Mische [1998, p. 962] conceptualizam agência como um processo incorporado de forma temporária de contrato social, informado pelo passado (no seu aspecto habitual ou "iterativo"), mas também orientado em direcção ao futuro (como uma capacidade "projectiva" para imaginar outras possibilidades) e em direcção ao presente (como uma capacidade "projectiva" para contextualizar hábitos passados e os projectos futuros no âmbito de contingências do momento).

A teoria da estruturação junta-se a numerosos outros argumentos teóricos para apoiar um papel mais proactivo para os actores individuais e organizacionais e uma visão dos processos institucionais mais interactivos e recíprocos. March e Olsen [1989] sublinham que as regras devem ser seleccionadas – muitas vezes mais do que uma regra pode ser aplicada – e também interpretadas – adaptadas às exigências de uma situação específica. Weick [1979, 1995] sublinha que as compreensões e os guiões emergem das acções e também as guiam, e que tais símbolos colectivos podem ser utilizados não só para justificar comportamentos passados, mas também guiar comportamentos actuais. Versões mais recentes da teoria da cultura vêem os indivíduos como desempenhando um papel activo, usando regras e recursos sociais existentes como reportório de possibilidades para construir estratégias de acção. Investigadores têm defendido uma "política de identidade" na qual indivíduos ou grupos organizados criam objectivos, identidades e solidariedades que dão significado e gerem compromissos sociais em desenvolvimento [Aronowitz 1992; Calhoun 1991; Somers e Gibson 1994]. Estes investigadores reconhecem cada vez mais até que ponto os participantes organizacionais nem sempre se conformam com os padrões convencionais, mas reagem de forma variável, por vezes criando novas formas de agir e organizar.

Todos os actores, tanto individuais como colectivos, possuem algum grau de agência, mas a quantidade da agência varia muito entre os actores e também entre os tipos de estrutura social. A própria agência é estruturada social e institucionalmente [Scott 2008, p. 78].

5.7.7 Processos Institucionais

Nesta subsecção aborda-se a forma como pode ser aplicada a teoria institucional, apresentando-se as diferentes classes que compõem o processo de aplicação da teoria

institucional, iniciando-se com a construção, ou seja, a criação institucional, seguindo-se o processo de institucionalização, com a definição das etapas que o constituem, posteriormente foca-se a mudança institucional e, por fim, as respostas estratégicas que podem ser estabelecidas pelas organizações em resposta ao ambiente institucional.

5.7.7.1 Construção

Para Scott [2008, p. 94] é um pouco arbitrário distinguir o processo envolvido na criação de instituições do utilizado para as alterar. As instituições não surgem do vácuo, desafiam sempre, pedem emprestado, e, em graus variáveis, deslocam instituições anteriores. A diferença assenta fortemente no objectivo do investigador. Se dirigir a atenção, principalmente, para o processo e condições, dando lugar a novas regras, compreensões e práticas associadas, então tem-se um estudo de criação institucional. Como Greif [2006, p. 17] assinalou "Crenças, normas e organizações herdadas do passado constituirão parte das condições iniciais nos processos que levam a novas instituições". Contudo, se o analista examina como é que um conjunto de crenças, normas e práticas é atacado, se torna "não legítimo" ou cai em desuso, para ser substituído por novas regras, formas e "*scripts*", tem-se um estudo de mudança institucional.

Segundo Greif [2006], as instituições deveriam ser consideradas como um sistema formado por componentes inter-relacionados – regras formais, crenças e normas sociais – que podem, às vezes, se agrupar de forma sistémica formando organizações. O ponto fundamental é que esses componentes ou elementos institucionais são exógenos em relação aos indivíduos por eles influenciados, apesar de endógenos à sociedade. É possível até que, em algumas formas, as regras, crenças e normas se institucionalizem como um resultado de equilíbrio. No seu conjunto, os elementos institucionais irão prover os micro-fundamentos comportamentais, permitirão, guiarão e motivarão os indivíduos em posições sociais particulares a determinadas escolhas, o que proporcionará as regularidades no comportamento observado.

Segundo Scott [2008, p. 119], de um "foco inicial dado à forma como as instituições existentes afectam as organizações, os teóricos institucionais expandiram a sua atenção às formas como as instituições são construídas. Os registos dos processos de construção variam de acordo com a importância dada ao intento e à concepção consciente, em oposição aos processos menos intencionais e mais evolutivos".

Ainda de acordo com as premissas do investigador anterior, os agentes institucionais incluem tanto actores individuais como colectivos, e estes diferem no facto de empregarem ou não ferramentas primariamente reguladoras, normativas ou culturais-cognitivas nos seus esforços de construção.

Scott [2008, p. 95] define no seu trabalho o tema dos limites da concepção institucional. Embora seja apropriado reconhecer o papel da agência na construção institucional, é importante não se atribuir qualidades heróicas àqueles que procuram criar novos quadros de referência de significado e governação. É caso frequente os actores trabalharem para criar instituições que reflictam, protejam e antecipem os seus interesses, que "os partidos precisem de instituições que ajudem a obter ganhos

provenientes da cooperação" [Weingast 2002, p. 670]. No entanto, há numerosas considerações que diminuem a capacidade dos actores atingirem os fins pretendidos.

Pierson [2004], através da ênfase na dimensão histórica dos processos sociais, oferece um resumo útil dos tipos de limitações que prejudicam as tentativas de projectar instituições:

- "Acordos institucionais específicos têm invariavelmente efeitos múltiplos" [Pierson 2004, p. 109], muitos dos quais são inesperados, não-intencionais e podem não ser bem-vindos.
- "Os *designers* institucionais podem não agir instrumentalmente" [Pierson 2004, p. 110], mas sim guiados por normas de "adequação", modas ou tentativas erradas de aplicar soluções pré-concebidas que não se adequam às circunstâncias actuais.
- "Os *designers* institucionais podem ter horizontes a curto prazo" [Pierson 2004, p. 112], enquanto que as instituições que desenvolvem têm efeitos a longo prazo que, muitas vezes, diferem daqueles que originalmente se procuravam.
- Os planos dos *designers* institucionais podem levar a efeitos inesperados porque as situações às quais se aplicam sofreram alterações.
- Os *designs* institucionais pressupõem que os actores e os seus interesses se manterão imutáveis, enquanto que, ao longo do tempo, os actores vêm e vão e os interesses mudam.

Tais preocupações deveriam tornar-nos cientes das assumpções que fazemos quando avaliamos o papel da agência, do interesse e da racionalidade na concepção das instituições. As limitações desse tipo de abordagem concentram-se, primeiramente, no facto de que nem todos os efeitos das instituições são antecipados ou previstos pelos agentes, o que impede que se entenda os resultados observados como consequências esperadas em sua criação.

5.7.7.2 Institucionalização

Desde a publicação do clássico artigo de Meyer e Rowan [1977], proliferaram análises organizacionais baseadas em uma perspectiva institucional [Tolbert e Zucker 1999]. Trabalhos sob a bandeira da teoria institucional têm investigado uma vasta gama de fenómenos, desde a expansão de políticas de pessoal [Baron et al. 1986; Edelman 1992; Tolbert e Zucker 1983] à redefinição elementar de missões e formas organizacionais [DiMaggio 1991; Fligstein 1985], passando pelo desenvolvimento de políticas nacionais e internacionais por organizações governamentais [Strang 1990; Zhou 1993].

Em 1999, Tolbert e Zucker [1999, p. 196] observavam que a abordagem institucional ainda teria que tornar-se institucionalizada. Existia pouco consenso sobre a definição de conceitos-chave, métricas ou métodos no âmbito desta tradição teórica. Ao contrário da ecologia populacional, com suas medidas padronizadas de densidade, a teoria institucional ainda não desenvolveu um conjunto central de variáveis-padrão, não tem uma metodologia-padrão de pesquisa e muito menos um conjunto de

métodos. Os estudos têm-se baseado em uma variedade de técnicas que incluem estudos de caso, regressão cruzada, modelos longitudinais de vários tipos, entre outras.

Também o novo institucionalismo tem encontrado abrigo nos estudos de estratégia e duas alternativas teóricas se apresentam para as pesquisas sobre institucionalização: considerar o contexto como instituição ou considerar a organização como instituição [Zucker 1987]. No primeiro caso, os processos de institucionalização vinculam-se ao poder coercivo da sociedade e do Estado, que formam o contexto institucional, favorecendo o isomorfismo [DiMaggio e Powel 1991]. No segundo caso, a institucionalização desdobra-se através dos grupos intra-organizacionais e dos processos internos que formam o campo organizacional. Tolbert e Zucker [1999] descrevem os processos inerentes à institucionalização de práticas e comportamentos como um conjunto sequencial de habituação, objectivação e sedimentação.

A institucionalização, para Meyer et al. [1994, p. 10] seria "o processo pelo qual um dado conjunto de unidades e um padrão de actividades são normativa e cognitivamente circunscritos e na prática tomados a *priori* como lícitos (seja em termos da lei formal, do costume ou do conhecimento)".

Os investigadores Tolbert e Zucker [1999] sugerem um processo sequencial de três etapas – denominadas habituação, objectivação e sedimentação – que possibilitam avaliar o nível ou grau de institucionalização de uma determinada realidade social. Isto poderá implicar que alguns padrões de comportamento social estão mais sujeitos do que outros à avaliação crítica, modificação e eliminação. Essas etapas, aplicadas à realidade organizacional, são expressas na Figura 18 que mostra o fluxo dos processos inerentes à institucionalização e às forças causais que são críticas em diferentes pontos do processo.

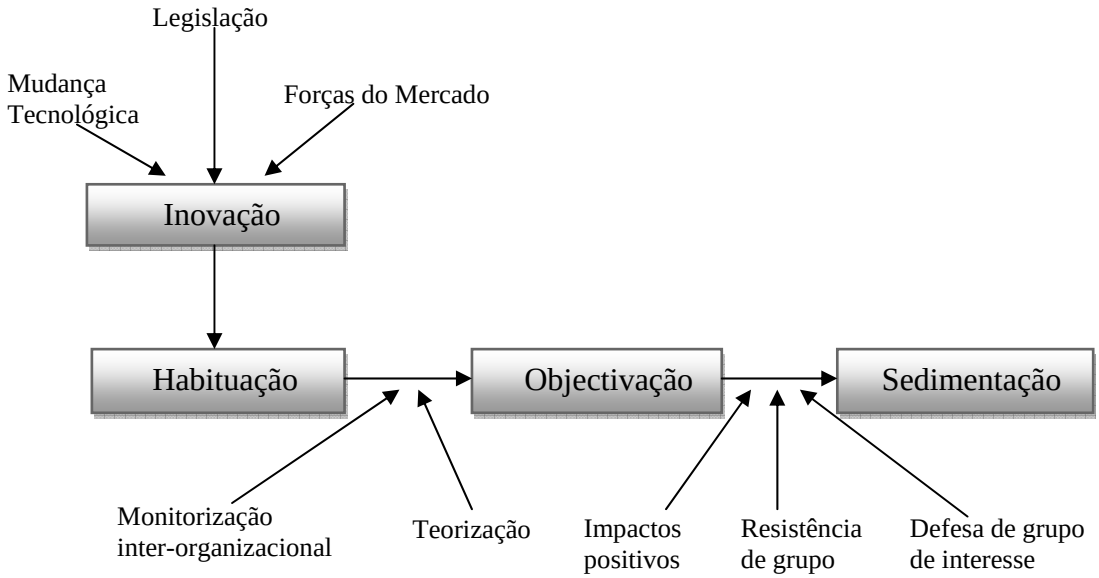


Figura 18: Processos Inerentes à Institucionalização
Adaptado de Tolbert e Zucker [1999]

O processo de institucionalização tem o seu início pela "Inovação" e ocorre em virtude de forças externas, tais como: mudanças tecnológicas, legislação ou forças do mercado. O termo inovação neste processo significa não uma melhoria de processos, produtos ou serviços, mas sim, o de rearranjos estruturais ou novas práticas organizacionais destinadas à solução de problemas das organizações.

Num contexto organizacional, o processo de "Habituação" abrange a formação de novos arranjos estruturais em resposta a problemas ou conjuntos de problemas organizacionais específicos, formalizados através de políticas e procedimentos de uma determinada organização ou um conjunto de organizações com problemas iguais ou semelhantes. Trata-se, assim, do estágio de pré-institucionalização [Tolbert e Zucker 1999].

Gerada a solução para o problema, o deslocamento em direcção a um estado mais permanente é difundido e baseia-se no processo de "Objectivação", que acompanha a difusão da nova estrutura, ampliando a sua utilização. A objectivação implica o desenvolvimento de certo grau de consenso social entre os gestores no que toca ao valor da estrutura e à crescente adopção pela organização com base nesse consenso. A objectivação pressupõe, também, o desenvolvimento de significados gerais, socialmente partilhados, tais como o uso de símbolos, ideias, imagens e vocabulário que os gestores e colaboradores decidem em comum.

Por um lado, as organizações podem utilizar evidências colhidas directamente de uma variedade de fontes (noticiários, observação directa, cotação accionista, etc.) para avaliar os riscos de adopção da nova estrutura. Na medida que se espera que os resultados da mudança estrutural se generalizem, os resultados aparentes para as organizações anteriores serão um determinante significativo da próxima decisão de adopção. Deste modo, a objectivação da estrutura é em parte uma consequência da monitorização que a organização faz dos concorrentes e de esforços para aumentar sua competitividade relativa. Reciclar "velhas invenções sociais" é uma estratégia de baixo custo, requerendo menos investimento de "recursos sociais" em relação à criação de uma nova estrutura organizacional [Tolbert e Zucker 1999].

Por implicação, a difusão de novas estruturas a uma determinada organização terá um obstáculo relativamente menor do que teria a criação de novas estruturas nesta mesma organização, porque outras organizações terão "pré-experimentado" a estrutura e a percepção dos custos e benefícios da adopção por parte dos decisores será influenciada pela observação do comportamento de outras organizações. Deste modo, quanto mais organizações tiverem adoptado a estrutura, maior probabilidade terão os decisores de perceber uma tendência favorável ao equilíbrio relativo dos custos e benefícios [Tolbert e Zucker 1999].

Estruturas que se objectivaram e foram amplamente disseminadas pela organização podem ser descritas como estando no estágio de semi-institucionalização [Silva 2007].

O estádio em que a institucionalização é total é denominado de "Sedimentação" e caracteriza-se pela "adopção da estrutura ou prática organizacional por toda a organização por um período consideravelmente longo no tempo. A sedimentação está relacionada com a continuidade histórica e, em particular, à transmissão aos

novos colaboradores. A institucionalização da estrutura ou prática organizacional depende dos efeitos conjuntos de uma relativa baixa resistência de grupos de oposição" [Silva 2007, p. 33].

A institucionalização total "ocorre com a etapa de sedimentação a qual representa um processo que fundamentalmente se apoia na continuidade histórica da estrutura e, especialmente, na sua sobrevivência pelas várias gerações de membros da organização" [Tolbert e Zucker 1999, p. 209]. Assim, envolve duas dimensões:

1) A propagação das estruturas para todos os indivíduos teorizados como adoptantes e
2) A perpetuação dessas mesmas estruturas ao longo de um tempo consideravelmente longo.

Para que o processo de institucionalização seja total é preciso que sejam identificados alguns factores que afectam tanto a difusão quanto a conservação ao longo do tempo das estruturas. Nesse sentido, Tolbert e Zucker [1999] identificam três factores principais, a saber:

1) Impactos positivos – resultados demonstráveis associados à estrutura,
2) Resistência de grupo – pessoas que são afectadas adversamente pela estrutura,
3) Defesa de grupo de interesse – pessoas que são favoráveis às mudanças na estrutura.

Percebe-se, portanto, no processo de institucionalização proposto por Tolbert e Zucker [1999] um conjunto de factores que podem determinar se uma mudança organizacional será ou não bem-sucedida.

O modelo dos processos de institucionalização apresentado por Tolbert e Zucker [1999], segundo Aidar [2003, p. 51], poderia ser complementado por uma última etapa, após a sedimentação, que seria a "Legitimação", ou o momento em que determinadas estruturas e conhecimentos são normalizados para serem transmitidos a uma nova geração. Na prática, porém, considerar a legitimação como uma última etapa no processo de institucionalização traria mais dificuldades metodológicas do que soluções, devido a duas questões. Em primeiro lugar, a institucionalização é um processo social que envolve múltiplos actores e organizações, não sendo possível identificar, na prática, o momento exacto em que a sedimentação está concluída para ser transmitida a uma nova geração, mesmo porque a própria noção do aparecimento de uma nova geração, nesse contexto, é muito subtil. Além disso, o processo de legitimação, enquanto explicação ou justificativa para uma determinada estrutura social ou organizacional, pode estar ocorrendo paralelamente em cada uma das etapas do processo de institucionalização, embora ele possa se tornar mais claro na fase de sedimentação. Assim, com o objectivo de aplicar o modelo no esquema proposto por Tolbert e Zucker [1999], é interessante considerar-se a legitimação no estádio de institucionalização completa, juntamente com o processo de sedimentação.

A Tabela 21 resume os argumentos apresentados sobre as características e consequências dos processos que compõem a institucionalização.

Dimensão	Estádio pré-institucional	Estádio semi-institucional	Estádio de total institucionalização
Processo	Habituação	Objectivação	Sedimentação
Características dos adoptantes	Homogéneos	Heterogéneos	Heterogéneos
Ímpeto para a difusão	Imitação	Imitação/ Normalização	Normativa
Actividade de teorização	Nenhuma	Alta	Baixa
Variância na implementação	Alta	Moderada	Baixa
Taxa de fracasso estrutural	Alta	Moderada	Baixa

Tabela 21: Estádios de Institucionalização e Dimensões Comparativas
Adaptado de Tolbert e Zucker [1999, p. 211]

Para os investigadores Meyer e Rowan [1992], a institucionalização não é algo planeado deliberadamente, mas envolvendo os processos através dos quais valores sociais (práticas, crenças, obrigações) assumem o estatuto de norma ou regra no pensamento e na acção social. Uma instituição é, portanto, o estádio final de um processo de institucionalização. Tolbert e Zucker [1999] discutem como se dá essa dinâmica, através de processos sequenciais (apresentados na tabela anterior), denominados: habituação, objectivação e sedimentação e os seus correspondentes estádios institucionais.

No primeiro estádio, denominado de "pré-institucionalização", muitas organizações podem adoptar uma dada estrutura, mas estas serão em pequeno número, limitadas a um conjunto de organizações similares e possivelmente interconectadas, que enfrentam circunstâncias similares e que variam consideravelmente em termos da forma pela qual a implementem. Tais estruturas não serão objecto de qualquer tipo de teorização formal [Strang e Meyer 1993], e o conhecimento da estrutura entre os que não a adoptaram – especialmente aqueles que não estão em contacto directo e frequente com os adoptantes – será extremamente limitado, em termos de operação e também de propósito [Nelson e Winter 1982].

No segundo estádio institucional definido como "semi-institucional", as estruturas que se objectivaram e que se tornaram razoavelmente difundidas podem ser descritas como estando no estádio de semi-institucionalização. Neste estádio, os adoptantes tipicamente serão bastante heterogéneos; consequentemente, o poder preditivo de determinadas características organizacionais que anteriormente se identificavam com a adopção será limitado [Tolbert e Zucker 1983]. O objectivo da difusão deixa de ser a simples imitação para adquirir uma base mais normativa, reflectindo a teorização implícita ou explícita das estruturas. Na medida que a teorização se desenvolve e se torna mais explícita, deve diminuir a variação na forma que as estruturas tomam em diferentes organizações.

O terceiro estágio, denominado de "total institucionalização" depende, segundo Tolbert e Zucker [1999, p. 15], provavelmente, dos efeitos conjuntos da baixa resistência relativa por parte de grupos de oposição, de promoção e de um apoio cultural contínuo por grupos de defensores e de uma correlação positiva com resultados desejados. A resistência provavelmente limitará a difusão da estrutura entre organizações identificadas por teóricos como adoptantes relevantes e a

promoção contínua e/ou benefícios demonstráveis são necessários para contrabalançar tendências entrópicas e, deste modo, assegurar a perpetuação da estrutura no tempo [Zucker 1988].

5.7.7.3 Mudança Institucional

Conforme se tem vindo a constatar, as mudanças tecnológicas e económicas geram mudanças no ambiente organizacional. Diante desse quadro, a busca constante por inovações apresenta-se como uma alternativa para a sobrevivência das organizações. O sucesso da organização passa a ser medido pela capacidade de sobreviver, de mudar e de antecipar as necessidades do mercado [Brown e Eisennhardt 2004]. Neste sentido, as organizações gradativamente institucionalizam práticas organizacionais para enfrentar novas realidades, que não podem ser encaradas através das práticas organizacionais até então existentes.

Por um lado, a mudança constitui um problema para os teóricos institucionais, muitos dos quais vêem as instituições como a fonte de estabilidade e da ordem. Se a natureza dos actores e dos seus modos de acção são constituídos e restringidos pelas instituições, como podem estes actores mudar as instituições nas quais estão envolvidos? Por outro lado, muita teoria e investigação sobre as instituições foca-se na mudança: a criação de novas formas institucionais e mudanças associadas nos campos organizacionais, nas populações e organizações individuais, já que estas entidades respondem a pressões para adoptar novas estruturas ou práticas [Scott 2008, p. 195].

Para Scott [2008], a ênfase tem estado na construção institucional e nos processos de mudança convergentes. Esta ênfase pressupõe que as instituições são construídas e depois exercem e provocam os seus efeitos, mas não estão sujeitas a mais mudanças. Apenas nas últimas duas décadas, os teóricos e os investigadores começaram a examinar argumentos e situações envolvendo mudança institucional que dá testemunho da desinstitucionalização das formas existentes e da sua substituição por novos acordos, que, no tempo, sofrem institucionalização. Utilizando a linguagem de Giddens, os institucionalistas têm focado a sua atenção em processos de estruturação, mas têm negligenciado processos que levam à desestruturação e à reestruturação [Scott 2008, p. 196].

A investigadora Oliver [1992] considera que, dadas condições específicas, o comportamento organizacional e a mudança não poderão ser explicados pelo consenso social existente em torno do significado e valor de uma actividade, nem pela conformidade às pressões institucionais, mas pela percepção de que aquela prática exercida pelas organizações não atende mais às necessidades actuais das mesmas, não havendo, neste sentido, o desejo ou habilidade das organizações em manter ou continuamente recriar a actividade organizacional institucionalizada.

Oliver [1992] aponta quatro razões para justificar a importância do estudo da desinstitucionalização e as suas causas:

- Poder explicar mudanças organizacionais negligenciadas pela perspectiva institucional, como desafios ao *status quo* institucional, abandono de hábito

ou costumes e a deterioração do consenso organizacional sobre uma prática ou actividade;

- Questionamento da estabilidade e longevidade de valores e práticas institucionalizadas, considerando que podem ser sujeitas a desafios, reavaliações ou rejeições;
- Apontar as condições sob as quais as pressões institucionais para conformidade falham no alcance de seus efeitos esperados e
- Analisar os factores não institucionalizados que moldam as respostas das organizações às pressões institucionais.

Nesse sentido, a referida investigadora apresenta as pressões políticas, instrumentais e sociais como ferramentas institucionais para explicar as razões que desencadeiam o processo de desinstitucionalização e as pressões para inércia e entropia, sendo que o primeiro dificulta o processo e o segundo acelera. A entropia organizacional enfatiza a tendência natural à erosão do fenómeno institucional, já a inércia supõe que os valores e actividades institucionalizadas exibirão uma resistência inevitável à erosão e mudança [Oliver 1992, p. 580].

Para compreender adequadamente as determinantes, os mecanismos e os efeitos de uma mudança institucional significativa – ou de uma estabilidade – exige que se dê atenção a períodos de tempo mais longos. Os campos de organização variam consideravelmente entre si e ao longo do tempo. O conceito de estruturação de campo fornece um quadro de referência analítico, permitindo aos investigadores avaliar as diferenças entre campos e traçar o percurso das mudanças que ocorreram ao longo do tempo no que se refere à coerência cultural do campo e à natureza das suas características estruturais [Scott 2008, p. 208].

5.7.7.4 Respostas Estratégicas

Não existem dúvidas quanto ao impacto que as instituições exercem sobre as organizações. Do consentimento até à manipulação das instituições, é amplo o leque de possíveis comportamentos que as organizacionais podem exibir. No que respeita à teoria institucional, Oliver [1991] esclarece que a preocupação central dos seus autores está nas pressões e coações vindas do ambiente institucional.

A investigadora Oliver [1991] sublinha que diversos tipos de comportamentos estratégicos podem ser estabelecidos pelas organizações em resposta ao ambiente institucional. Cinco tipos de respostas estratégicas são propostos: Concordância, Compromisso, Fuga, Desafio e Manipulação. A cada estratégia foram associadas três táticas. A Tabela 22 sintetiza quais as possíveis respostas das organizações, bem como as táticas seguidas.

Estratégias	Táticas	Exemplos
Concordância	Hábito	Seguir normas invisíveis e tidas como verdadeiras
	Imitação	Imitação de modelos institucionais
	Obediência	Obediência a regras e aceitação de normas
Compromisso	Equilíbrio	Equilibrar as expectativas de múltiplos actores
	Pacificação	Apaziguar e acomodar elementos institucionais
	Negociação	Negociar com grupos de interesses institucionais
Fuga	Ocultação	Disfarçar não-conformidade
	Protecção	Livrar-se de ligações institucionais
	Saída	Mudar objectivos, actividades ou domínios
Desafio	Rejeição	Ignorar normas e valores explícitos
	Recusa	Contestar regras e requerimentos
	Ataque	Atacar origens de pressões institucionais
Manipulação	Importação	Importar actores influentes
	Influência	Dar forma a valores e critérios
	Controlo	Dominar actores e processos institucionais

Tabela 22: Respostas Estratégicas a Processos Institucionais
Adaptado de Oliver [1991, p. 152]

A primeira estratégia, "Concordância", refere-se ao consentimento das organizações às pressões institucionais e incluem o hábito, a imitação e a obediência. Por hábito entende-se a aderência inconsciente ou cega a regras ou valores pré-conscientes. Nesse caso, as organizações reproduzem acções e práticas do ambiente institucional que se tenham tornado historicamente repetidas ou convencionais. A imitação corresponde ao conceito de isomorfismo mimético e ocorre em situações nas quais uma organização – consciente ou inconscientemente – mimetiza modelos institucionais provenientes de organizações bem-sucedidas ou conselhos de firmas de consultoria ou ainda de associações profissionais. Por sua vez, obediência é a submissão consciente a valores, normas ou requisitos institucionais. Por ser consciente, é considerada mais activa do que hábito ou imitação à medida que uma organização – consciente e estrategicamente – escolhe obedecer a pressões institucionais em antecipação a benefícios específicos que podem variar de apoio social a recursos ou previsibilidade.

A segunda estratégia proposta por Oliver [1991] é denominada de "Compromisso" e é representada por uma concordância parcial com os padrões estabelecidos. Procura estar conforme os padrões institucionais, desde que os interesses do grupo ou da organização sejam preservados. O compromisso é composto pelas seguintes táticas: equilíbrio, pacificação e negociação. Equilíbrio refere-se à acomodação de múltiplas procuras em resposta a pressões institucionais e expectativas. É, portanto, a tentativa organizacional de alcançar equilíbrio entre múltiplos grupos e interesses internos. A pacificação também constitui conformidade com as expectativas de um ou mais actores. Uma organização que aplique tácticas de pacificação tipicamente enquadra um nível menor de resistência a pressões institucionais, e devota a maior parte de suas energias para tornar plácido a fonte institucional à qual tem resistido. A tática de negociação, por sua vez, é uma forma mais activa de compromisso do que a pacificação. Segundo Oliver [1991], essa táctica envolve o esforço da organização para exigir algumas concessões de um actor externo em suas procuras ou expectativas.

A terceira estratégia para resposta a processos institucionais é a “Fuga”, sendo definida como a tentativa organizacional de impossibilitar a necessidade da conformidade. As organizações conseguem esconder a sua não-conformidade, protegendo-se das pressões institucionais ou escapando das regras ou das expectativas institucionais. As táticas da evasão são: ocultação, protecção e saída. A primeira táctica (ocultação) envolve disfarçar não-conformidade por trás de uma fachada de aquiescência. Protecção diz respeito à tentativa organizacional de reduzir o grau pelo qual ela é externamente inspeccionada, escrutinada ou avaliada. Isso é feito através da separação parcial de suas actividades técnicas de contacto externo. A terceira táctica de fuga é a mais dramática pois envolve um escape, ou seja, uma organização pode sair de um domínio dentro do qual a pressão é exercida. Pode, ainda, alterar os seus objectivos ou domínio de actuação para evitar a necessidade de conformidade em geral. Muitas empresas que escolheram o Terceiro Mundo para instalar suas fábricas recorreram à saída como tática para evitar pressões institucionais.

A quarta estratégia proposta por Oliver [1991] é o “Desafio” que é uma forma mais activa de resistência aos processos institucionais. O desafio utiliza as táticas de rejeição, recusa e ataque. Rejeição é uma opção estratégica que as organizações exercem, mais provavelmente, quando o poder de coação externo de regras institucionais é percebido como baixo ou quando objectivos internos são divergentes ou muito conflituantes com requisitos ou valores institucionais. Nesses casos, a organização opta por ignorar tais regras e valores. A segunda táctica (recusa) é um processo mais activo e tem mais sentido quando pode ser reforçado por demonstrações de probidade ou de racionalidade organizacional. A terceira táctica da estratégia desafio é o ataque e diferencia-se da anterior pela intensidade e agressividade da actividade organizacional face a pressões e expectativas institucionais. Ao usar o ataque, uma organização tenta agredir, menosprezar ou veementemente denunciar valores institucionalizados e os actores externos que os expressam.

Por último, a quinta estratégia apresentada por Olíver [1991] é a “Manipulação”, que é a resposta mais activa a essas pressões, utilizando as tácticas de importação, influência e controlo. A manipulação pode ser definida como a tentativa propositada e oportunista de influenciar ou controlar pressões e avaliações institucionais. A primeira táctica (importação) pretende neutralizar a oposição institucional e aumentar a legitimidade. O uso oportunista de elos institucionais é revelado em processos de construção de coligações e no uso estratégico de laços institucionais para demonstrar o mérito e a aceitabilidade da organização a outros actores externos dos quais espera obter recursos e aprovação. Táticas de influência podem ser geralmente mais direccionadas a valores e crenças institucionalizadas ou definições e critérios de práticas ou desempenho aceitáveis. A tática de controlo, por sua vez, é um esforço específico para estabelecer poder e dominância sobre actores externos que estão aplicando pressão sobre a organização. O objectivo, nesse caso, é dominar mais do que influenciar, modelar ou neutralizar fontes institucionais. Oliver (1991) explica que o uso de tácticas de controlo é mais provável quando as expectativas institucionais são incipientes, localizadas ou fracamente promovidas.

Conforme Oliver [1991] sugere, as organizações respondem de modo diferente ao ambiente mediante a formulação de acções estratégicas, que variam desde a conformidade até a resistência, de acordo com as pressões contextuais que pendem

sobre elas, além da sua capacidade interna e dos motivos que geram tais pressões, de quem as exercem, do tipo de pressões, de como, por quais meios e onde são exercidas.

5.7.8 Aplicações da Teoria Institucional em SI e em SSI

A teoria institucional é uma das teorias actualmente usadas na análise organizacional [Weick 2003]. Também do domínio dos sistemas de informação se verifica a existência de um número considerável de estudos com diferentes campos de aplicação. Nesta secção procurar-se-á apontar alguns dos estudos mais ilustrativos nesse domínio e, posteriormente, localizar-se-á a revisão de literatura sobre a aplicação da teoria institucional no campo da segurança de sistemas de informação.

Orlikowski [1992] analisou a relação entre tecnologia e organização, destacando diferentes visões desse relacionamento. Essa autora propôs uma visão inovadora do tema, partindo da discussão dos primeiros estudos disponíveis até chegar ao seu modelo de análise. Para tal, fez uma caracterização do conceito da tecnologia baseada em dois aspectos: propósito – definido como a tecnologia contida, ou hardware, e papel ou função – que corresponde à interacção entre tecnologia e organização.

Segundo Orlikowski [1992], a evolução dos estudos mostra que na associação entre tecnologia e organizações a princípio a tecnologia era vista como força externa que tinha impacto determinístico sobre a estrutura organizacional. Mais tarde, os investigadores focaram-se no aspecto humano da tecnologia, vendo esta como o resultado de uma escolha estratégica e da interacção social. Sugere-se então neste estudo uma nova conceitualização da relação, considerando que esta se dá com base numa interacção daquelas duas visões, sugerindo a noção de dualidade da tecnologia. A tecnologia “é criada e mudada pela acção humana, e é também usada pelos humanos para concluir algumas acções" [Orlikowski 1992, p. 215].

Essa dualidade da tecnologia, proposta por Orlikowski [1992, p. 401; 1995, p. 426], por ser entendida como uma extensão da Teoria da Estruturação de Giddens [1984]. Por estruturação, Giddens (1984) compreende o processo de intermediação prática entre acção e estrutura. Giddens não faz, porém, nenhuma menção ao papel das tecnologias da informação no jogo das inter-relações entre estrutura e acção. Orlikowski [1995] estende a teoria de Giddens, propondo a inter-relação entre os três pólos (Estrutura, Acção e TI).

Premkumar et al. [1997] desenvolveram um estudo onde aplicam a teoria institucional para examinar o impacto de vários factores ambienteis, organizacionais e tecnológicos e a adopção da inovação no contexto de troca electrónica de dados na indústria transportadora. Esses autores identificaram 11 variáveis, pertencentes a três grandes categorias – ambientais, organizacionais e inovação – que poderiam influenciar potencialmente a adopção da troca electrónica de dados.

Outros autores que apresentaram um estudo com base na teoria institucional foram Chatterjee et al. [2002]. O estudo destes autores assenta na teoria institucional e emprega visões conceptuais de estruturar e meta-estruturar acções para explicar a importância de três factores – competição de gestão de topo, raciocínio de investimento estratégico e extensão da coordenação – ao alcançar níveis mais

elevados de assimilação da Web numa organização. Os autores usaram os dados recolhidos através de um questionário para testar uma rede monológica de relações entre estes factores e a extensão da assimilação organizacional das tecnologias da Web. Segundo Chatterjee et al. [2002, p. 82], "à medida que cada vez mais empresas contemporâneas procuram transformar as suas actividades de cadeias de valores e estratégias negociais, através da assimilação de tecnologias da Web, há um desejo de perceber quais os factores que melhor promovem níveis mais elevados de assimilação da tecnologia". Recorrendo às perspectivas da teoria institucional, esta investigação examina o significado dos três factores em estudo, com vista a promover uma maior assimilação daquelas tecnologias.

Outra investigação que merece ser destacada dentro deste contexto é a dos autores Teo et al. [2003], que apresentaram um estudo que usou a teoria institucional como lente para perceber os factores que permitem a adopção de sistemas inter-organizacionais. Este trabalho estabelece que pressões miméticas, coercivas e normativas que existem num ambiente institucionalizado podem influenciar a predisposição organizacional em direcção a uma ligação inter-organizacional baseada em TI. Os resultados deste estudo mostram que as três pressões têm uma influência significativa na intenção das empresas em adoptar a troca electrónica de dados financeiros.

Um último trabalho que se entende ilustrativo da aplicação da teoria institucional no domínio dos sistemas de informação foi conduzido por King et al. [1994]. Para estes autores, a inovação em TI "está bem estabelecida em países desenvolvidos, recém-industrializados e países em desenvolvimento através da criação de intervenções governamentais para acelerar a inovação em TI dentro das suas fronteiras. A falta de uma política coerente de aconselhamento para a criação de políticas governamentais para as TI é sinal de um défice de investigação na compreensão do papel do governo perante as instituições de forma mais ampla, de inovação em TI" [King et al. 1994, p. 139].

No estudo em análise, King et al [1994] avançam três argumentos principais. O primeiro reconhece a insuficiência das perspectivas intelectuais em matéria de inovação da economia neoclássica e teoria da organização para explicar a dinâmica de mudança real inovadora no sector das TI. Os autores contrapõem que uma visão mais ampla adoptada da história económica e do novo institucionalismo em Sociologia fornece uma base mais forte para a compreensão do papel das instituições de inovação em TI. O segundo funda-se na defesa de que a intervenção institucional de inovação em TI pode ser construída no cruzamento da influência e poderes de regulação das instituições e as ideologias da oferta e da procura de modelos de inovação. O terceiro realça que a formação política institucional sobre a inovação em TI é facilitada por uma compreensão do papel multifacetado das instituições no processo de inovação e sobre as contingências que regem qualquer mistura instituição/inovação. Segundo Nelson e Soete [1988], entidades governamentais estão claramente entre as forças institucionais mais poderosas que afectam a inovação.

Os exemplos anteriormente apresentados, seleccionados de um número considerável de estudos, ilustram como a teoria institucional tem vindo a ser aplicada no domínio de investigação dos sistemas de informação.

Centrando agora a atenção no campo da Segurança de Sistemas de Informação, Björck [2004] observa que, globalmente, a investigação realizada nesse campo tem sido pouco fundada em teorias. Da sua investigação, que envolveu a análise de 5000 artigos científicos, Björck concluiu que nenhuma das teorias abordadas nesses artigos, com excepção à que Porter denomina de "teoria da gestão do conhecimento", diz respeito ao conhecimento social – que é exactamente o que trata a Gestão da Segurança de Sistemas de Informação e Tecnologias de Informação. Apesar da lente teórica institucional se aplicar no domínio genérico dos sistemas de informação, conforme se procurou realçar anteriormente, Björck não encontrou utilização habitual de teorias, institucionais ou outras, no que respeita à SSI.

Segundo Björck [2004], a teoria dos sistemas tem sido aplicada a todos os métodos de análise na segurança de SI/TI – dos *bits* e *bytes* dentro do sistema informático, passando pelas pessoas e suas acções, até às entidades supra-nacionais. O seu ponto forte é o facto de ser genérica – não interessa se desejamos analisar uma máquina ou um homem. Mas isto também é a sua maior desvantagem. Por contraponto, a teoria institucional é mais específica no que toca à sua área de aplicação, só é aplicável às unidades de análise que demonstrem algum tipo de comportamento social, o que exclui os sistemas informáticos.

Muitas empresas e organismos públicos criam sistemas de gestão de segurança da informação ambiciosos, contendo políticas de SSI e procedimentos de segurança da informação. Contudo, os documentos resultantes (estrutura formal da segurança da informação), nem sempre são consultados pelos gestores e pelos empregados quando tomam decisões críticas acerca de como agir em segurança com a informação e os sistemas de SI/TI no decurso de actividades negociais. É por isso que estes documentos são muitas vezes designados por "tigres de papel" – tendem a ser esquecidos na prateleira dos escritórios da segurança da informação e em certos gabinetes de gestão. Isto não se aplica a todas as empresas, mas parece ser muito comum. Numa primeira análise parece não haver razões racionais, económicas ou negociais para tal facto. A teoria institucional pode sugerir inúmeras razões, e realmente mostrar que pode ser bastante racional (do ponto de vista da empresa) deixar, por exemplo, o documento da política de segurança da informação não implementado. Sob a perspectiva da teoria institucional, o documento da política da segurança da informação poderia ser visto como resposta às forças institucionais que pressionam as empresas a conformarem-se com as ideias que prevalecem acerca do que uma política da segurança da informação deveria idealmente incluir. Estas forças podem afectar as empresas através de mecanismos coercivos, miméticos e normativos, resultando em estruturas de segurança formais que são semelhantes umas às outras (por exemplo, no âmbito do campo ou sector em que a organização opera). Alguns exemplos destas forças podem ser:

- **Mecanismos isomórficos coercivos:** Requisitos legais (privacidade dos indivíduos, legislação de contas e taxas, etc.). Requisitos dos consumidores ("Se quiser vender-nos tem que estar em conformidade com a norma ISO/ICE 27001"). Requisitos do proprietário.

- **Mecanismos isomórficos miméticos:** Competição (seguir o líder e esperar ter o mesmo sucesso).

- **Mecanismos isomórficos normativos:** Consultores (políticas resultantes de *copy-and-paste*). Gabinetes de segurança certificados (visão semelhante de segurança na mesma escola ou em escolas semelhantes).

Estes são apenas exemplos de mecanismos potenciais que podem ajudar a determinar a estrutura de semelhança formal. Assim se compreende que um trabalho de investigação potencial poderia envolver a identificação das forças institucionais que afectam a forma como são redigidas as políticas de segurança da informação, quem são os "remetentes", como estão estas instituições difundidas através dos campos organizacionais e até que ponto afectam a estrutura de segurança formal [Björck 2004, p. 4].

Há outros aspectos das instituições para lá dos puramente regulamentares. Há aspectos cognitivos das instituições que afectam a segurança de SI/TI nas organizações. A teoria institucional pode também ajudar a explicar o que é que determina as escolhas feitas pelos funcionários em matéria de SSI, nomeadamente no nível comportamental. Por exemplo, em certas organizações os funcionários bloqueiam os seus sistemas durante o almoço para impedir o acesso não autorizado. Outros funcionários deixam o computador não bloqueado e a porta aberta. Haverá instituições (na forma de comportamento social habitual) que possam fazer a diferença? De novo, trabalhos de investigação interessantes consistiriam em identificar que forças institucionais afectam o verdadeiro comportamento social com implicações de segurança dos SI/TI, quem são os remetentes (de onde vêm), como estas instituições se difundiram através de subgrupos organizacionais (através de que transportadores institucionais) e até que ponto afectam a abrangência da segurança no sistema de informação [Björck 2004, p. 4].

Björck [2004] propõe que a teoria institucional pode auxiliar a compreender a gestão da segurança de SI/TI nas empresas. Em primeiro lugar, pode ajudar a perceber e explicar em que diferem estruturas de segurança formais e comportamentos de segurança actuais. Em segundo lugar, pode auxiliar a perceber porque é que as empresas, frequentemente, criam e mantêm estruturas de segurança formais sem tentarem implementá-las completamente. Finalmente, pode ajudar a identificar e explorar os principais mecanismos através dos quais se controla o comportamento no âmbito da SSI. Se os investigadores e utilizadores de segurança SI/TI empregarem a perspectiva institucional para a análise destes assuntos nas organizações, poderão potenciar o alcance de uma infra-estrutura de gestão de segurança SI/TI mais segura e de custo mais reduzido. Deste modo, Björck lança um repto claro para a aplicação da teoria institucional no campo da SSI.

Pelo exposto, defende-se que a teoria institucional constitui neste trabalho, cujo foco é a adopção de políticas de SSI, um enquadramento teórico adequado para a interpretação dos resultados decorrentes da análise de dados.

5.8 Conclusão

Apesar das limitações enumeradas, considera-se que o método de investigação proposto para o estudo providencia um contributo válido para os objectivos fixados, nomeadamente no que concerne ao levantamento das políticas de segurança

existentes e às práticas relacionadas com a adopção de políticas de SSI nas Câmaras Municipais de Portugal.

Sendo a intenção da investigação qualitativa, segundo Locke et al. [2007], compreender uma situação social particular, um evento, um papel, um grupo ou interacção, entende-se ser a que melhor se coaduna com a investigação em causa.

O método Estudo de Casos é um método de investigação qualitativo que se presta a ser aplicado por investigadores com diferentes perspectivas filosóficas. No caso vertente, a aplicação daquele método será informada por uma perspectiva filosófica face à investigação de cariz interpretivista.

O método de investigação Estudo de Casos é particularmente bem aplicado à investigação em SI e por sua vez aos objectivos pretendidos com este estudo, uma vez que o objectivo é o estudo das políticas de SSI nas organizações, ou seja, a investigação em questão é sobre um fenómeno contemporâneo dentro do seu contexto de vida real.

Capítulo 6

Análise das Políticas de SSI

6.1 Introdução

Neste Capítulo apresenta-se o estudo dos dados resultantes da análise documental das políticas de SSI disponibilizadas pelos Municípios.

Os Municípios aos quais se pediu primeiramente para disponibilizarem o documento da Política de SSI foram aqueles que tinham sido entrevistados e que tinham indicado dispor de uma política de SSI. Seguidamente, foram contactados todos os restantes Municípios que aquando da realização do inquérito disseram ter uma política. Assim, das 38 Câmaras que afirmaram ter uma política de SSI conseguiu-se obter 25 desses documentos. No decurso de obtenção desses documentos foram experimentadas dificuldades, uma vez que se tratam de documentos reservados das Câmaras Municipais e só com persistência apreciável se conseguiu este número de documentos, o qual se considera significativo (66% do total de Câmaras Municipais que sinalizaram dispor de tal documento).

As Câmaras das quais foram analisadas as políticas de SSI distribuem-se do seguinte modo:

Critério	Número
Clusters	
Cluster 1 (Câmaras que têm uma política de SSI)	21
Cluster 2 (Câmaras que não têm implementada uma política de SSI, mas estão em processo de formulação ou adopção)	4
Dimensão	
Classe A (Autarquias muito grandes)	4
Classe B (Autarquias grandes)	4
Classe C (Autarquias médias)	13
Classe D (Autarquias pequenas)	4

Tabela 23: Classificação dos Municípios que Disponibilizaram a Política

A distribuição individual em termos de dimensão da Câmara e de *Cluster* de cada uma das políticas de SSI, pode ser observada na Tabela 24.

Neste capítulo desenvolve-se a análise dos dados ao longo de quatro secções. Após a introdução, na Secção 6.2 são apresentadas as características das políticas através da análise dos 25 documentos, segue-se a Secção 6.3 que apresenta as componentes das políticas de segurança resultantes da análise conjunta da totalidade das políticas de SSI. Na Secção 6.4 apresentam-se as conclusões deste capítulo.

Identificação	*Cluster*	Dimensão
1	*Cluster* 1	Classe C
2	*Cluster* 1	Classe C
3	*Cluster* 1	Classe C
4	*Cluster* 1	Classe D
5	*Cluster* 1	Classe D
6	*Cluster* 1	Classe C
7	*Cluster* 1	Classe A
8	*Cluster* 1	Classe D
9	*Cluster* 1	Classe C
10	*Cluster* 1	Classe C
11	*Cluster* 1	Classe C
12	*Cluster* 2	Classe A
13	*Cluster* 2	Classe A
14	*Cluster* 2	Classe A
15	*Cluster* 1	Classe C
16	*Cluster* 1	Classe C
17	*Cluster* 1	Classe B
18	*Cluster* 1	Classe B
19	*Cluster* 1	Classe C
20	*Cluster* 1	Classe C
21	*Cluster* 1	Classe B
22	*Cluster* 1	Classe D
23	*Cluster* 1	Classe C
24	*Cluster* 1	Classe C
25	*Cluster* 2	Classe B

Tabela 24: Lista das Políticas Analisadas

A análise documental iniciar-se-á com a identificação das características das políticas de SSI em estudo. Para tal, procurar-se-á orientar a análise dos documentos alicerçando-a na revisão da literatura efectuada sobre políticas de SSI (Capítulo 2). Ou seja, atentar-se-á em aspectos como a sua dimensão, forma como está escrita, itens focados, profundidade e abrangência.

Recorda-se que, conforme se explanou no Capítulo 5, se recorre ao enquadramento para a análise da mudança proposto por Walsham [1993], o qual é composto por três dimensões fundamentais: conteúdo das políticas de SSI, processo associado às políticas de SSI e contexto relativo às políticas de SSI. A dimensão a que a análise dos documentos "políticas de SSI" dá resposta é ao "conteúdo", sendo os aspectos inerentes a esta dimensão os seguintes:

- Características das Políticas de SSI – Dimensão do documento, estrutura, nível de abstracção, linguagem, formato, suporte, etc;
- Componentes das Políticas de SSI – Objectivos, declarações gerais de metas, responsabilidades, sanções, contactos, datas, proibições, permissões, etc.

Nas duas secções seguintes procurar-se-á responder à questão de investigação número 2, designadamente "Quais são as características e componentes das políticas

de SSI existentes nas Câmaras Municipais Portuguesas?", mediante a análise das políticas de SSI das Câmaras Municipais a que a investigadora teve acesso.

Essa análise é feita conjuntamente tanto para as características como para as componentes. A análise individual dos 25 documentos encontra-se no Apêndice H. Observe-se que a caracterização das políticas funcionou como o primeiro passo da análise das políticas.

Cada uma destas Câmaras Municipais constitui um caso de análise que será identificado por um número. Sempre que nas transcrições do conteúdo dos documentos houver referência ao nome da Câmara a que a política de SSI pertence, essa referência surgirá só como "Câmara".

Ao longo do capítulo são apresentados extractos retirados dos documentos das políticas, identificados por [Caso X], onde "X" é o número da política de onde o extracto foi retirado.

6.2 Características das Políticas de SSI

A análise conjunta das características das 25 políticas de SSI é apresentada no que respeita à sua dimensão, estrutura, nível de abstracção, linguagem, formato e suporte.

Dimensão do documento

O tamanho dos documentos em análise varia entre o tamanho máximo de 26 páginas e o mínimo de uma página. O tamanho médio das 25 políticas analisadas é de nove páginas, dimensão que excede um pouco o definido como óptimo, por investigadores desta temática e já indicado neste trabalho de investigação, que apontam que uma política não deve ser demasiado grande, definindo o tamanho de cinco páginas como o mais indicado.

O número de palavras contidas em cada documento em análise varia entre o tamanho máximo de 5497 palavras e o mínimo de 125 palavras. O tamanho médio das 25 políticas analisadas é de 2180 palavras.

A identificação de cada política com o respectivo número de páginas e número de palavras é feito na Tabela 25.

Estrutura do documento

A estrutura dos 25 documentos é diversificada. Em alguns casos a estruturação do documento é feita com recurso a capítulos e artigos (sete casos), em outros é dividido em grandes pontos, conforme as temáticas abordadas (14 casos), em outros documentos a divisão é feita com recurso a artigos (dois casos), em um caso a política está dividida em dois documentos e em igual número o documento é dividido em pontos.

Identificação	Nº. Páginas	Nº. Palavras
1	5	2128
2	3	655
3	19	4624
4	1	170
5	14	2802
6	9	2124
7	6	1866
8	14	2557
9	8	3005
10	4	969
11	8	1682
12	11	3270
13	8	2790
14	9	1124
15	26	5497
16	1	125
17	10	1640
18	20	3767
19	4	2318
20	4	1105
21	4	833
22	5	2241
23	10	1207
24	13	5271
25	3	727

Tabela 25: Dimensão das Políticas de SSI

Nível de Abstracção

Entendendo-se por abstracção a subtração de detalhes, ou seja, a capacidade de expressar algo de maneira concisa, abstrata, sem que os detalhes se evidenciem, poder-se-á dizer que a maior parte dos documentos das políticas de SSI apresentam estas características. Contudo, há documentos cujo nível de abstracção é diminuto, ou seja, são demasiado detalhados, o que torna os documentos demasiado extensos.

Este tipo de documentos deve ter uma nível de abstração razoável, sendo conciso nos assuntos abordados, uma vez que se for muito extenso as probabilidades dos utilizadores não o lerem é maior, diminuindo assim a sua eficiência.

Linguagem

Em relação à linguagem presente nos documentos, pode-se afirmar que é uma linguagem clara, concisa, directa e objectiva, na sua maioria.

Os documentos são escritos com um conteúdo preciso, utilizando termos claros e entendíveis. Estes documentos são dirigidos a utilizadores bastante heterogéneos, pelo que se entende a utilização de uma linguagem de fácil leitura e compreensão.

Formato e Suporte

O formato presente nos documentos das políticas de SSI, e dadas as suas características inerentes à distribuição por todos os utilizadores do sistema de informação do município, deveria ser um documento electrónico, contudo e indo de encontro à opinião de muitos autores, que defendem que os utilizadores devem assinar um termo de compromisso, verifica-se que na prática o formato utilizado é em papel.

Cada formato tem as suas vantagens e desvantagens. Alguns formatos são mais apropriados para leitura on-line, enquanto outros são mais eficazes em formato impresso. O tamanho do documentos também condiciona o tipo de suporte a utilizar.

6.3 Componentes das Políticas de SSI

O processo de análise conjunta das políticas na vertente das componentes foi executado com o apoio do software Atlas.ti (versão 5.7.1), tendo sido criados 294 códigos relacionados com as componentes das políticas de SSI. Os códigos foram distribuídos por nove famílias (agrupamentos) dentro dos 25 documentos primários (que formaram a base da análise, ou seja são os "dados em bruto") da unidade hermenêutica (ficheiro que reúne toda a informação relacionada com a análise).

A base metodológica utilizada para a interpretação foi a análise de conteúdo. De forma a garantir o rigor e a qualidade dos dados analisados e das conclusões da investigação, é necessário que possua validade e fiabilidade. Para tal diferentes pessoas intervieram no processo. Para além da autora, um investigador externo procedeu à codificação das entrevistas. Após a verificação de alguns pontos díspares, foi feita uma reunião com o investigador externo e alguns ajustes foram feitos. No presente trabalho aplicou-se o *codebook* desenvolvido por de Sá-Soares [2010], que potenciou a validade e fiabilidade dos dados analisados.

Dada a complexidade e diversidade de componentes abordados nos documentos é fundamental que a atribuição de significado aos segmentos de texto se mantenha homogéneo durante toda a análise, de modo a que o codificador interprete da mesma forma um código durante todo o processo de análise.

Grande parte dos códigos foram transpostos directamente para o Atlas.ti, mas com vista a se operacionalizar o *codebook* no software Atlas.ti optou-se por estabelecer nove famílias de códigos, concretamente:

- CONTAC – O nome e os meios de contacto (morada, número de telefone e telemóvel, endereço de correio electrónico, etc.) de uma pessoa ou organização
- DEF – Definição de conceito, expressão, palavra ou sigla
- SCOPE – Âmbito da política: unidades organizacionais, pessoas, sistemas e informação
- OR – As responsabilidade específicas do proprietário da política
- OB – Um tipo de responsabilidade que transmite a obrigação de realizar uma tarefa específica relacionada com a segurança da informação

- PR – Um tipo de responsabilidade que transmite uma proibição de realizar uma tarefa específica relacionada com a segurança da informação
- DU – Um tipo de responsabilidade que transmite um dever de realizar uma tarefa específica relacionada com a segurança da informação
- RE – Um tipo de responsabilidade que transmite uma recomendação de realizar uma tarefa específica relacionada com a segurança da informação
- XREST – Outro tipo de responsabilidades

Este procedimento aplicou-se para extrair mais facilmente alguns dados ao analisar as políticas codificadas. Mas para isso foi necessário saber a que questões a análise das políticas de SSI daria respostas. Para esse efeito, foi elaborado um conjunto de questões cuja resposta se pretende obter ao longo da análise e que está descrita no Capítulo 8. Essas questões são seguidamente enumeradas.

1 – Qual o propósito das políticas de SSI?

2 – Que componentes contêm as políticas de SSI?

3 – As componentes que as políticas analisadas contêm são coincidentes com as apresentadas na literatura?

4 – Podem estes documentos servir de base para sustentar a proposta de um modelo de política de SSI para as Câmaras Municipais?

5 – Qual é o âmbito das políticas?

6 – Quem elabora esses documentos?

7 – Que recomendações específicas contêm as políticas?

8 – As políticas são documentos que estabelecem proibições ou permissões?

9 – Os documentos são mais prescritivos ou descritivos?

10 – Que tipo de documentos são?

11 – A incidência em determinadas temáticas é coincidente às diferentes políticas?

O processo da análise iniciou-se com a transcrição dos 25 documentos para o formato apropriado e de possível reconhecimento pelo Atlas.ti, procedimento bastante moroso, uma vez que os ficheiros se encontravam na sua maioria em formato PDF, e a sua transposição para o formato RTF não ser automática. Após este procedimento fez-se a inserção desses ficheiros no Atlas.ti.

Seguiu-se o carregamento para o Atlas.ti dos códigos a aplicar retirados do *codebook*. A codificação efectiva das políticas iniciou-se a 27 de Julho de 2010 e terminou a 15 de Agosto de 2010. O tempo total de codificação perfez 68 horas, o que equivale em média a 2.4 horas por documento.

Para cada política foi feito um registo contendo dados do processo de codificação conforme definido nas *coding instructions*. O corpo desse ficheiro de registos contém dois campos, o primeiro identifica a pessoa que codificou a política e o segundo campo é a “Data (Tipo, Duração)”. À frente da designação deste campo é

indicada a data em que a codificação ocorreu, o tipo de codificação (primeira codificação ou revisão) e a duração do processo de codificação nesse dia.

A maior dificuldade a enunciar durante este processo foi decorrente da enorme quantidade de códigos e diversidade de assuntos abordados nas políticas, o que induzia por vezes à dúvida em relação a códigos já aplicados em situações análogas.

As dúvidas surgidas no processo de codificação da política foram anotadas, conforme definido nas *coding instructions*, através da criação de um ficheiro. No corpo do ficheiro foi anotada a dúvida através da indicação da linha do ficheiro com a política a que a dúvida dizia respeito, seguindo-se uma explicação clara da dúvida que ocorreu.

As dúvidas verificaram-se na codificação de quatro documentos, e foram de três tipos, nomeadamente dúvidas específicas ao software Atlas.ti, dúvidas em relação a que código aplicar e falta de um código, para aplicar no texto referente à entrada em vigor da política de SSI.

Ao longo da codificação houve interacção com o autor do *codebook* para se proceder ao esclarecimento das dúvidas anotadas e ajustamentos no *codebook*. Após esta reunião procedeu-se à revisão das codificações já efectuadas. Este procedimento teve a duração de 2.36 horas.

Após estes procedimentos os dados estavam prontos para serem extraídos. O processo iniciou-se com a elaboração de uma tabela (Tabela 26) com todas as componentes focadas e o número de políticas em que foram referenciadas. Para além dessa identificação foi verificado que componentes não foram referidas em nenhuma das políticas.

Só existe uma componente que está presente em todas as políticas que é a "Responsabilidade", esta componente diz respeito às responsabilidades do indivíduo ou entidade, ou seja, traduz comportamentos que um agente deve realizar ou comportamentos que não são admitidos no que concerne à SSI.

Referida a componente presente em todas as políticas de SSI é de mencionar também aquelas que nunca foram referenciadas, que são:

- Monitorização do cumprimento (a forma como o cumprimento da política vai ser verificado e medido).
- Crenças (declaração exprimindo uma crença ou opinião relativamente à protecção dos activos do SI).
- Importância da segurança da informação (expressa o valor atribuído à segurança da informação).
- Nível de segurança pretendido (o nível de segurança que se pretende, explícito quantitativamente ou qualitativamente).

Tabela 26: Componentes Presentes nas Políticas de SSI

	Políticas																										
Componentes	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**Nº**	**%**
Sumário executivo										X							X							X		3	12
Objectivo da segurança da informação			X							X		X			X			X								5	20
Propósito da política	X		X	X	X	X	X	X	X		X	X		X	X	X			X	X		X	X	X	X	19	76
Âmbito da política	X		X		X	X					X	X		X			X	X	X	X	X	X	X	X	X	16	64
Definições	X							X	X			X			X											5	20
Relação obj segurança/obj negócio	X														X											2	8
Linhas orientadoras					X																					1	4
Requisitos	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X			X	X	X	21	84
Directivas	X		X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	23	92
Responsabilidade	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	25	100
Responsabilidade do proprietário			X									X						X								3	12
Comunicação de incidentes	X																	X					X			3	12
Responsável pela gestão de risco	X																									1	4
Coordenação entre as entidades			X																					X		2	8
Atribuição de recursos	X		X				X					X	X	X	X											7	28
Ética relativamente à segurança																							X			1	4
Ameaças												X														1	4
Punições	X				X	X		X	X		X	X	X	X	X				X	X		X	X	X		15	60
Procedimento de comunicação					X	X					X			X									X			5	20
Alvo de comunicação da política	X		X		X	X		X														X				6	24
Declaração de conhecimento		X	X		X			X	X					X		X						X			X	9	36
Data em que teve conhecimento					X			X								X									X	4	16
Localização da política					X		X				X			X								X	X			6	24
Autor da política	X	X	X		X	X									X					X	X				X	9	36
Data elaboração	X		X									X													X	4	16
Data aprovação			X		X		X	X		X	X				X			X	X	X		X		X		12	48
Data entrada em vigor																	X	X	X					X		4	16
Data da revisão					X																					1	4
Aprovação da política	X		X		X		X	X		X	X			X				X	X	X		X		X		13	52
Programa da revisão											X				X											2	5
Aprovação das revisões															X											1	4
Contactos			X		X	X	X	X	X		X	X			X		X	X	X	X	X	X	X	X	X	18	72

- Entidade responsável pela política (Nome ou função da pessoa ou designação da entidade responsável pela política).
- Compromisso da gestão (declaração de compromisso da gestão para a segurança da informação).
- Controlos imprescindíveis (os controlos de segurança de informação classificados como fundamentais. Um controlo é um meio para gerir o risco da segurança da informação).

As componentes presentes nos documentos das políticas são seguidamente listadas em diferentes tópicos que vão contemplar a análise conjunta das políticas de SSI. A análise compreende 31 tópicos, conforme se apresenta nos pontos seguintes.

Identificação da Política

Dentro do universo dos 25 documentos, 23 (92%) possuem um título identificador, contudo a diversidade é muito elevada, ou seja, existem diferenças no nome a atribuir a uma política de SSI.

Conforme se observa na Tabela 27, que lista os vários títulos atribuídos às políticas, verifica-se que os mesmos variam muito, podendo-se agrupar do seguinte modo:

- Regulamento (Interno, Utilização, Municipal, Acesso, Informática)
- Norma (Interna, Utilização, Segurança, Controlo interno)
- Política
- Manual de normas e procedimentos
- Instruções de trabalho
- Regra

De todos os títulos só dois se repetem, um duas vezes e outro três vezes, estando os mesmos seleccionados na tabela a negrito: Normas de utilização dos sistemas de informação do Município de … e Manual de normas e procedimentos de segurança na rede informática da Câmara Municipal de… . Um dos documentos não possui qualquer título.

Desta diversidade de nomes, os que se destacam por serem mencionados em nove documentos cada são as denominações de “Regulamento” e “Normas”, segue-se a denominação de “Manual” em dois casos, e em um caso cada, “Política”, “Instrução de Trabalho” e “Regra”.

As denominações, embora com nomes diferentes, são dirigidas às TIC, como se verifica na tabela com a totalidade dos títulos atribuídos às políticas de SSI. Os tipos de TIC mais versados são o correio electrónico, equipamento informático e a Internet.

Títulos
Regulamento interno de acesso à internet e contas de correio electrónico
Regulamento interno de utilização das tecnologias de informação e comunicação
Regulamento interno de gestão e utilização dos meios informáticos
Regulamento interno sobre a utilização dos meios informáticos de comunicação e de transmissão de dados pelos trabalhadores e colaboradores do Município da …
Regulamento de utilização de equipamento informático
Regulamento municipal de informática sobre regras de uso dos computadores, programas de software e internet/mail
Regulamento de acesso e de utilização dos recursos informáticos da Câmara Municipal de …
Regulamento de informática da Câmara Municipal de …
Regulamento e política de uso do computador, software e internet
Norma Interna de utilização dos recursos informáticos da Câmara Municipal de …
Norma Interna – Câmara Municipal de … (Segurança informática e dos sistemas de informação e Informática – Procedimentos de aquisição, Instrução e utilização)
Normas de utilização do correio electrónico
Normas de utilização
Normas de utilização dos sistemas de informação do Município de …
Normas de utilização de serviços (internet/e-mail) – Carta do utilizador
Normas de segurança e funcionamento dos sistemas de informação do Município de …
Normas de controlo interno das aplicações e do ambiente informático
Política de uso de computador, programas de software e internet
Manual de normas e procedimentos de segurança na rede informática da Câmara Municipal de…
Instrução de trabalho – Gestão de segurança na óptica do utilizador
Regras para utilização dos meios informáticos

Tabela 27: Títulos dos Documentos em Análise

Sumário Executivo

Os documentos com um sumário claramente demarcado são três (12%). Os sumários retratam do que vai constar a política de segurança.

Em um dos casos o sumário é de dimensão reduzida, contudo ilustra sobre o que vai tratar o resto do documento.

Os outros dois casos são similares entre si, ou seja, ambos são denominados por "Preâmbulo", estando a sua ênfase dirigida para o que se pretende com a política de SSI, só o desenvolvimento do conteúdo é que é mais extenso em um dos casos.

Objectivo da Segurança da Informação

Das 25 políticas de SSI em análise cinco (20%) mencionam quais são os objectivos de segurança da informação, ou seja, o que se pretende alcançar como resultado dos esforços de segurança da informação da organização.

Os objectivos apontados vão desde garantir a integridade, a confidencialidade e a disponibilidade dos dados e o de ajudar a avaliar a fidelidade dos mesmos (um caso); ao esclarecimento dos utilizadores sobre os riscos e a necessidade e natureza das medidas de segurança (um caso); responsabilizar os intervenientes no sistema pela protecção de dados e programas (um caso) e garantir a segurança dos dados (dois casos).

Em suma, os objectivos vão muito de encontro à formação e responsabilização das pessoas e dos diferentes intervenientes na questão da consciencialização para a segurança da informação. Outro aspecto incide directamente nos dados e na importância da sua integridade, confidencialidade e disponibilidade.

Propósito da Política

O propósito da política de SSI é mencionado em 19 documentos (76%). O propósito do documento da política aparece algumas vezes como o porquê da formulação da política e em outros casos com o que se pretende atingir com a política. Por se tratar em ambas as situações de propósitos da política, mas a ênfase ser bem diferente, são apresentadas algumas citações divididas conforme se dirigem para o porquê da formulação da política ou para o que a política pretende atingir.

A elaboração do documento teve como principal preocupação, ou seja, o porquê da formulação:

> "…informar sobre a correcta utilização dos equipamentos informáticos disponibilizados aos funcionários e agentes, de forma a prevenir incidentes e prover a instituição de meios que garanta as exigências regulamentadas e/ou legisladas". [Caso 3]

> "…proteger os activos de informação detidos e utilizados pelo município de todas as ameaças, quer internas ou externas, deliberadas ou acidentais e satisfazer todas as exigências regulamentadas e/ou legisladas". [Caso 5]

> "…definir responsabilidades e orientar a conduta dos profissionais e utilizadores da rede informática da Câmara na utilização dos recursos informáticos, visando proteger a integridade e confidencialidade das informações, assim como manter a continuidade operacional". [Caso 6]

> "…regulamentar alguns aspectos relacionados com aquisição e uso das tecnologias de informática, nas suas diversas componentes (hardware, software, comunicações, Internet, etc.)". [Caso 7]

> "…definir um conjunto de regras/normas básicas que definem de forma clara as responsabilidades de cada utilizador do sistema, com vista a uma gestão cuidada e

precisa do parque informático e a uma optimização dos recursos disponíveis". [Caso 8]

"…definir um conjunto de regras/normas básicas, com vista a uma gestão cuidada e precisa do parque informático e a uma optimização dos recursos disponíveis. Esta, visa complementar as leis gerais em vigor e que regulamentam esta matéria". [Caso 8]

"…proteger os activos de informação detidos e utilizados pelo Município de qualquer intromissão, quer internas ou externas, deliberadas ou acidentais". [Caso 11]

"…proteger a integridade dos sistemas de TIC e pôr em prática a política de licenciamento de software do Município". [Caso 12]

"…definir os termos e condições de atribuição de material informático da autarquia aos seus colaboradores elegíveis no âmbito desta regulamentação, e sua utilização". [Caso 14]

Quanto ao que o documento pretende atingir:

"Para que o serviço de acesso à Internet e o sistema de correio electrónico seja eficaz e actualizado, é necessário que se respeitem determinadas regras que contribuam quer para a segurança, quer para a celeridade das consultas e das transacções, ajudando a prevenir sobrecargas na rede informática e riscos para a segurança do sistema informático do Município". [Caso 1]

"…estabelece e define as regras e as condições a que devem obedecer todos os elementos que utilizam os recursos computacionais e da rede de dados e comunicações do Município". [Caso 3]

"…regulamentam a utilização apropriada dos recursos informáticos, com vista à protecção e privacidade efectiva de utilizadores e dados, bem como a própria administração desses recursos na Câmara. O cumprimento destas normas não dispensa normas gerais aplicáveis". [Caso 9]

"…a segurança do sistema informático". [Caso 18]

"…informar todo o pessoal a prestar serviço no Município das suas responsabilidades no manuseamento e protecção da tecnologia e informação do Município, de forma a que todos cooperativamente possam oferecer um melhor serviço aos utentes, trabalhem com mais facilidade e por outro lado aumentem a segurança e diminuam o risco de perda de informação". [Caso 20]

"…estabelece os direitos e deveres dos utilizadores registados como funcionários e/ou agentes da Câmara". [Caso 22]

De entre os vários propósitos o seu foco ou incidência é variável conforme se verifica na Tabela 28.

Incidência do propósito	Número
Recursos informáticos	8
Acesso à Internet e ao sistema de correio electrónico	5
Activos de informação	5
Tecnologias de informação	3
Optimização dos recursos	2

Tabela 28: Incidência do Propósito

A incidência do propósito da política verifica-se maioritariamente na componente informática: em oito casos nos recursos informáticos de uma forma geral e em cinco nos acessos à Internet e ao sistema de correio electrónico.

Em cinco casos a incidência é nos activos da informação, ou seja, proteger a integridade e confidencialidade da informação, manter a continuidade operacional, assim como proteger de qualquer intrusão, quer internas ou externas, deliberadas ou acidentais.

A boa utilização das tecnologias de informação é mencionada em três políticas de SSI, como sendo o propósito do documento.

A optimização dos recursos, ou seja, optimizar os recursos de um modo geral de forma que contribuam para uma melhor rentabilização dos meios ao dispor, aparece em dois documentos.

É de mencionar que algumas políticas têm mais do que um propósito, por isso a diferença entre o número de políticas que têm descrito um propósito e o número de incidências presentes na tabela.

Verifica-se que a incidência do propósito da política de SSI é basicamente nas TIC, que coincide com a denominação já mencionada anteriormente para os vários documentos.

Âmbito da Política

O âmbito da política pode comportar vários aspectos, como por exemplo: unidades organizacionais; pessoas ou funcionários; sistemas, informação e outros. Da análise das 25 políticas de SSI verifica-se que o âmbito é definido em 13 casos (52% dos documentos) e aborda mais que um tipo, conforme se observa na Tabela 29.

Tipo do âmbito	Número
Pessoas, funcionários, utilizadores e outros agentes	9
Sistemas	7
Unidades organizacionais	3

Tabela 29: Âmbito da Política

A abrangência da política referida no âmbito das “pessoas, funcionários, utilizadores” refere-se a:

- Colaboradores directos e indirectos, e para qualquer empresa que no papel de fornecedor necessite de integrar com os sistemas proprietários do Município. [Caso 3]
- Funcionários e agentes. [Caso 5]
- Colaboradores do Município ou terceiros. [Caso 11]
- Todos os funcionários. [Caso 12]
- Funcionários e agentes, os contratados ao abrigo de contrato individual e os colaboradores em regime de prestação de serviços. [Caso 17]
- Todos os funcionários e terceiros. [Caso 19]
- Pessoas pertencentes ao quadro de pessoal e/ou contratados. [Caso 22]
- Pessoas, enquanto utilizadores dos recursos informáticos integrados temporária ou permanentemente na Autarquia. [Caso 23]
- Todos os utilizadores. [Caso 25]

A abrangência da política exposta no âmbito dos "sistemas" refere-se a:

- Serviços de acesso à Internet e das contas de correio electrónico institucionais. [Caso 1]
- Equipamento informático, tecnologias de informação e comunicação. [Caso 3]
- Áreas partilhadas, sistema de e-mail, pastas públicas do e-mail, áreas pessoais na rede e salvaguarda dos portáteis. [Caso 14]
- Todas as comunicações ou transmissões de dados efectuadas por telefone, correio electrónico ou outras formas de transmissão de dados por via telemática e o acesso à Internet. [Caso 17]
- Sistema informático. [Caso 19]
- Rede informática, do equipamento de informática, do correio electrónico e da Internet. [Caso 20]
- Equipamento da Autarquia. Estrutura lógica e infra-estrutura física de suporte à actividade informática. [Caso 23]

A abrangência da política referida no âmbito das "unidades organizacionais" refere-se a:

- Órgãos e aos diversos serviços e organismos. [Caso 1]
- Todos os órgãos e serviços. [Caso 5]
- Todos os serviços. [Caso 18]

Como se verifica na Tabela 29, o âmbito da política aborda em nove casos as pessoas e em sete os sistemas, seguindo-se em menor número as unidades organizacionais (três casos). O âmbito para a informação não foi mencionado em nenhum dos documentos, bem como outros âmbitos.

Dos 13 documentos que mencionam o âmbito da política de SSI, verifica-se conforme se observa na Tabela 30, que só em sete casos é definido um único âmbito, sendo que os restantes mencionam mais do que um âmbito para a política de SSI.

Âmbitos combinados das políticas	Número
Pessoas, funcionários, utilizadores e outros agentes	4
Sistemas	2
Unidades organizacionais	1
Pessoas, funcionários, utilizadores e Sistemas	4
Pessoas, funcionários, utilizadores e Unidades organizacionais	1
Sistemas e Unidades organizacionais	1

Tabela 30: Âmbitos Combinados das Políticas

Definições

O *codebook* contempla dois códigos para as definições, um para a definição de segurança da informação e outro para outras definições. Da análise conjunta verificou-se que em cinco políticas há definições.

Nas políticas de SSI analisadas verificou-se que o código atribuído para seleccionar o texto que define segurança de informação não foi utilizado, ou seja, não é definido o que se entende por segurança da informação. Contudo, são definidas em cinco políticas 32 termos diferentes, distribuídos da seguinte forma:

- [Caso 1] – *Spam*, Encriptação, *Attachment*, *Malware*, *Cracking*.
- [Caso 8] – Recursos informáticos.
- [Caso 9] – Sistema informático, Privilégios da administração, Recurso informático.
- [Caso 12] – Disponibilidade, Confidencialidade, Integridade, Repúdio, Fidelidade, Licenciamento de software, *Freeware*, *Shareware*, Software do domínio público, *Plug-in*, Vírus, *Worm*, Cavalo de Tróia, Computadores, Hardware, Direitos, Permissões, Perfil do utilizador, *User account*, Correio electrónico.
- [Caso 15] – Software de sistema, Suportes físicos e Software aplicacional.

As definições presentes nos cinco documentos estão organizadas de forma distinta. Em um caso estão no final do documento com o título de "Glossário", em dois casos são artigos designados de "Definições" inseridos em capítulos, em um caso definido por "Introdução" e no outro por "Definições", nos outros dois documentos aparecem diluídas no documento no início de pontos que na sua composição vão utilizar esses termos.

A única definição que se repete em dois documentos é a de "Recursos Informáticos". Em dois outros casos poderá parecer duplicação, mas a abrangência é diferente, a definição de "Computador" está também na de "Suportes físicos", mas esta última engloba outros dispositivos e equipamentos para além dos computadores.

Relativamente à definição de termos, verifica-se que só em cinco documentos é que é feito, o que poderá levar a um entendimento dificultado da política de SSI nos restantes casos. Os termos definidos não se repetem com excepção de "Recursos Informáticos". Estes 32 termos são considerados como "outras definições", pois a definição fulcral numa política de SSI é a de "segurança da informação", contudo, não foi mencionada em nenhum caso, poderá ser entendido como um termo que

consideram como corrente ou de difícil especificação e consequentemente de difícil definição.

Dos termos definidos nas políticas de segurança verifica-se que se concentram maioritariamente em termos da área informática.

Relação Objectivo Segurança/Objectivo do Negócio

A relação entre as tarefas ou objectivos da segurança da informação e os objectivos ou tarefas de negócio é mencionada em apenas dois dos documentos (8% das políticas analisadas).

A interligação entre os objectivos de negócio e os objectivos de segurança da informação indica a importância que a empresa atribui em termos de segurança da informação e expressa como a segurança da informação permite a realização de objectivos de negócio ou como se relaciona com a realização de tarefas do negócio.

Na presente análise é mencionado um caso que relaciona as tarefas do negócio com a utilização do correio electrónico. É mencionado que o correio electrónico é um instrumento de comunicação e um veículo por excelência para circulação e troca de documentos entre os diversos serviços do Município e também com entidades externas, e é disponibilizado aos trabalhadores e colaboradores dos órgãos, serviços e organismos que integram o Município como uma ferramenta de trabalho, pelo que este recurso deve ser utilizado estritamente para fins inerentes ao desempenho das funções atribuídas aos diversos utilizadores, no âmbito da sua actividade profissional.

É manifestamente considerado reduzido o número de casos que mencionam a relação entre as tarefas ou objectivos da segurança da informação e os objectivos ou tarefas de negócio.

Linhas Orientadoras

Entende-se por “Linhas orientadoras” o estabelecimento de linhas de orientação ou intenções acerca da segurança da informação.

Essas linhas orientadoras estão definidas em uma (4%) política de SSI. Define responsabilidades, compromisso e cooperação de todos os colaboradores e define o estabelecimento de princípios que contribuam para a uniformização de procedimentos.

Requisitos

Por “requisitos” entende-se uma exigência para os esforços de segurança da informação empreendidos pela organização. Um requisito implica geralmente um tipo e nível de protecção necessário para assegurar um certo nível de segurança para o sistema de informação.

Das 25 políticas de SSI, 21 (84%) mencionam algum tipo de esforço de segurança da informação delineada pela organização.

Os requisitos podem ser de várias ordens e associados a várias áreas. Os requisitos presentes nas políticas de SSI e o número de vezes citados apresentam-se na Tabela 31.

Requisitos	Número
Cumprimento dos requisitos legais	38
Troca de informação	20
Responsabilidade por activos	10
Gestão de acessos dos utilizadores	9
Política de segurança da informação	8
Procedimentos operacionais e responsabilidades	6
Segurança dos sistemas de informação	6
Backup	4
Cumprimento das normas de segurança e da política	4
Organização interna da segurança da informação	4
Monitorização	4
Segurança de ficheiros do sistema	4
Considerações de auditoria de sistemas de informação	3
Gestor SI/TI	3
Gestão da segurança de redes	3
Denúncia ou mudança de emprego	3
Continuidade do negócio	2
Controlo de acesso	2
Computação móvel e teletrabalho	2
Controlo de acesso ao sistema operacional	2
Protecção contra códigos maliciosos	2
Entidade externa na prestação de serviços de gestão	2
Controlo de acesso às aplicações e à informação	1
Equipamento de segurança	1
Manipulação de meios de comunicação	1
Antes do emprego	1
Áreas de segurança	1
Responsabilidades do utilizador	1

Tabela 31: Requisitos

De entre os requisitos há três a destacar pelo número de ocorrências nas políticas de SSI, são eles o cumprimento dos requisitos legais, a troca de informação e a responsabilidade por activos.

O cumprimento dos requisitos legais refere-se ao cumprimento das normas legais, estatutárias e obrigações de segurança regulamentares e contratuais. Como exemplo, "o Município das … reserva-se o direito de auditar o cabeçalho das mensagens enviadas e recebidas, assegurando o cumprimento da Lei da Protecção de Dados Pessoais e assegurar o cumprimento deste regulamento". [Caso 3]

A troca de informação refere-se à segurança da informação e troca de software dentro de uma organização e com qualquer entidade externa. Como exemplo de citação tem-se "as trocas de dados, electrónicas ou manuais, com outras organizações devem ser rigorosamente controladas segundo o grau de sensibilidade e

sujeitas a cuidados especiais que permitem controlar a origem, o destino, o formato, o conteúdo, o autor da cópia e outros elementos que se considerem importantes". [Caso 15]

A responsabilidade por activos refere-se ao inventário de activos de SI. Como por exemplo, "todos os equipamentos informáticos da Câmara Municipal de … deverão ser identificados com uma etiqueta de inventário, colocado no exterior do equipamento da qual será responsável a secção de Património". [Caso 14]

Estes três requisitos mereceram um número de 68 citações contra 79 citações em 25 requisitos. O número significativo de citações reforça claramente o seu destaque e importância nesta lista de requisitos.

Directivas

Entende-se por "Directivas" as decisões para a implementação da segurança da informação. Estas decisões fazem parte de 23 (92%) políticas. Contudo, as directivas abrangem um leque muito alargado de áreas, num total de 43 focos diferentes. A Tabela 32, apresenta as directivas cuja ocorrência é mais significativa.

Directivas	Número
Responsabilidade do utilizador	50
Procedimentos operacionais e responsabilidades	41
Troca de informação	28
Responsabilidade por activos	25
Gestão de acessos dos utilizadores	25
Monitorização	24
Gestão da segurança de redes	21
Controlo de acesso à rede	18
Cumprimento dos requisitos legais	17
Equipamento de segurança	17
Backup	15
Manipulação de meios de comunicação	11
Controlo de acesso ao sistema operacional	10
Protecção contra códigos maliciosos	10
Áreas de segurança	10

Tabela 32: Directivas

De entre as directivas há sete a destacar pelo número de ocorrências nas políticas de SSI, são elas responsabilidade do utilizador, procedimentos operacionais e responsabilidades, troca de informação, responsabilidade por activos, gestão de acessos dos utilizadores, monitorização e gestão da segurança de redes.

Nas responsabilidades do utilizador destaca-se a selecção e utilização de *passwords* pelos utilizadores. Como por exemplo, "as palavras chave devem ser mudadas a intervalos regulares – O *helpdesk* ajudá-lo-á demonstrando como fazê-lo. Os sistemas serão instalados a forçar a mudança da palavra-chave, sempre que necessário". [Caso 5]

Os procedimentos operacionais e responsabilidades dizem respeito ao manuseamento e exploração de informações e inclui a documentação, manutenção e disponibilização de procedimentos operacionais. Como por exemplo, “todos os documentos que se coloquem na intranet/portal devem encontrar-se em formato PDF e nunca em formato editável (doc, xls, ppt, etc.)”. [Caso 3]

A troca de informação refere-se à segurança da informação e troca de software dentro de uma organização e com qualquer entidade externa. Como por exemplo, “as mensagens de correio electrónico (e-mails) internos e externos devem ser exclusivamente de carácter profissional, sendo proibido qualquer tipo de utilização particular. O mesmo se aplica para arquivos anexos”. [Caso 6]

A responsabilidade por activos refere-se ao inventário dos activos de SI. Como por exemplo, “O código de identificação do bem dos equipamentos informáticos é o nº de série dos mesmos, sempre que possível, de modo a permitir a verificação imediata do mesmo, tanto para efeitos de controlo interno como externo”. [Caso 3]

A gestão de acessos dos utilizadores define a atribuição de direitos de acesso ao sistema de informação e serviços. Como por exemplo, “para cada tipo de acesso electrónico ao exterior, é necessária uma autorização específica, podendo um mesmo utilizador estar autorizado a usar apenas um ou, diversos tipos de acesso electrónico ao exterior, de acordo com as regras …”. [Caso 10]

Por monitorização entende-se o acompanhamento dos sistemas e o registo de eventos de segurança da informação. Como por exemplo, “reserva-se a C.M o direito de auditar a utilização das suas contas de correio electrónico da Câmara fornecidas aos utilizadores, sem se caracterizar invasão de privacidade. Estas auditorias são realizadas de forma aleatória e são parte importante da monitorização necessária a manter a operacionalidade dos sistemas”. [Caso 6]

Por gestão de segurança de redes entende-se a protecção da informação em redes e a protecção das infra-estruturas de apoio. Como por exemplo, “o uso individual dos recursos informáticos, tais como mensagens electrónicas, acesso à Internet, armazenamento de dados em computadores (downloads) ou a impressão de ficheiros não devem ser excessivos nem interferir na utilização e acesso de outros utilizadores a esses recursos”. [Caso 9]

As decisões para a implementação da segurança da informação, conforme se observa, são bastante abrangentes focando um número considerável de pontos, número que reflecte as várias vertentes sobre as quais as políticas incidem.

	Políticas																										
Directivas	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**Nº**	**%**
Informação sobre a avaliação de riscos de segurança						X	X																			2	8
Informação sobre tratamento de riscos de segurança							X																			1	4
Política de seg urança da Informação								X	X	X		X														4	16
Partes externas						X	X		X			X									X		X			6	24
Responsabilidade pelos activos															X											1	4
Classificação da informação	X		X		X		X				X	X	X	X	X				X				X		X	12	48
Antes do emprego															X											1	4
Durante o emprego						X																				1	4
Mudança de emprego						X	X	X													X					4	16
Areas seguram								X	X			X			X											4	16
Equipamentos de segurança															X			X								2	8
Procedimentos e responsabilidades operacionais										X					X			X								3	12
Entidade externa na prestação de serviços de gestão			X		X	X		X	X	X	X	X	X		X		X		X	X		X			X	15	60
Backup					X	X					X	X			X				X	X	X					8	32
Gestão de segurança de rede	X				X		X			X	X				X			X	X							8	32
Manipulação de suportes informáticos					X	X		X	X		X		X						X		X		X			9	36
Troca de informação	X		X	X		X		X	X												X	X				8	32
Serviço de comércio electrónico					X	X						X							X		X	X	X		X	8	32
Requisitos para o controlo de acesso						X	X			X		X	X		X						X	X	X	X	X	11	44
Gestão de acessos dos utilizadores						X	X								X											3	12
Responsabilidades do utilizador					X				X	X	X		X		X		X	X	X	X			X			11	44
Controlo de acesso à rede					X	X		X	X	X	X	X	X		X				X	X	X		X	X	X	15	60
Controlo de acesso ao sistema operativo					X	X	X	X	X	X	X		X		X			X	X		X			X		13	52
Controlo de acesso às aplicações e à informação	X			X	X				X	X					X				X				X			8	32
Computação móvel e teletrabalho															X											1	4
Requisitos de seg dos SI												X	X		X											3	12
Segurança de ficheiros de sistema															X								X			2	8
Seg. em processos de desenvolvimento e suporte				X								X										X	X			4	16
Gestão de vulnerabilidades técnicas									X			X								X						3	12
Gestão de incidentes de seg e melhorias								X							X											2	8
Continuidade do negócio															X											1	4
Cumprimento dos requisitos legais					X	X					X		X		X		X		X		X	X				9	36
Cumprimento das normas de seg					X			X			X	X							X							5	20
Considerações de auditoria de SI					X			X	X		X		X	X					X							7	28

Tabela 33: Tipo de Directivas por Política

A indicação do número de políticas em que cada tipo de directiva está presente pode ser observada na Tabela 33.

Conforme se verifica na tabela anterior, a frequência com que cada directiva aparece nas políticas é muito variável. Importa também realçar que há várias directivas que não são referidas em nenhuma política: Organização interna da segurança da informação, Planeamento e aceitação de sistemas, Protecção contra códigos maliciosos, Monitorização, Correcto processamento dos pedidos, Controlos criptográficos e Relatório de informações de eventos e fraquezas de segurança.

Responsabilidades

Por "Responsabilidade do indivíduo ou da entidade" entendem-se as obrigações, proibições, deveres, recomendações e outras responsabilidades que indivíduos, grupos ou entidades devem ter em relação à segurança da informação. A responsabilidade especifica um comportamento que deve ser realizado por um agente. Também pode especificar um comportamento proibido que um potencial agente não deve executar.

Das 25 políticas de SSI em análise todas abordam de alguma forma responsabilidades, o que corresponde a 100% dos casos.

As responsabilidades são divididas por tipo, designadamente: Obrigação, Proibição, Dever, Recomendação e outro tipo de responsabilidade. A Tabela 34 apresenta o número de ocorrências para cada um dos tipos de responsabilidades na totalidade das políticas.

Tipos de responsabilidade	Número
Proibição	207
Obrigação	179
Dever	148
Recomendação	28
Outro tipo de responsabilidade	2

Tabela 34: Tipos de Responsabilidade

Conforme se observa na tabela anterior, o tipo de responsabilidade mais predominante é a "Proibição", seguindo-se a "Obrigação" e o "Dever". As "Recomendações" são em número reduzido, bem como outro tipo de responsabilidade.

A responsabilidade é de diferentes tipos que por sua vez varia conforme para quem é dirigido esse tipo de responsabilidade, nomeadamente Utilizador genérico, Técnico de SI/TI, Gestor SI/TI, Gestor de linha, Gestor de topo, Unidade de SI/TI e outra unidade individual ou organizacional. A Tabela 35 apresenta a distribuição por tipo de responsabilidade e para quem é dirigida.

	Direcção da responsabilidade	Número
Obrigação	Utilizador genérico	102
	Técnico SI/TI	37
	Gestor SI/TI	14
	Gestor de linha	1
	Gestor de topo	6
	Unidade de SI/TI	18
	Outra Unidade	1
Proibição	Utilizador genérico	206
	Técnico SI/TI	1
Dever	Utilizador genérico	40
	Técnico SI/TI	53
	Gestor SI/TI	44
	Gestor de linha	3
	Gestor de topo	2
	Unidade de SI/TI	4
	Outra Unidade	1
Recomendações	Utilizador genérico	22
	Técnico SI/TI	4
	Unidade de SI/TI	2
Outro	Utilizador genérico	1
	Técnico SI/TI	1

Tabela 35: Direcção da Responsabilidade

Embora as diferentes responsabilidades não sejam dirigidas para todas as categorias, verifica-se que em todos os casos a direcção inclui o utilizador genérico, seguindo-se os técnicos de SI/TI.

Como forma de exemplificar os vários tipos de responsabilidades (Proibições, Obrigações, Deveres, Recomendações e Outros) são apresentados seguidamente nas Tabelas 36 a 40, dentro de cada tipo, aqueles cuja frequência de citações é maior.

Frequência por tipo de responsabilidade – Proibição	Nº
Utilizador genérico	
Controlo de Acesso à Rede "É expressamente proibido utilizar ferramentas externas de conversação (*chat*, *messenger*, etc.) na infra-estrutura disponibilizada…". [Caso 3] "É expressamente proibido disponibilizar, enviar, transferir, transmitir qualquer conteúdo que seja ilegal". [Caso 3]	41
Troca de Informação "Mensagens cujo conteúdo reflicta a intenção de obter proveitos financeiros pessoais". [Caso 13] "Para criação ou distribuição de informação ofensiva ou imprópria, incluindo mensagens com conteúdo ofensivo sobre origem racial ou étnica, género, idade, pornografia, orientação sexual, fé religiosa, convicções políticas ou filosóficas, filiação sindical ou partidária, nacionalidade ou deficiências". [Caso 1]	29
Responsabilidade pelos Activos "Não é permitido, sem autorização expressa dos serviços, abrir os	21

computadores, substituir ou retirar peças". [Caso 1] "Destruir ou estragar intencionalmente equipamentos, software ou dados pertencentes ao Município". [Caso 8]	
Responsabilidades do Utilizador "É proibido aos utilizadores ligar computadores pessoais ou de terceiros à rede da Câmara sem o prévio conhecimento do Gabinete de Informática". [Caso 6] "Nunca escreva a sua *password* nem a envie por correio electrónico". [Caso 12]	21
Controlo de Acesso ao Sistema Operativo "Registar-se no sistema informático de Município com a conta de outro utilizador ou aceder a informação às quais o utilizador não está autorizado a aceder". [Caso 15]	20
Técnico SI/TI	
Controlo de Acesso ao Sistema Operativo "É expressamente proibido ao Gabinete de Informática guardar qualquer registo das *passwords* dos utilizadores ou delas dar conhecimento a terceiros". [Caso 15]	1

Tabela 36: Frequência por Tipo de Responsabilidade – Proibição

A tabela seguinte apresenta a frequência com que o tipo de responsabilidade "Obrigação" é citado nas políticas de SSI em análise.

Frequência por tipo de responsabilidade – Obrigação	Nº
Utilizador genérico	
Procedimentos e Responsabilidades Operacionais "O Utilizador é obrigado a comunicar ao Gabinete de Informática, por escrito, toda e qualquer violação ou quebra de segurança, incluindo quebra de confidencialidade da *password*". [Caso 3] "Nunca deixe um computador ligado à rede desacompanhado e com a *password* introduzida (sessão aberta)". [Caso 5]	31
Responsabilidades do Utilizador "Alterar a *password* periodicamente e sempre que o sistema o solicite". [Caso 8] "O utilizador obriga-se a respeitar todos e quaisquer direitos de terceiros, sejam eles de natureza pessoal ou patrimonial". [Caso 22]	19
Responsabilidade pelos Activos "Todos os utilizadores são responsáveis pelos equipamentos que lhe são atribuídos, devendo zelar pelo bom estado de utilização e conservação dos mesmos". [Caso 3] "Todos os utilizadores são responsáveis pelo uso correcto das ferramentas electrónicas de propriedade da Câmara". [Caso 6]	10
Técnico SI/TI	
Responsabilidade pelos Activos "A configuração do computador é da responsabilidade do Gabinete de Informática". [Caso 12]	9

"O Gabinete de Informática ficará responsável pelo registo e actualização de todo o software conforme fornecido pelos respectivos fornecedores, instalando as actualizações consoante venham a ser disponibilizadas, mantendo o controlo de todas as versões disponíveis no Município". [Caso 15 e19]	
Backup	5
"A responsabilidade de todos os dados que se encontram nos servidores de rede é dos Serviços de Informática que assegurará que os *backups* são executados regularmente e armazenados em local seguro". [Caso 5,6 e 11]	
"A equipa do gabinete de informática é responsável por fazer as cópias de segurança dos ficheiros guardados em servidor". [Caso 12]	
Controlo de Acesso à Rede	4
"O Gabinete de Informática verifica regularmente todos os sistemas e eventuais tentativas de acesso não autorizado aos mesmos. Qualquer tentativa de acesso não autorizado é passível da elaboração de relatório de intrusão". [Caso 5]	
"Os utilizadores serão responsabilizados por tentar ter acesso deliberado a um sistema para o qual não tenha autorização. O Gabinete de Informática monitorizará regularmente todos os sistemas e eventuais tentativas de acesso não autorizado aos mesmos". [Caso 13]	
Gestor SI/TI	
Cumprimento dos Requisitos Legais	3
"O Administrador de Sistemas deve rever e observar periodicamente as informações, certificando-se de que não houve a violação de leis, ou a utilização para fins não autorizados". [Caso 8]	
Considerações de Auditoria de SI	3
"O Administrador de Sistemas possui autorização para utilizar o sistema de segurança ou qualquer mecanismo que julgue adequado para a auditoria e controlo dos computadores e da rede". [Caso 8]	
Política de Segurança da Informação	
"O Administrador de Sistemas é responsável pela implementação de medidas de segurança necessárias para garantir a integridade da informação, independentemente da maneira pela qual esteja armazenada e comunicar superiormente o desrespeito por qualquer norma". [Caso 8]	
"O administrador dos recursos informáticos é responsável pelas medidas de segurança necessárias para garantir a salvaguarda dos dados da CME no geral e de cada utilizador em particular". [Caso 9]	3
Gestor de linha	
Política de Segurança da Informação	1
"Compete às Direcções de Departamento, de Divisão e Chefias de Secção, dentro das respectivas unidades orgânicas, dar cumprimento às normas definidas neste documento". [Caso 18]	
Gestor de topo	
Gestão de Acessos dos Utilizadores	3
"O Município, através dos seus órgãos de gestão ou seus representantes, pode suspender todos os privilégios de determinado utilizador em relação ao uso	

dos recursos informáticos, por razões ligadas à segurança física e ao bem-estar do utilizador, ou por inobservância das regras constantes neste documento". [Caso 8] "O acesso será prontamente restabelecido quando a segurança e o bem-estar ou os interesses puderem estar assegurados; a suspensão do acesso pode continuar se for resultado de uma acção disciplinar imposta pelos órgãos executivos do Município". [Caso 8]	
Unidade de SI/TI	
Responsabilidade pelos Activos "Elaborar propostas tendentes à adopção de novas soluções informáticas e desenvolvimento de projectos, visando um melhor e mais eficaz funcionamento de todas as unidades orgânicas". [Caso 3] "Optimizar a gestão dos equipamentos informáticos e respectivos consumíveis, coordenando a integração de meios entre os serviços". [Caso 3]	10
Controlo de Acesso à Rede "Garantindo os mecanismos de protecção, segurança e controlo de acesso definidos, de forma a garantir a privacidade e a integridade, quer dos vários componentes que formam os sistemas informáticos e de comunicações, quer da informação constante dos ficheiros informáticos centralizados ou que circulem na rede, desde que tenha condições técnicas para efectuar os mesmos". [Caso 3] "Assegurar a manutenção e boa utilização do equipamento e dar suporte às aplicações informáticas institucionais e apoiar os utilizadores locais e remotos". [Caso 3]	2
Outra Unidade	
Responsabilidade pelos Activos "Os computadores pessoais são da responsabilidade do pessoal a quem estão afectos ou que os utilizam regularmente. Quando se trate de equipamentos de uso colectivo ficam à guarda do coordenador da unidade orgânica onde estão colocados". [Caso 15]	1

Tabela 37: Frequência por Tipo de Responsabilidade – Obrigação

A tabela seguinte apresenta a frequência com que o tipo de responsabilidade "Dever" é citado nas políticas de SSI em análise.

Frequência por tipo de responsabilidade – Dever	Nº
Utilizador genérico	
Responsabilidade pelos Activos "Sempre que seja detectado uma anomalia no computador do local de trabalho, o utilizador deve efectuar uma verificação primária (verificação dos cabos) ao equipamento". [Caso 3]	8
Troca de Informação "Para evitar o desperdício dos recursos da rede, é aconselhável comprimir os ficheiros anexos que são enviados para fora e, se possível, também os que são recebidos. Esta prática reduz o risco de uma congestão da rede e limita a quantidade de espaço de armazenamento necessária". [Caso 1]	7

"Quando a informação for directamente para a caixa de correio dos funcionários/serviço e tiver carácter oficial, deve-se reencaminhar o e-mail para o serviço de expediente e arquivo para a caixa de correio para que se dê o respectivo registo de entrada e saída". [Caso 2]	
Organização Interna da Segurança da Informação	5
"Responder pelo uso exclusivo e intransferível das suas senhas de acesso". [Caso 6]	
Técnico SI/TI	
Monitorização	7
"Os equipamentos de comunicações que estão fora do "*Data Center*" serão acedidos periodicamente pelo pessoal do Gabinete de Informática para verificar as respectivas condições de funcionamento e eventuais ligações não autorizadas". [Caso 15]	
"A existência de uma manutenção que garanta o bom funcionamento das aplicações é da responsabilidade do Gabinete de Informática". [Caso 18]	
Responsabilidade pelos Activos	6
"Instalar ou remover componentes, fazer manutenção e controlar hardware e software". [Caso 6]	
"A instalação de equipamentos e aplicações deve apenas ser executada pelo Gabinete de Informática ou sob a sua supervisão, não sendo atribuídos aos utilizadores direitos de administração sobre o equipamento informático que lhe estiver distribuído". [Caso 10]	
Outro Objecto de Segurança da Informação	6
"O uso de *freewa*re ou *sharewa*re só deverá ser permitido para propósitos da actividade da Câmara, devendo ser providenciado e instalado pelo Gabinete de Informática". [Caso 5,6,11,13 e 19]	
Gestor SI/TI	
Política de Segurança da Informação	13
"Manter no Município um registo de ocorrências de violação dos regulamentos". [Caso 8]	
"Transmitir e fazer cumprir todas as directivas e instruções do órgão executivo do Município respeitantes ao sistema informático, às bases de dados e aos sistemas de telecomunicações". [Caso 17]	
Monitorização	4
"Extrair relatórios estatísticos referentes à actividade dos sistemas". [Caso 17]	
"Assegurar a correcção dos dados pessoais constantes das bases de dados e determinar a rectificação de todos os erros detectados". [Caso 17]	
Áreas Seguras	4
"Controlar o acesso físico aos equipamentos sob sua responsabilidade". [Caso 8 e 9]	
"Sempre que existam obras no edifício, as alterações relativas à passagem de cabos, deverão ser controladas pelo Coordenador Técnico do Gabinete de Gestão de Sistemas de Informação". [Caso 15]	
Gestor de linha	
Durante o Emprego	1

"Educar os funcionários sobre os princípios/procedimentos de segurança da informação, bem como lhes assegurar formação para o uso correcto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas". [Caso 6]	
Política de Segurança da Informação	1
"Zelar pelo cumprimento destas normas e procedimentos e notificar imediatamente o Gabinete de Informática de quaisquer vulnerabilidades e ameaças de quebra de segurança". [Caso 6]	
Procedimentos e Responsabilidades Operacionais	1
"Solicitar ao Gabinete de Informática autorização para acesso do utilizador aos sistemas de informação, bem como actualizar as solicitações de autorização sempre que houver alterações nos sistemas ou funções nas áreas de actuação". [Caso 6]	
Gestor de topo	
Outro Objecto de Segurança da Informação	2
"No seguimento do despacho do Sr. Presidente da Câmara e após leitura detalhada do documento em anexo, julgo que o mesmo está em condições de ser aprovado e distribuído pelos serviços". [Caso 1]	
"Sem prejuízo de uma decisão superior em contrário, anexa-se uma proposta do Regulamento Interno de Acesso à Internet e Contas de Correio Electrónico e Boas Práticas, para análise e aprovação". [Caso 1]	
Unidade de SI/TI	
Responsabilidade pelos Activos	3
"Sempre que o equipamento for considerado obsoleto, deteriorado ou depreciado, deverá ser colocado à avaliação do Gabinete de Informática para ser efectuado um parecer técnico para que os responsáveis pelo equipamento possam elaborar o Auto de Abate". [Caso 3]	
"No caso de abatimentos por incapacidade do bem, deverá ser o Gabinete de Informática a propor as características principais para a sua substituição de acordo com as actividades efectuadas pelo utilizador e/ou sector envolvente. Este procedimento pressupõe a apreciação global de integração de toda a estrutura existente ou planeada". [Caso 3]	
Outra Unidade	
Responsabilidade pelos Activos	1
"O funcionamento das diversas aplicações informáticas existentes ou a implementar na autarquia, em termos de utilização (introdução, movimentação e triagem dos elementos necessários), é da responsabilidade dos respectivos serviços, através dos utilizadores designados para o efeito". [Caso 7]	

Tabela 38: Frequência por Tipo de Responsabilidade – Dever

A tabela seguinte apresenta a frequência com que o tipo de responsabilidade "Recomendação" é citado nas políticas de SSI em análise.

Frequência por tipo de responsabilidade – Recomendação	Nº
Utilizador genérico	
Procedimentos e Responsabilidades Operacionais "Não se devem abrir anexos de correio electrónico executáveis, a menos que os Serviços de Informática expressamente autorizem essa tarefa, e mesmo assim recomendamos extrema precaução". [Caso 5] "Sempre que tiver que enviar ficheiros anexos a mensagens estes devem ter o tamanho mais pequeno possível". [Caso 12]	11
Backup "Diariamente executar a rotina de cópia dos ficheiros no servidor para efeitos de *backups*". [Caso 16]	2
Manipulação de Suportes Informáticos "Sempre que um utilizador se encontre de férias, deverá activar o reencaminhamento das mensagens e deixar um aviso automático de ausência". [Caso 3]	2
Segurança de Ficheiros de Sistema "Guardar todos os documentos de serviço na pasta c:\documentosdecarmindapires". [Caso 16] "Não é aconselhável que o utilizador deixe ficheiros guardados em áreas comuns, devendo utilizar sempre a sua área pessoal ou um periférico pessoal, se assim for autorizado". [Caso 23]	2
Técnico SI/TI	
Controlo de Acesso às Aplicações e à Informação "Detecção de processamentos incompletos ou duplicados, reposição das bases de dados e ficheiros no ponto de partida, recuperação de ficheiros ou registos destruídos e verificação periódica do estado das bases de dados e ficheiros". [Caso 15]	4
Unidade de SI/TI	
Política de Segurança da Informação "Com a colocação de uma página da Câmara na Internet, será posto ao serviço do munícipe um conjunto de endereços de correio electrónico, que permitirão um acesso mais fácil e rápido à informação e de uma forma menos burocratizada. Para que sejam cumpridos estes pressupostos, e porque estes novos instrumentos vêm permitir uma modificação nas formas tradicionais de comunicação entre a Administração e os administrados, alerta-se para alguma legislação em vigor sobre o assunto e estabelecem-se algumas normas". [Caso 2] "Colaborar na elaboração de normas de utilização do equipamento Informático". [Caso 3]	2

Tabela 39: Frequência por Tipo de Responsabilidade – Recomendação

A tabela seguinte apresenta a frequência com que o tipo de responsabilidade – "Outro" é citado nas políticas de SSI em análise.

Frequência por tipo de responsabilidade – Outro	Nº
Utilizador genérico	
Responsabilidades do Utilizador "A utilização de páginas de webmail que possam causar infecção na rede de dados e comunicações do Município será da responsabilidade do utilizador ". [Caso 3]	1
Técnico SI/TI	
Responsabilidade pelos Activos "O *helpdesk* do Gabinete de Informática não terá qualquer responsabilidade por problemas de hardware resultantes de instalações não supervisionadas/ não aprovadas". [Caso 12]	1

Tabela 40: Frequência por Tipo de Responsabilidade – Outro

A análise das responsabilidades individualmente por códigos é feita seguidamente, abordando 13 pontos diferentes. Esta análise é precedida por uma tabela que apresenta todos os códigos relacionados com as diferentes responsabilidades relativamente as políticas em que são mencionados.

Conforme se verifica na Tabela 41, a frequência com que cada responsabilidade aparece nas políticas é muito variável. Há várias responsabilidades que não são referidas em nenhuma política: Informação sobre a avaliação de riscos de segurança, Informação sobre tratamento de riscos de segurança, Classificação da informação, Antes do emprego, Mudança de emprego, Equipamento de segurança, Serviço de comércio electrónico, Controlos criptográficos, Gestão de vulnerabilidades técnicas e Continuidade do negócio

Avaliação e Tratamento de Riscos

A avaliação e tratamento de riscos abrange dois âmbitos diferentes que são: Informação sobre a avaliação de riscos de segurança e Informação sobre tratamento de riscos de segurança. Estes dois temas aparecem como sufixo do código "Directivas". O primeiro é mencionado em dois documentos e o segundo em um, e determinam que:

- "O departamento de informática, tão breve quanto possível, desencadeará e desenvolverá os mecanismos necessários e adequados para a resolução do problema". [Caso 7]
- "Todas as anomalias serão analisadas e tratadas de forma idêntica, salvaguardando, obviamente, questões de carácter prioritário, em consequência do quadro de pessoal existente". [Caso 7]

Tabela 41: Tipo de Responsabilidade por Política

	Políticas																									
Responsabilidades	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**Nº**	**%**
Política de seg da Informação	X	X	X		X	X		X	X			X			X		X	X				X				12	48
Organização interna da seg da informação			X			X			X						X		X					X		X		7	28
Partes externas															X											1	4
Responsabilidade pelos activos	X		X		X	X	X	X	X	X	X	X	X	X	X		X		X	X	X		X	X	X	20	80
Durante o emprego						X	X																			2	8
Áreas seguras								X	X						X											3	12
Procedimentos e responsabilidades operacionais			X		X	X	X	X	X		X	X	X		X				X	X		X		X	X	15	60
Entidade externa na prestação de serviços de gestão																		X								1	4
Planeamento e aceitação de sistemas			X																							1	4
Protecção contra códigos maliciosos	X		X		X			X	X		X	X	X		X				X			X	X	X		13	52
Backup			X		X	X	X	X	X		X	X	X		X	X	X		X				X		X	15	60
Gestão de segurança de rede	X		X	X		X		X	X	X		X	X													9	36
Manipulação de suportes informáticos			X				X					X			X											4	16
Troca de informação	X	X										X	X				X		X	X		X	X	X		10	40
Monitorização							X					X		X	X		X	X								6	24
Requisitos para o controle de acesso			X					X							X		X									4	16
Gestão de acessos dos utilizadores								X	X						X							X		X		5	20
Responsabilidades do utilizador	X		X			X		X	X			X			X		X	X		X	X	X	X	X		14	56
Controlo de acesso à rede			X		X	X		X	X		X		X				X		X	X	X			X		12	48
Controlo de acesso ao sistema operativo					X	X		X	X		X	X			X		X	X	X	X	X	X	X	X		15	60
Controlo de acesso às aplicações e à informação			X					X	X						X											4	16
Computação móvel e teletrabalho							X					X		X	X							X	X			6	24
Requisitos de seg dos SI							X								X											2	8
Processamento correcto de aplicações								X	X																	2	8
Segurança de ficheiros de sistema					X	X	X	X	X			X	X	X	X	X	X		X	X			X	X		15	60
Seg. em processos de desenvolvimento e suporte	X				X	X			X		X		X	X	X			X	X				X			11	44
Relatório de infor. de eventos e fraquezas de seg																		X								1	4
Gestão de incidentes de seg e melhorias																		X								1	4
Cumprimento dos requisitos legais								X	X					X	X		X					X		X		7	28
Cumprimento das normas de seg							X	X	X						X		X					X			X	7	28
Considerações de auditoria de SI								X	X					X												3	12
Outros objectos de segurança da informação	X				X	X					X								X			X				6	24

Política de Segurança da Informação

Este código diz respeito aos documentos que fornecem direcção e apoio para a segurança da informação, em conformidade com os requisitos de negócio e as leis e regulamentos pertinentes.

Aparece nas políticas em análise associado às directivas e às responsabilidades. Relativamente às directivas é citado em quatro documentos diferentes e aborda aspectos como:

- "Os computadores ligados em rede têm de obedecer aos procedimentos de segurança estabelecidos no documento". [Caso 8]
- "Procedimentos em conformidade com o determinado no documento". [Caso 9]
- "Obrigação de todos, no âmbito das suas funções, contribuírem para que os princípios gerais e os procedimentos de segurança sejam respeitados e os dispositivos de segurança se mantenham operacionais". [Caso 10]
- "Todos os utilizadores devem conhecer a Política Pessoal de Segurança". [Caso 12]

Relativamente às responsabilidades este tema é focado conforme o tipo de responsabilidade em três dos cinco tipos previstos: Dever, Obrigação e Recomendação, só o tipo proibição e outro tipo de responsabilidade é que não são considerados.

A frequência com que os documentos são citados é como "Dever" em 13 casos, como "Obrigação" em 11 casos e como "Recomendação" em dois casos.

Organização da Segurança da Informação

A organização da segurança da informação refere-se à estruturação dos esforços de segurança da informação e divide-se em dois âmbitos: Organização interna da segurança da informação e Partes externas. Este tema é utilizado como sufixo para directivas, requisitos e responsabilidades.

A organização interna da segurança da informação é citada nas três possibilidades. Como "Directivas" é citada em 9 casos, como "Requisito" em 4 casos e como "Responsabilidade" em 14 casos, divididos como "Dever" em 9 casos, como "Obrigação" em 3 casos e como "Proibição" em 2 casos.

Na sua maioria a organização interna da segurança da informação refere-se a responsabilidades, como um dever a cumprir pelos diferentes tipos de utilizadores, e determina que:

- "Responder pelo uso exclusivo e intransferível das suas senhas de acesso". [Caso 6]
- "Assegurar a integridade e a actualização dos dados que tenha o dever de tratar profissionalmente". [Caso 17]
- "Promover todas as medidas organizativas e técnicas necessárias ao bom funcionamento do sistema informático, à integridade e segurança das bases

de dados e à fidedignidade e correcta utilização dos dados pessoais, bem como ao planeamento gestão e implementação necessárias ao sistema informático". [Caso 17]

Quando a manutenção da segurança da informação é gerida por terceiros é citada em igual número como "Directivas" e "Responsabilidades". Ambos têm uma citação sendo no caso das responsabilidades um dever.
Como responsabilidade, determina que:

- "O desenvolvimento de software por elementos externos à organização deverá ser acompanhado por pessoal do Gabinete de Gestão de Sistemas de Infirmação de forma a garantir o domínio necessário e o conhecimento dos novos programas". [Caso 15]

Como directiva, determina que:

- "Nas comunicações com o exterior, sempre que possível devem ser utilizados mecanismos que garantam a certificação absoluta do ponto externo de onde faz a comunicação". [Caso 15]

Gestão de Activos

Por gestão de activos entende-se a gestão dos activos do SI, estando este supercódigo dividido em Responsabilidade pelos activos e Classificação da informação.

A responsabilidade pelos activos é citada nos três casos como sufixo de "Directivas", "Requisitos" e "Responsabilidades". Como "Directivas" é citada em 25 casos, como "Requisito" em 10 casos e como "Responsabilidade" em 70 casos, divididos como "Obrigação" em 29 casos, como "Proibição" em 21 casos, como "Dever" em 19 casos e como "Outro tipo de responsabilidade" em um caso.

A responsabilidade dos activos refere-se maioritariamente às responsabilidades que diferentes tipos de utilizadores têm. O tipo de responsabilidade que se destaca é o tipo obrigação, e determina o seguinte:

- "O Gabinete de informática ficará responsável pelo registo e actualização de todo o software conforme fornecido pelos respectivos fornecedores, instalando actualizações consoante venham a ser disponibilizadas, mantendo o controlo de todas as versões disponíveis na C.M". [Caso 6]
- "Gerir os contratos de manutenção dos equipamentos informáticos e de comunicações, bem como dos sistemas operativos e das aplicações comuns". [Caso 3]

A classificação da informação só é citada em três casos como sufixo do código "Directivas" e determina:

- "Acesso Reservado - Pastas de acesso reservado afectas aos Eleitos Locais e cargos de direcção e de chefia". [Caso 15]

Segurança dos Recursos Humanos

A segurança dos recursos humanos refere-se a procedimentos de segurança que se aplicam aos recursos humanos, abarcando três âmbitos diferentes: Antes do

emprego, Durante o emprego e Terminação ou mudança de emprego. Este tema é utilizado como sufixo para directivas, requisitos e responsabilidades.

O sufixo "antes do emprego" é citado em dois dos três casos possíveis. Como "Directivas" é citado em um caso e como "Requisito" em igual número. Como exemplo de Directiva tem-se:

- "Os novos colaboradores/utilizadores receberão o mesmo material por ocasião da sua admissão à rede informática da C.M.". [Caso 6]

O sufixo "durante o emprego" é citado em dois casos. Como "Directivas" é citado em cinco casos, como "Responsabilidade" em quatro casos referente à responsabilidade "Dever". Como exemplo de Directiva tem-se:

- "O acesso será prontamente restabelecido quando a segurança e o bem-estar ou os interesses puderem estar assegurados; a suspensão do acesso pode continuar se for resultado de uma acção disciplinar imposta pelos órgãos executivos do MC". [Caso 8]

O último sufixo "terminação ou mudança de emprego" é citado em dois dos três casos possíveis. Como "Directivas" é citado em oito casos e como "Requisito" em três casos. Como exemplo de Directiva tem-se:

- "Sempre que se verifiquem alterações ao nível dos recursos humanos as mesmas devem ser formalmente comunicadas ao Gabinete de Gestão de Sistemas de Informação, no intuito de serem criados, alterados, suspensos ou revogados os inerentes acessos para utilização das aplicações". [Caso 15]

Segurança Física e Ambiental

A segurança física e ambiental refere-se à protecção de áreas e equipamentos e divide-se em dois âmbitos diferentes: Áreas Seguras e Segurança de Equipamentos. Este tema é utilizado como sufixo para directivas, requisitos e responsabilidades.

As áreas de segurança são citadas nos três casos possíveis. Como "Directivas" é citada em 10 casos, como "Requisito" em um caso e como "Responsabilidade" em quatro casos. Como exemplo de Directiva tem-se:

- "As instalações físicas do gabinete de Sistemas de Informação devem merecer uma atenção especial, sem prejudicar a comunicação entre o pessoal do gabinete de gestão de sistemas de informação e os utilizadores dos sistemas". [Caso 15]

O sufixo "segurança de equipamentos" é citado em dois dos três casos possíveis. Como "Directivas" é citado em 17 casos e como "Requisito" em um caso. Como exemplo de Directiva tem-se:

- "A rede de energia eléctrica deverá ser instalada com respeito pelas especificações dos construtores dos equipamentos, devem existir sistemas de regulação autónoma e sistemas de fornecimento ininterrupto de energia, de forma a: Garantir o bom funcionamento dos equipamentos; Permitir o trabalho contínuo indispensável; Garantir a segurança básica dos equipamentos e instalações". [Caso 18]

Gestão de Comunicações e Operações

A gestão de comunicações e operações refere-se à gestão da informação segura e correcta e aborda dez âmbitos diferentes: Procedimentos e responsabilidades operacionais, Gestão da prestação de serviços por terceiros, Planeamento e aceitação de sistemas, Protecção contra códigos maliciosos, *Backup*, Gestão de segurança de redes, Manipulação de suportes informáticos, Troca de informação, Serviços de comércio electrónico e Monitorização. Este tema é utilizado como sufixo para directivas, requisitos e responsabilidades.

Os procedimentos e responsabilidades operacionais são citados nos três casos possíveis. Como "Directivas" é citado em 41 casos, como "Requisito" em seis casos e como "Responsabilidade" em 58 casos, divididos como "Obrigação" em 34 casos, como "Recomendação" em 11 casos, como "Proibição" em sete casos e como "Dever" em seis casos.

A gestão da prestação de serviços por terceiros é citada em dois dos três casos possíveis. Como "Requisito" em dois casos e como "Responsabilidade" em dois casos.

O planeamento e aceitação de sistemas é citado como "Responsabilidade" em um caso como uma "Obrigação".

A protecção contra códigos maliciosos é citada nos três casos possíveis. Como "Directivas" é citada em 10 casos, como "Requisito" em dois casos e como "Responsabilidade" em 31 casos, divididos como "Proibição" em 15 casos, como "Recomendação" em 12 casos, como "Dever" em um caso.

Backups são citados nos três casos possíveis. Como "Directivas" é citado em 15 casos, como "Requisito" em quatro casos e como "Responsabilidade" em 24 casos, divididos como "Obrigação" em 13 casos, como "Dever" em nove casos e como "Recomendação" em dois casos.

A gestão de segurança de rede é citada nos três casos possíveis. Como "Directivas" é citada em 21 casos, como "Requisito" em três casos e como "Responsabilidade" em 18 casos, divididos como "Proibição" em 12 casos e como "Obrigação" em seis casos.

A manipulação de suportes informáticos é citada nos três casos possíveis. Como "Directivas" é citada em 11 casos, como "Requisito" em um caso e como "Responsabilidade" em dez casos, divididos como "Dever" em 4 casos, como "Obrigação" em três casos, como "Recomendação" em dois casos e como "Proibição" em um caso.

A troca de informação é citada nos três casos possíveis. Como "Directivas" é citada em 28 casos, como "Requisito" em 20 casos e como "Responsabilidade" em 41 casos, divididos como "Proibição" em 29 casos, como "Dever" em sete casos, como "Obrigação" em quatro casos e como "Recomendação" em um caso.

Os serviços de comércio electrónico não são citados em nenhuma das três possibilidades.

A monitorização é citada nos três casos possíveis. Como "Directivas" é citada em 24 casos, como "Requisito" em quatro casos e como "Responsabilidade" em 16 casos, divididos como "Dever" em 13 casos e como "Obrigação" em três casos.

Do subcódigo gestão de comunicações e operações, destacam-se pelo número de citações os procedimentos e responsabilidades operacionais, a protecção contra códigos maliciosos e a troca de informação.

Realçam-se nos procedimentos e responsabilidades operacionais as directivas que lhe estão afectas e que determinam aspectos relacionados com o arranque e encerramento do computador, *backups*, manutenção de equipamento, mudança de instalações, entre outros:

- "Só a colaboradores afectos aos Serviços de Informática é permitido mover qualquer equipamento, dentro ou fora das Instalações da Câmara Municipal". [Caso 5]
- "Certos procedimentos de manutenção implicam que sejam parados e reiniciados os sistemas informáticos. Para evitar perdas de informação e outros riscos, estes procedimentos só devem ser efectuados se não existirem utilizadores activos na rede informática, podendo para isso, o administrador dos sistemas tomar as medidas convenientes". [Caso 10]

Destaca-se na protecção contra códigos maliciosos as proibições que lhe estão afectas, relacionadas com vírus, *worms*, etc:

- "Criar ou propagar vírus, danificar serviços e ficheiros". [Caso 8]
- "É proibido o envio de cartas para cadeias de solidariedade, caridade, concursos ou outros ganhos pessoais. O correio electrónico de origem desconhecida ou de conteúdo suspeito não deve ser aberto ou reenviado para qualquer funcionário, dentro ou fora do Município, devendo ser solicitada a ajuda do Gabinete de Informática". [Caso 19]

Realçam-se na troca de informação as proibições que lhe estão afectas e que determinam a troca de software dentro da organização e com qualquer entidade externa:

- "É proibido ouvir música, ver televisão e vídeos através da Internet, pois prejudicará o bom funcionamento da rede, salvo autorização do Presidente da Câmara Municipal". [Caso 20]
- "É proibida a participação em jogos on-line ou ter canais activos incluindo qualquer canal de conversação, como por exemplo o Messenger para uso que não seja estritamente profissional". [Caso 19]

Controlo de Acesso

O Controlo de acesso refere-se ao tratamento e acesso da informação e aborda sete âmbitos diferentes: Requisitos para o controlo de acesso, Gestão de acessos dos utilizadores, Responsabilidades do utilizador, Controlo de acesso à rede, Controlo de acesso ao sistema operativo, Controlo de acesso às aplicações e à informação e Computação móvel e teletrabalho.

Os requisitos para o controlo de acesso são citados nos três casos possíveis. Como "Directivas" é citado em 5 casos, como "Requisito" em dois casos e como "Responsabilidade" em 6 casos, divididos como "Obrigação" em três casos e como "Dever" em igual número.

A gestão de acessos dos utilizadores é citada nos três casos possíveis. Como "Directivas" é citada em 25 casos, como "Requisito" em nove casos e como "Responsabilidade" em seis casos, divididos como "Proibição" em três casos e como "Obrigações" em igual número.

As responsabilidades do utilizador são citadas nos três casos possíveis. Como "Directivas" é citada em 50 casos, como "Requisito" em um caso e como "Responsabilidade" em 41 casos, divididos como "Proibição" em 21 casos, como "Obrigações" em 19 casos e como "Recomendação" em um caso.

O controlo de acesso à rede é citado em dois dos três casos possíveis. Como "Directivas" é citado em 18 casos, como "Responsabilidade" em 45 casos, divididos como "Proibição" em 41 casos, como "Dever" em dois casos e como "Obrigação" em dois casos.

O controlo de acesso ao sistema operativo é citado em dois dos três casos possíveis. Como "Directivas" é citado em 10 casos, como "Responsabilidade" em 26 casos, divididos como "Proibição" em 21 casos, como "Dever" em 4 casos e como "Obrigação" em um caso.

O controlo de acesso às aplicações é citado nos três casos possíveis. Como "Directivas" é citado em 2 casos, como "Requisito" em um caso e como "Responsabilidade" em sete casos, divididos como "Recomendação" em 4 casos, como "Dever" em dois casos e como "Obrigação" em um caso.

A computação móvel e teletrabalho é citada nos três casos possíveis. Como "Directivas" é citada em sete casos, como "Requisito" em dois casos e como "Responsabilidade" em oito casos, divididos como "Obrigação" em quatro casos, como "Proibição" em três casos e como "Dever" em um caso.

O subcódigo controlo de acesso divide-se em diferentes temas, destacando-se as responsabilidades do utilizador e o controlo de acesso à rede. As responsabilidades do utilizador referem-se à selecção e uso de *passwords* e protecção de equipamentos. O controlo de acesso à rede refere-se ao acesso dos utilizadores internos e externos à rede.

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

A aquisição, desenvolvimento e manutenção de sistemas de informação refere-se aos procedimentos envolvidos na aquisição, desenvolvimento e manutenção de SI e aborda seis temáticas diferentes: Requisitos de segurança dos SI, Processamento correcto de aplicações, Controlos criptográficos, Segurança de ficheiros de sistema, Segurança em processos de desenvolvimento e suporte e Gestão de vulnerabilidades técnicas.

Os requisitos de segurança dos SI são citados em dois dos três casos possíveis. Como "Requisito" em seis casos e como "Responsabilidade" em três casos, divididos como "Dever" em dois casos e como "Obrigação" em um caso.

O processamento correcto de aplicações não é citado em nenhum dos três casos possíveis.

Os controlos criptográficos são citados como "Directivas" em três casos.

A segurança de ficheiros de sistema é citada nos três casos possíveis. Como "Directivas" é citada em seis casos, como "Requisito" em quatro casos e como "Responsabilidade" em 21 casos, divididos como "Proibição" em 12 casos, como "Dever" em cinco casos, como "Obrigação" em dois casos e como "Recomendação" em dois casos.

A segurança em processos de desenvolvimento e suporte é citada em dois dos três casos possíveis. Como "Directivas" é citada em cinco casos e como "Responsabilidade" em 16 casos, divididos como "Proibição" em oito casos, como "Obrigação" em cinco casos e como "Dever" em três casos.

A gestão de vulnerabilidades técnicas não é citada em nenhum dos três casos possíveis.

Gestão de Incidentes de Segurança de Informação

A Gestão de Incidentes de Segurança de Informação refere-se às actividades e procedimentos envolvidos na comunicação e gestão de incidentes de segurança da informação e fraquezas e aborda dois temas: Relatório de informação de eventos de segurança e fraquezas e Gestão de incidentes de segurança de informação e melhorias.

O relatório de informação de eventos de segurança e fraquezas é citado em dois dos três casos possíveis. Como "Directivas" é citado em dois casos e como "Responsabilidade" em um caso como "Dever".

A gestão de incidentes de segurança de informação e melhorias é citada em dois dos três casos possíveis. Como "Directivas" é citada em um caso e como "Responsabilidade" em três casos como "Dever".

Continuidade do Negócio

A gestão de continuidade do negócio no que diz respeito à segurança da informação é citada em dois casos como "Directivas", tendo-se a título ilustrativo:

- "De forma a garantir a funcionalidade do equipamento informático fundamental à continuidade dos serviços, devem existir contratos de manutenção que contemplem dois tipos de serviços: Manutenção preventiva; Manutenção correctiva". [Caso 18]

Observância

A observância refere-se à observação dos requisitos e aborda três temas: Cumprimento dos requisitos legais, Cumprimento das normas e políticas de segurança e cumprimento técnico e Considerações de auditoria de SI.

O cumprimento dos requisitos legais é citado nos três casos possíveis. Como "Directivas" é citado em 17 casos, como "Requisito" em 38 casos e como "Responsabilidade" em 16 casos, divididos como "Obrigação" em 10 casos, como "Dever" em três casos e como "Proibição" em três casos.

O cumprimento das normas de segurança e políticas e cumprimento técnico é citado nos três casos possíveis. Como "Directivas" é citado em seis casos, como "Requisito" em quatro casos e como "Responsabilidade" em nove casos, divididos como "Obrigação" em quatro casos, como "Proibição" em três casos e como "Dever" em dois casos.

As considerações de auditoria de SI são citadas nos três casos possíveis. Como "Directivas" são citadas em oito casos, como "Requisito" em três casos e como "Responsabilidade" em quatro casos, divididos como "Obrigação" em três casos e como "Dever" em um caso.

Após a análise individual de cada código, que no *codebook* dizem respeito aos códigos incluídos no código "*What*", outros códigos são analisados de seguida.

Responsabilidade do Dono da Política

A responsabilidade do dono da política pode ser subdivida em cinco âmbitos diferentes: Execução, Desenvolvimento, Revisão, Avaliação e Manutenção. Na totalidade das 25 políticas só em três (12%) casos são mencionadas responsabilidades do dono, contudo no mesmo documento há referência a responsabilidades de âmbitos diferentes. As diferentes responsabilidades focadas estão expostas na Tabela 42.

Responsabilidade do dono da política	Número
Execução	2
Desenvolvimento	1
Revisão	1
Avaliação	1
Manutenção	1

Tabela 42: Responsabilidade do Dono da Política

A atribuição ao dono da política da responsabilidade pela execução da política é mencionada duas vezes. Em um dos casos é indicado que "compete ao Órgão Executivo aprovar e manter em funcionamento a Norma de Controlo Interno das Aplicações e do Ambiente Informático adequado à Autarquia, assegurando o seu acompanhamento e avaliação permanente". [Caso 18]

Os restantes âmbitos de responsabilidade são mencionados uma única vez, nomeadamente na responsabilidade pela manutenção, revisão, desenvolvimento e avaliação da política de SSI. Como exemplo tem-se que é da "responsabilidade do Centro de Informática, sistemas e Telecomunicações a manutenção actualizada de um plano de segurança, assim como garantir a correcta aplicação dos procedimentos definidos". [Caso 18]

É de referir que um aspecto tão relevante como a responsabilidade do dono da política perante o desenvolvimento, revisão, avaliação e manutenção da política de SSI só seja referido em três documentos.

Comunicação de Incidentes de Segurança

Os procedimentos que os indivíduos devem usar para comunicar ameaças identificadas ou suspeitas, anomalias e incidentes estão descritos em três documentos.

Os utilizadores devem comunicar de imediato aos serviços de informática sempre que se detectem as seguintes situações:

- Situações anómalas com a utilização indevida e abusiva do sistema. [Caso 18]
- Violação ao regulamento ou à segurança. [Caso 23]
- Vírus, *worms, trojans* ou código informático malicioso. [Caso 1]

Coordenação entre Entidades Organizacionais

Entende-se por "Coordenação entre as entidades" uma declaração de como as várias entidades organizacionais coordenam as suas acções no âmbito da segurança da informação.

Nos documentos em análise verifica-se que em dois casos é referida essa coordenação. A coordenação verifica-se entre os seguintes serviços:

Coordenação	Número
Serviços do Município – Gabinete de Informática	2
Gabinete de Informática – Director de departamento	1

Tabela 43: Coordenação entre as Entidades

O tipo de coordenação centra-se nos seguintes âmbitos:

- Informação sobre todos os aspectos que dizem respeito ao gabinete de informática (uma citação – Serviço do Município e Gabinete de Informática).
- Promoção da melhoria das condições de utilização e optimização dos equipamentos informáticos e recursos associados (uma citação – Serviço do Município e Gabinete de Informática).
- Aquisição de hardware e software ou serviços externos (duas citações – Serviço do Município e Gabinete de Informática).
- Deslocação de equipamento entre diferentes serviços (uma citação – Serviço do Município e Gabinete de Informática), (uma citação – Gabinete de Informática e Património).

- Manutenção e actualização do inventário do equipamento (uma citação – Serviço do Município e Gabinete de Informática), (uma citação – Gabinete de Informática e Património).
- Indicação de hierarquia (uma citação - Gabinete de Informática e Director de Departamento).

Embora a coordenação entre entidades organizacionais esteja mencionada em sete políticas de SSI, verifica-se que as citações dessa coordenação são feitas em nove casos. Esta diferença deve-se ao facto de duas políticas mencionarem dois âmbitos de coordenação cada.

Atribuição de Recursos

Por "Atribuição de recursos" entende-se a nomeação de uma fonte (instalação, dinheiro, pessoal, equipamento) para a implementação dos controlos da segurança da informação.

Nos documentos em análise verifica-se que a "Atribuição de recursos" é mencionada em sete (28%) das políticas de SSI. A sua distribuição por tipo de atribuição está representada na Tabela 44.

Atribuição de recursos	Número
Software (Anti-vírus, *firewall*)	5
Equipamento informático	2
Formação dos utilizadores	1

Tabela 44: Atribuição de Recursos

Referido em cinco políticas, o software é utilizado para a implementação dos controlos da segurança da informação, nomeadamente para detectar de forma pró-activa vírus, *worms* ou *trojans*; a instalação de *firewall* é também referida como forma de proteger a rede e garantir a integridade dos dados e programas. Um exemplo são as mensagens com ficheiros anexos com conteúdo potencialmente perigoso ser devolvida ao remetente com um aviso. [Caso 12]

A atribuição de recursos a nível de equipamento informático (todos os custos imputáveis ao funcionamento e utilização normal do equipamento [Caso 14]) e formação dos utilizadores (não é mencionado o tipo de formação) depende como é referido da "disponibilidade financeira para cada ano e de acordo com o Plano de Actividades estabelecido, proceder-se-ão às actualizações indispensáveis e devidamente fundamentadas, a nível dos equipamentos, software e formação dos utilizadores". [Caso 7]

Ética relativa à Segurança

Declarações de natureza ética relativamente à segurança da informação aparecem só em um dos documentos. É referido dentro do ponto dedicado ao acesso à internet do seguinte modo "a manutenção das regras de ética é da responsabilidade de todos" [Caso 23], é também indicado que "os princípios éticos da utilização dos recursos de informática da autarquia são os expostos no preâmbulo deste regulamento" [Caso 23]. No preâmbulo é referido que "os recursos informáticos constituem um bem

valioso, fundamental para o funcionamento da autarquia. Os actos abusivos sobre eles praticados afectam todos aqueles que os utilizam e o seu impacto no exterior põe em causa a reputação e a imagem da mesma", seguindo-se a este parágrafo um conjunto de pontos onde é indicado como devem ser usados os serviços informáticos da Autarquia.

Ameaças

Entende-se por "Ameaças" uma potencial causa de incidente indesejado, que pode resultar em danos a um sistema organizacional.

Dos documentos em análise só em um (4%) deles é referida um conjunto de ameaças, ou seja, só em uma política de SSI [Caso 12] são expostas ameaças, entre elas:

> "O risco de integridade de dados surge quando a perda, a corrupção ou a modificação não autorizada de dados são eminentes".
> "O próprio utilizador pode causar, acidentalmente, a perda de dados, devido ao fraco conhecimento de uma aplicação, a utilização de uma metodologia imprópria ou por simples distracção".
> "O computador, a configuração incorrecta do seu hardware e/ou software, as aplicações, a sua incorrecta instalação e/ou configuração podem, igualmente, colocar em perigo a integridade dos dados".
> "O roubo de computadores, portáteis em particular, ou meios de arquivo, como CD's/DVD's ou de tapes de *backup*, podem obviamente causar uma grande perda de dados".
> "Os vírus podem representar uma séria ameaça à segurança dos dados".

Os danos que podem resultar dessas ameaças são os seguintes:

- Pôr em causa a integridade de dados
- Revelação de dados confidenciais
- Pôr em causa a fidelidade de dados
- Provocar o repúdio de dados
- Pôr em causa a segurança dos dados através do "ataque" de vírus

É de mencionar que os danos resultantes de uma potencial ameaça são todos direccionados para os dados e para a informação.

Punições

As consequências da violação da política de SSI são assinaladas em 15 (60%) documentos, número considerado significativo, mas entendível dado se tratar de punições a aplicar em caso de prevaricação. As punições a aplicar são as apresentadas na Tabela 45.

Punições	Número
Processo disciplinar	8
Acção criminal	7
Multas	3

Tabela 45: Punições

As transgressões na política de SSI que estão na origem das punições são as citadas na Tabela 46.

Transgressões	Número
Utilização de software ilegal	7
Violação do estipulado no regulamento	6
Utilização de recursos ou serviços para actividades ilegais	5
Actos previstos na Lei de Criminalidade Informática e outra legislação	4
Acesso não autorizado a um sistema	4
Quebra de confidencialidade	2

Tabela 46: Transgressões

As transgressões e punições anteriormente referidas são em quase todos os casos actos que vão afectar os utilizadores, com excepção da utilização ilegal de software, nomeadamente cópias não autorizadas de software, que poderão acarretar consequências legais, cíveis ou criminais, quer para a Edilidade e seus Dirigentes, quer para o funcionário ou colaborador que tenha procedido a tal acto.

Procedimento de Comunicação

Os mecanismos ou meios de comunicação a utilizar para comunicar a política de SSI aos seus alvos são indicados em cinco casos (20%).

A forma escrita (cópia da política) é o mecanismo utilizado em três casos, o correio electrónico em um caso, o mesmo número verifica-se para a utilização da internet e da intranet. Em um dos casos a forma de comunicação poder ser por correio electrónico ou de forma escrita.

Verifica-se, assim, que os mecanismos de comunicação da política de segurança são em 50% utilizando as TIC e nos restantes 50% de forma escrita em papel.

Alvo de Comunicação da Política

O destinatário da comunicação da política de segurança de SSI está previsto nos documentos em análise em seis casos, ou seja, em 24% dos documentos.

A incidência sobre os destinatários ou público do documento da política são nos seis casos todos os utilizadores. Só em um dos casos é que são todos os que têm acesso à Internet e ao correio electrónico. Nos restantes casos não especificam o alvo, a designação dos utilizadores é que varia entre: trabalhadores, colaboradores, funcionários e terceiros.

Declaração de Conhecimento

A declaração assinada pelo utilizador em como se responsabiliza no que diz respeito à segurança da informação faz parte de nove (36%) políticas de SSI.

Um exemplo de "declaração" compreende após o título o nome do funcionário, seguindo-se um parágrafo com o conteúdo que o funcionário se compromete a tomar conhecimento e acatar o previsto no regulamento/norma. No final a declaração tem a data e a assinatura do funcionário.

Data de Conhecimento

A data em que o utilizador teve conhecimento da política de SSI está indicada em quatro (16%) documentos, ou seja, há declarações em que o utilizador se responsabiliza em como tomou conhecimento, mas onde não consta a data em que tomou esse conhecimento, uma vez que o utilizador tem conhecimento em nove documentos e só em quatro é que a data está inserida.

Quando se refere que o utilizador tomou conhecimento em nove dos documentos, significa dizer que essa declaração está inserida na política, estando previsto um campo específico para aquele assinar. Uma vez que as políticas de SSI são maioritariamente dirigidas aos utilizadores eles têm de conhecer os regulamentos, contudo alguns documentos não têm mencionado no documento essa responsabilização.

Localização da Política de SSI

O número de documentos que fazem referência ao local onde vai ser colocada a política é de seis. Os locais referidos encontram-se listados na Tabela 47.

Locais	Número
Intranet	2
Procedimentos internos	1
Apenso à acta de aprovação	1
Correio electrónico interno	1
Sector da Informática	1

Tabela 47: Localização do Documento

Verifica-se que em metade dos casos são utilizados meios informáticos para o seu armazenamento, o formato em papel é utilizado em dois casos, quando é referido que são utilizados os procedimentos internos, não é explicitado de que tipo de procedimento se trata.

Autor da Política

A função ou nome da pessoa ou entidade que elaborou a política é mencionado em nove (36%) políticas de SSI. A indicação de quem elaborou a política encontra-se na Tabela 48.

Autor da Política	Número
Gabinete de informática	4
Chefe de Divisão de Informática	2
Chefe de Departamento/Serviço	2
Departamento de Administração Geral	1

Tabela 48: Autor da Política

Em seis das nove políticas foi o gabinete de informática que elaborou a política, em dois dos casos é só mencionado ou apresentado pelo chefe departamento/serviço sem indicar a que unidade orgânica pertence.

Data da Elaboração, Aprovação, Entrada em Vigor e Revisão

As datas de elaboração, aprovação, entrada em vigor e revisão são mencionadas em 21 políticas de SSI. Essa distribuição apresenta-se na Tabela 49. Com excepção da data de aprovação que está em 12 documentos, as outras datas são em número reduzido. Estes resultados levantam uma questão evidente que é a de qualquer documento deveria ter sempre a data de elaboração, aprovação e entrada em vigor, principalmente um documento intitulado por normas, regulamentos ou regras.

A data da revisão só é mencionada em um dos casos, mas esta diferencia-se das anteriores pois só pode existir se alguma revisão tiver ocorrido.

Datas da Política	Número
Data de aprovação	12
Data de elaboração	4
Data de entrada em vigor	4
Data da revisão	1

Tabela 49: Datas da Política

Verifica-se também que a data da aprovação aparece em alguns casos diferente da data da elaboração que por sua vez também difere da data de entrada em vigor. Por exemplo, a data de entrada em vigor é única em um dos casos, ou seja, não é feita referência nem à data de elaboração nem da aprovação.

Aprovação da Política

A aprovação da política de SSI pode ser em forma de declaração do responsável pelo órgão onde foi aprovada a política. A aprovação pode, por exemplo, assumir a forma de uma assinatura de um dos elementos do Executivo.

Nos documentos em análise a aprovação da política está patente em 13 (52%) casos. Os agentes que aprovaram as políticas são apresentados na Tabela 50.

Verifica-se que com excepção de dois documentos todos os restantes são aprovados pelo executivo da Câmara Municipal, quer pela totalidade do executivo quando é aprovado em Reunião de Câmara ou individualmente por algum dos seus elementos, nos restantes casos.

Aprovação da política	Número
Reunião de Câmara	7
Presidente da Câmara	2
Vice-Presidente	2
Assembleia Municipal	1
Vereador	1
Chefe de Divisão	1

Tabela 50: Aprovação da Política

O número de documentos aprovados é diferente dos apresentados na tabela, pelo facto de uma política ser constituída por dois documentos, em que um foi aprovado pelo Chefe de Divisão e outro pelo Presidente de Câmara.

Data da Revisão

A data ou período em que se procederá a uma revisão formal à política estão previstas em dois (8%) casos. A indicação pode revestir a forma de uma data precisa ou pode apontar para um intervalo de tempo após o qual deverá ser revista.

Nas políticas de SSI em análise verifica-se que em um dos casos há indicação de um ano como intervalo entre as revisões, no outro caso menciona-se que as normas deverão ser revistas sempre que se torne necessário.

Aprovação das Revisões

A aprovação da revisão, que só é possível em documentos que foram submetidos a um processo de revisão, aparece nas políticas em análise em um (4%) caso. Essa alteração é proposta por um Técnico de Informática que posteriormente mereceu o despacho dos superiores hierárquicos com a aprovação da revisão proposta.

Contactos

Os contractos podem ser subdivididos em contactos para solicitar excepções, para sugerir actualizações, para mais informações, receber orientações, esclarecimentos de questões e dúvidas, para notificação de incidentes e para outros fins.

Das 25 políticas de SSI 18 (72%) fazem referência a contactos de várias ordens, conforme se pode observar na Tabela 51.

Tipos de Contractos	Número
Notificação de incidentes	6
Receber orientações, esclarecimentos de questões e dúvidas	6
Solicitar excepções	3
Sugerir actualizações	2
Outros fins	13

Tabela 51: Tipos de Contactos

Conforme se verifica na tabela anterior, há vários tipos de contactos na mesma política, daí a diferença entre as 18 políticas que mencionam contactos e o número total do tipo de contacto. O tipo de contacto “outros fins” desta-se nas citações, que

vão desde a comunicação de uso ilícito ou indevido de software a vários tipos de avarias.

6.4 Conclusão

Neste capítulo, após uma breve introdução apresentou-se a análise conjunta das características das políticas de SSI, seguindo-se a análise conjunta das políticas de SSI na vertente das componentes.

Um ponto que merece referência neste capítulo é a aplicabilidade do software Atlas.ti na realização de análise de conteúdo na área das políticas de SSI. A análise da junção dos documentos das políticas de SSI iniciou-se com o acesso ao *codebook* e a sua aplicabilidade nos documentos, desse trabalho resultou a obtenção de 294 códigos. Seguiram-se os passos inerentes à análise com a criação de famílias e estabelecimento de relações entre os diferentes códigos e citações e terminou com a recolha dos dados.

A quantidade de códigos criados evidencia, por um lado, a complexidade que compreende a presente análise e, por outro, a riqueza de detalhe que os dados recolhidos possuem.

Capítulo 7

Análise das Entrevistas

7.1 Introdução

Neste Capítulo apresenta-se o estudo dos dados resultantes da análise das entrevistas realizadas nas Câmaras Municipais Portuguesas.

No universo das 308 Câmaras Municipais existentes em Portugal continental e regiões autónomas da Madeira e dos Açores foram entrevistados 44 responsáveis ou funcionários autárquicos, entre eles, Vereadores, Directores e técnicos do departamento de informática. De referir que os entrevistados, independentemente do cargo ocupado na Câmara Municipal, eram responsáveis pela área de informática.

A selecção dos Municípios onde realizar as entrevistas foi feita tendo por base a dimensão eleitoral dos mesmos, bem como os *Clusters* definidos para este estudo. Desta forma, as 44 Câmaras em que se procedeu a entrevistas distribuem-se de acordo com o apresentado na Tabela 52.

Critério	Número
Clusters	
Cluster 1 (Câmaras que têm uma política de SSI)	11
Cluster 2 (Câmaras que não têm uma política de SSI, mas estão em processo de formulação)	11
Cluster 3 (Câmaras que não têm uma política de SSI, mas têm intenção de adoptar uma política de SSI)	11
Cluster 4 (Câmaras que não têm uma política de SSI e não têm intenção de adoptar uma política de SSI)	11
Dimensão	
Classe A (Autarquias muito grandes)	5
Classe B (Autarquias grandes)	7
Classe C (Autarquias médias)	27
Classe D (Autarquias pequenas)	5

Tabela 52: Classificação dos Municípios em que se Realizaram Entrevistas

A distribuição individual de cada entrevista por *Cluster* e dimensão eleitoral da Câmara correspondente é feita na Tabela 53.

Das 18 capitais de distrito existentes em Portugal continental, 11 foram contempladas neste estudo. Relativamente à sua posição em relação aos *Clusters* considerados no âmbito desde estudo, a sua distribuição é uniforme, tendo sido contempladas 11 dentro de cada um. Em relação à Dimensão da Autarquia a sua distribuição foi a seguinte: 25% consideradas Autarquias muito grandes (o número

total é 20), 33% Autarquias grandes (o número total é 21), 18% Autarquias médias (o número total é 150) e 4% Autarquias pequenas (o número total é 117).

Entrevista	*Cluster*	Dimensão	Entrevista	*Cluster*	Dimensão
1	C 4	Classe C	23	C 2	Classe A
2	C 4	Classe D	24	C 2	Classe A
3	C 1	Classe C	25	C 1	Classe B
4	C 3	Classe A	26	C 4	Classe C
5	C 3	Classe C	27	C 3	Classe C
6	C 1	Classe C	28	C 2	Classe A
7	C 4	Classe C	29	C 1	Classe C
8	C 3	Classe C	30	C 1	Classe C
9	C 3	Classe C	31	C 3	Classe B
10	C 3	Classe D	32	C 1	Classe C
11	C 2	Classe C	33	C 4	Classe C
12	C 4	Classe C	34	C 1	Classe B
13	C 3	Classe C	35	C 3	Classe B
14	C 4	Classe C	36	C 1	Classe C
15	C 1	Classe C	37	C 1	Classe C
16	C 2	Classe C	38	C 2	Classe B
17	C 3	Classe C	39	C 4	Classe B
18	C 2	Classe C	40	C 2	Classe B
19	C 4	Classe C	41	C 2	Classe A
20	C 1	Classe C	42	C 3	Classe D
21	C 2	Classe C	43	C 4	Classe C
22	C 4	Classe C	44	C 2	Classe D

Tabela 53: Lista das Câmaras em que se Realizaram Entrevistas

No capítulo desenvolve-se a análise dos dados ao longo de cinco secções. Após a introdução, na secção 7.2 é apresentada a análise das 44 entrevistas de forma individual, na secção 7.3 a análise das entrevistas apresenta-se na forma intra-*cluster* e na secção 7.4 apresenta-se a análise das entrevistas inter-*clusters*. Na última secção são apresentadas as conclusões principais do capítulo.

Neste capítulo procuram-se analisar os dados que posteriormente vão sustentar a resposta às questões de investigação números 1 e 3, designadamente "Que factores condicionam (facilitando ou inibindo) a adopção e políticas de SSI nas Câmaras Municipais Portuguesas?" e "De que forma se articulam os factores condicionantes da adopção de políticas de SSI no âmbito das Câmaras Municipais Portuguesas?" e, parcialmente, à questão de investigação número 4, cuja formulação é "Que recomendações poderão ser avançadas de forma a potenciar a adopção de políticas de SSI nas Câmaras Municipais Portuguesas?".

Conforme referido, estes resultados serão apresentados tendo por base três fases distintas da análise das entrevistas:

- Análise individual
- Análise intra-*cluster*
- Análise inter-*clusters*

O processo de análise foi suportado informaticamente pelo software de análise de dados qualitativos Atlas.ti. Na codificação dos dados recorreu-se à lista de códigos inicialmente elaborada para esse fim, tendo o *codebook* sido apresentado no Capítulo 5 – "Descrição do Estudo", no ponto inerente à "Análise dos Dados", e disponibilizado no Apêndice G.

Não se encerra esta secção introdutória sem se tecerem algumas considerações quanto à forma como as entrevistas decorreram. É importante mencionar estas considerações para que não se desenvolva a percepção de que as entrevistas foram processos de geração de dados lineares e passivos. Na base destes comentários encontra-se a oralidade destas técnicas de geração de dados. Assim, observou-se que por vezes, certos comentários dos entrevistados diziam respeito a questões que só iriam ser colocadas posteriormente. Outro aspecto a apreciar é que inicialmente se considerou que o número razoável de entrevistas para este tipo de estudo estaria compreendido entre 35 a 40, contudo no decorrer da realização das mesmas, verificou-se que algumas não correspondiam às expectativas, uma vez que as respostas ficaram aquém do pretendido em termos da riqueza do seu conteúdo, constatando-se uma certa dispersão e ideias apenas afloradas. Assim, foram realizadas mais quatro entrevistas, perfazendo assim o número de 44 entrevistas realizadas.

Ao longo do capítulo são apresentados alguns extractos retirados das entrevistas, identificados na forma [CX.Y], onde "CX" é o *Cluster* a que a entrevista pertence e "Y" o número da entrevista de onde foi retirado.

7.2 Análise Individual

A análise de cada caso individualmente iniciou-se com a leitura de todas as entrevistas, depois de devidamente transcritas, e tendo em conta os quatro guiões elaborados para a realização das entrevistas (apresentados no Capítulo 5 "Descrição do Estudo", no ponto referente às "Técnicas de Geração de Dados"), pois o número de questionários é o mesmo que o número de *clusters.*

A partir desses guiões identificaram-se os aspectos significativos que serviram de base para a elaboração do *codebook*, que tornou possível que os códigos se mantivessem homogéneos durante todo o processo de codificação e posterior análise.

O *codebook* e as *coding instructions* foram desenvolvidos no âmbito deste trabalho, para servirem de base para todo o processo de codificação. Uma forma de sistematizar os conteúdos a acrescentar aos comentários dos códigos é seguir o modelo proposto por MacQueen et al. [1998] que identifica como comentários a associar a cada código: o nome do código, uma descrição breve, uma descrição ampla, indicação de quando usar, indicação de quando não usar e um exemplo. Este modelo foi seguido na elaboração do *codebook*, onde cada código foi descrito numa tabela estando nela definidos todos estes pontos abordados por MacQueen et al. [1998].

A análise de cada caso individualmente culminou com a codificação das 44 entrevistas utilizando para o efeito o software Atlas.ti. A codificação conjunta das entrevistas requereu a aplicação dos 49 códigos definidos no *Codebook* previamente elaborado.

Após a codificação tendo por base o *codebook* referido e as *coding instructions*, optou-se por criar quatro famílias de documentos (*Cluster 1*, *Cluster 2*, *Cluster 3* e *Cluster 4*), com o conteúdo das entrevistas pertencentes a cada um dos *clusters*.

A transcrição das entrevistas do formato áudio para formato de texto e posteriormente para o formato elegível para o Atlas.ti, bem como o carregamento para o Atlas.ti dos códigos a aplicar retirados do *codebook*, requereu algumas horas de trabalho. A transcrição das entrevistas demorou 66 horas, o que equivale em média a 1.3 horas por entrevista. O tempo total de codificação perfez 18 horas, o que equivale em média a 25 minutos por entrevista. A codificação efectiva das entrevistas iniciou-se a 8 de Setembro de 2010 e terminou a 14 de Setembro de 2010.

7.3 Análise Intra-Cluster

Nesta secção analisam-se as entrevistas agrupadas no mesmo *cluster*. Assim, serão analisadas conjuntamente todas as entrevistas pertencentes ao *Cluster* 1, ou seja, aquelas referentes a Câmaras que já têm uma política de SSI, as que pertencem ao *Cluster* 2, que não têm implementada uma política de SSI, mas estão em processo de formulação ou adopção, as do Cl*uster* 3 que não têm uma política de SSI, mas que têm intenção de as adoptar e as pertencentes ao *Cluster* 4 que não têm uma política de SSI e não têm intenção de as adoptar.

A análise *intra-cluster* apresenta os resultados individuais de cada *cluster* divididos por diferentes perspectivas, alcançando os códigos aplicados resultantes do *codebook*, pois são estes que evidenciam as diferentes perspectivas presentes nas entrevistas, estando por sua vez subdivididos nas componentes do enquadramento apresentado no Capítulo 5,designadamente “Conteúdo”, “Processo” e o “Contexto”.

7.3.1 Cluster 1

Esta subsecção debruça-se sobre as temáticas contidas no guião que serviu de base para a realização das entrevistas às Câmaras Municipais que se enquadram neste *Cluster* e aborda os seguintes tópicos: Benefícios das Políticas, Processo – Formulação, Processo – Implementação, Processo – Revisão, Contexto – Externo e Contexto – Interno.

A primeira perspectiva diz respeito à dimensão “Benefícios”, que aborda aspectos associados aos benefícios esperados com uma política e se os mesmos se concretizaram.

Benefícios das Políticas

No que respeita aos benefícios esperados com a adopção da política obteve-se a agregação das respostas apresentada na Tabela 54.

Benefícios Esperados de uma Política de SSI	Número
Melhor desempenho das TIC	4
Maior controlo no acesso às TIC	4
Diminuição do acompanhamento pelo departamento de informática	3
Informação dos utilizadores	2

Tabela 54: Benefícios Esperados com uma Política de SSI (*Cluster* 1)

Conforme se observa na tabela anterior, um dos benefícios mais esperados vai de encontro às TIC, nomeadamente em termos de velocidade de transferência, salvaguarda da informação, como se pode apreciar nas seguintes transcrições:

"Os benefícios passam por não se perderem documentos importantes,…". [C1.29]

"Uma maior rapidez na rede". [C1.30]

Em igual número que a "melhoria do desempenho das TIC" está o "maior controlo no acesso às TIC", nomeadamente em termos de delimitar acessos e evitar problemas com abusos ao nível de utilização dos e-mails e da Internet. Como exemplos deste benefício indicam-se:

"… com a criação da política de SSI iria deixar de haver abusos, deixamos de ter problemas com programas ilegais, com abusos ao nível da utilização dos e-mails e da internet, porque havia alguns, e as pessoas ficaram muito mais restringidas". [C1.32]

"Melhor controlo dos acessos à Internet". [C1.20 e C1.37]

Segue-se a diminuição do acompanhamento pelo departamento de informática, com três citações, entre elas:

"… diminuir a monitorização do nosso lado (Gabinete de informática), … nem precisam de tanto apoio nosso, nem de monitorização constante". [C1.3]

" … em termos de gestão, facilita-nos bastante quanto à gestão da infra-estrutura". [C1.29]

Com duas citações está a informação aos utilizadores, nomeadamente:

"… quase uma formação interna aos utilizadores, alertando-os quer para os perigos, quer para as boas práticas que se devem ter". [C1.15]

"Por um lado permitir que todos passem a saber como comportar-se nos mais diferentes aspectos". [C1.6]

Questionados sobre se os benefícios esperados com a política se concretizaram, mereceram resposta positiva a totalidade das respostas a esta questão, podendo-se mencionar os seguintes (cf. Tabela 55):

Benefícios Concretizados com a Política de SSI	Número
Diminuição do número de intervenções por má utilização ou erro humano	2
Utilizadores mais informados	1
Melhor velocidade da rede informática	1
Os sistemas foram implementados com mais segurança e estabilidade	1

Tabela 55: Benefícios Concretizados com uma Política de SSI (*Cluster* 1)

O primeiro benefício diz respeito à diminuição da monitorização do departamento de informática com a implementação da política de SSI, o segundo e terceiro benefícios dizem respeito ao benefício apontado como esperado com uma política de SSI que é manter os utilizadores informados e maior velocidade na rede informática da Câmara, e o último benefício diz respeito á implementação dos sistemas com mais segurança e estabilidade.

Estas mais-valias surgiram porque os benefícios esperados com a política se concretizaram, só em cinco casos foi mencionado que benefícios foram, os restantes responderam só que efectivamente se verificou a concretização dos objectivos. Como citação que ilustra que os benefícios efectivamente se concretizaram, relativamente à "Diminuição do número de intervenções por mau uso ou erro humano" indica-se:

> "significando que o número de intervenções por mau uso ou erro humano, quase que desapareceram". [C1.15]

Segue-se outro tópico que diz respeito à dimensão "Processo", que aborda aspectos associados a processos de formulação, implementação e revisão das políticas de SSI.

Processo – Formulação

Os aspectos relacionados com o processo da formulação da política de SSI focam diferentes perspectivas, entre elas de como foi formulada a política, quem a elaborou, os problemas na formulação e soluções para resolver problemas experimentados na formulação da política.

Os entrevistados questionados sobre quem elaborou a política de SSI, responderam que em sete (64%) dos casos foi elaborada pelo departamento de informática. Em dois casos foi pelo Vereador do Pelouro da Informática, em uma das Câmaras foi pelo Gabinete de Informática com o apoio do Gabinete Jurídico, em um dos casos foi também com o apoio do Gabinete Jurídico, mas elaborada pelo Vereador. Os dados relativos a quem elaborou a política são apresentados na Tabela 56.

Como se observa, o gabinete de informática destaca-se dos demais órgãos como o responsável pela elaboração do documento.

Autor da Política	Número
Gabinete de Informática	7
Vereador	2
Gabinete de Informática mais Gabinete Jurídico	1
Vereador mais Gabinete Jurídico	1

Tabela 56: Autor da Política (*Cluster* 1)

Questionados sobre como formularam a política de SSI, as respostas obtidas agrupam-se em seis classes, conforme se pode observar na Tabela 57.

Formulação da Política	Número
Com base nas necessidades	4
Apoiada em política de outra Câmara	2
Pesquisaram na Internet	2
Com ajuda externa	1
Em agrupamento com outras Câmaras	1
Escrita de mensagens para acções de sensibilização	1

Tabela 57: Formulação da Política (*Cluster* 1)

Com maior número, as respostas incidiram sobre a política de SSI ter sido criada de acordo com as necessidades, ou seja, foi a prática que lhes mostrou "quais eram as coisas que deviam ser atalhadas, o que era absolutamente inconveniente, transpondo essas necessidades sentidas para um documento". [C1.34]

Outra forma utilizada para formular a política foi "pedindo a outras Câmaras que já tinham adoptado uma política que lhes disponibilizassem o documento. Com esse documento foi feito outro pelo gabinete de informática adaptada aos serviços do Município". [C1.6]

Uma Câmara indicou que a política foi formulada "através de pesquisa na Internet sobre como formular políticas de SSI". [C1.32]

Outra referiu que foi "com ajuda externa, através de uma empresa de informática que colaborava com a Câmara". [C1.36]

Um Município elaborou a política "em agrupamento com outras Câmaras e depois adaptou-a a regulamento interno de acordo com a realidade da Câmara em questão". [C1.30]

Outra Câmara mencionou que "fizeram várias normas, mas que as mesmas ao fim de algum tempo eram esquecidas e para ultrapassar essa questão elaboraram acções de sensibilização e divulgam, por exemplo, semanalmente ou quando acham que é necessário". [C1.3]

Relativamente aos métodos de formulação só um entrevistado (alguns já o fizeram aquando da questão de como foi formulada a política) referiu que foi por iniciativa do Gabinete de Informática e que recorreram a pesquisas na Internet, para procurar modelos que lhes pudesse servir de base para a formulação de uma política de SSI para a Câmara, referindo que "…foi por iniciativa do núcleo de Informática e

utilizamos a internet para ir explorar modelos. Encontramos um modelo padrão e adaptamo-lo às necessidades da Câmara". [C1.20]

Os problemas experimentados na formulação da política, mencionados por dois inquiridos, são problemas:

> "… inerentes ao arranque de qualquer processo, nomeadamente a falta de vontade dos utilizadores". [C1.25]
>
> "… falta de um modelo de política de SSI a seguir e pouca informação sobre esta temática". [C1.36]

A existência de um modelo de uma política de SSI pelo qual as Câmaras Municipais se pudessem orientar para a formular do seu documento constituiria uma mais-valia para as autarquias.

Processo – Implementação

Os aspectos relacionados com a implementação da política de SSI vão desde como foi implementada a política, a problemas que surgiram e possíveis soluções, incluindo a identificação do responsável pela observância da política, o cumprimento da política e o grau de satisfação com a implementação da política.

Questionados sobre como foi implementada a política de SSI, obtiveram-se as respostas que sinteticamente se apresentam na Tabela 58. Com vista à implementação da Política de SSI é necessária a consciencialização dos utilizadores e dirigentes da obrigatoriedade de utilizar essa política com o máximo rigor e seriedade.

Implementação da Política	Número
Distribuída em papel	5
Distribuída via Intranet	3
Distribuída via Correio Electrónico	2
Lembretes no computador de cada utilizador	1

Tabela 58: Implementação da Política (*Cluster* 1)

A forma como chegam aos utilizadores é por diferentes vias, sendo a mais usual em formato de papel, seguindo-se a distribuição na Intranet. Em dois casos é feita por via de correio electrónico e por fim, em um dos casos, por lembretes no computador de cada utilizador.

As TIC são o meio utilizado para a distribuição da política de SSI em seis (55%) casos, o formato de papel é utilizado nos restantes cinco (45%) casos. A forma como a política foi distribuída configura a implementação da política em termos práticos, ou seja, como ela chega aos destinatários.

Relativamente a problemas detectados aquando da implementação da política de SSI, em seis (55%) casos não se verificaram quaisquer problemas e nos restantes cinco (45%) casos foi detectado um problema que é o mesmo na totalidade dos casos.

O problema mencionado foi o da resistência dos utilizadores à política, conforme se pode observar nos extractos seguintes:

> "Notou-se algum cepticismo e incredulidade no início da implementação da política que se foi desvanecendo com o passar do tempo". [C1.29]
>
> "Surgem sempre bastantes dificuldades. Há pessoas que não conseguem perceber que aquele é o local de trabalho, e tratam os equipamentos como sendo equipamentos pessoais … ". [C1.3]
>
> "Houve por parte de alguns utilizadores uma certa resistência, … ". [C1.6]

Relativamente à resolução dos problemas experimentados na implementação, "no princípio houve uma reacção menos boa por parte dos utilizadores, mas neste processo como em outros, teve que haver um reajustamento por parte desses mesmos utilizadores e esse problema foi facilmente ultrapassado" [C1.32]. Uma resposta idêntica indica que "houve por parte de alguns utilizadores uma certa resistência, que há sempre, mas depois foi tudo pacífico" [C1.6]. Em alguns casos foram tomadas medidas, "aqueles que não fizeram esse reajuste o acesso a alguns sítios da Internet foi-lhes negado". [C1.3]

Questionados sobre quem é responsável pela observância ou cumprimento da política de SSI, os resultados são visíveis na Tabela 59. Conforme se observa, não há unanimidade em termos de quem deve ser responsável pela implementação da política: as respostas variam entre o gabinete de informática e o vereador responsável pela informática, embora na maioria dos casos essa responsabilidade seja do gabinete de informática.

Responsável pela Implementação	Número
Gabinete de Informática	6
Director do Gabinete de Informática	2
Técnico de Informática	1
Gabinete de Informática e Chefes de Divisão	1
Vereador	1

Tabela 59: Responsável pela Observância e Cumprimento da Política (*Cluster* 1)

Como exemplos em que é o gabinete de informática o responsável pela observância ou cumprimento da política tem-se:

> "somos responsáveis pala política e pelo cumprimento da política. Mas não quer dizer que nós tenhamos as sete horas de trabalho diárias a ver quem prevaricou ou não… Claro que tiramos depois as estatísticas mensais também para dar a conhecer ao Vereador". [C1.6]

> "… não ando todos os dias junto das pessoas para verificar o que elas andam a fazer nos computadores... as pessoas têm que ser responsáveis, as regras estão estabelecidas, e se alguém está a prevaricar em excesso, conseguimos prová-lo. Os registos informáticos estão feitos e a partir daí sabemos se há abusos por parte das pessoas ao nível da internet, ao nível do e-mail". [C1.32]

Questionados sobre se os utilizadores cumprem o descrito na política, no dia-a-dia, as respostas foram unânimes tendo todos respondido afirmativamente.

Questionados se estão satisfeitos com a implementação da política de SSI a resposta reúne consenso à volta do sim. Estão satisfeitos com a política, contudo têm a percepção de que eventualmente poderá ser melhorada, mas que até ao momento tem sido eficaz para o propósito para a qual foi criada.

Relativamente à satisfação dos utilizadores com a política de SSI, as respostas não são unânimes: em oito respostas, cinco são inequivocamente sim, mas em três casos os inquiridos respondem que é impossível quando se trata de normas e regras novas que sejam do agrado de todos, ou seja, uns estão serenos e satisfeitos com as restrições impostas outros mantêm-se com algumas resistências.

Processo – Revisão

Relativamente às revisões que uma política deve ter periodicamente, várias questões foram colocadas.

Questionados de como foi feita a revisão da política dos 11 inquiridos, sete nunca fizeram nenhuma revisão na política em vigor, quatro já fizeram uma revisão e um dos entrevistados manifestou intenção de fazer a revisão brevemente. Estes dados podem ser observados na Tabela 60.

Revisão da Política	Número
A política ainda não foi revista	6
A política já foi revista alguma vez	4
Há intenção de fazer a revisão brevemente	1

Tabela 60: Revisão da Política

Os resultados da revisão são concretizados em um dos casos através da emissão de folhetos actualizados.

Em dois outros Municípios a revisão ocorreu adaptando a política existente às novas aplicações informáticas, como se evidencia seguidamente:

> "tivemos que acabar com o Messenger, foi uma das situações que tivemos que resolver por causa dessa situação. Em termos de ficheiros de vídeo o youtube. Foi mais por causa desses exemplos que nós procedemos à revisão da política". [C1.6]

> "… o que acontece é que cada utilizador já tem o seu próprio computador no serviço, mas trazem mais o portátil para trabalhar, e então foi necessário fazer o bloqueio desses acessos". [C1.29]

Em outro caso é revista no início de cada mandato autárquico.

Nos seis casos em que ainda não se efectuou nenhuma revisão, tal deve-se ao facto de as políticas serem recentes ou não ter sido necessário alterar o documento.

Em um caso a revisão vai ser feita brevemente, pelo facto de já se encontrar desactualizada em relação a aplicações informáticas recentes sobre as quais é necessário definir proibições e deveres dos utilizadores, de forma a salvaguardar a segurança da informação, "neste momento estamos a iniciar um processo de

aquisição de um novo *data center*, que vai mudar um pouco as políticas que nós temos na Câmara e isso vai-nos obrigar também a alterar o documento que escrevemos inicialmente". [C1.36]

Relativamente à aprovação da revisão só em um dos casos é referido que as revisões são aprovadas e em que órgão, nomeadamente pelo Presidente da Autarquia, uma vez em cada início de mandato.

Questionados sobre com que periodicidade devem ser feitas as revisões da política de SSI, em cinco casos nunca foi definida essa periodicidade, em outros cinco casos é mencionado que as revisões serão feitas sempre que se justifique e em um dos casos está definido que é sempre que há mudança de executivo, ou seja, pelo menos de quatro em quatro anos.

Periodicidade das Revisões	Número
Não está definida	5
Quando for necessário	5
Mudança de Executivo	1

Tabela 61: Periodicidade das Revisões

Segue-se a dimensão "Contexto", que incide sobre os factores facilitadores e inibidores da adopção de políticas de SSI pelas Câmaras Municipais, com ênfase no contexto interno e externo.

Contexto – Externo

Entende-se por "Contexto externo" os factores económicos, políticos, legais, etc., que influenciam a adopção de políticas de SSI.

Só um dos entrevistados mencionou um factor externo, considerado fundamental para que uma política não tenha sucesso no âmbito de uma Câmara que é a não contemplação de financiamento para formação dos utilizadores das autarquias em TIC no âmbito de programas governamentais ligados às TIC em que as Autarquias são os agentes implementadores.

Neste caso é pois referido um factor político. Se o Governo lança um programa novo a implementar nas Autarquias, tem de apoiar economicamente as mesmas de modo a formar os utilizadores. Com utilizadores com formação a adopção de uma política de SSI será mais facilmente bem sucedida.

O entrevistado que mencionou este factor externo referiu que "temos aqui grandes lacunas de formação e talvez por isso seja tão importante que nós nos empenhemos em colmatar essas lacunas". [C1.3]

Contexto – Interno

Por "Contexto interno" entende-se os factores estruturais, sociais, culturais, etc., internos à Câmara, que influenciam a adopção ou aplicação de uma política de SSI.

Questionados sobre se existiram ou não ocorrências, como eventuais entraves, obstáculos ou problemas na adopção ou aplicação das políticas de SSI, obtiveram-se as indicações que se observam na Tabela 62.

Entraves, Obstáculos ou Problemas na Adopção	Número
Observaram-se ocorrências	7
Não se observaram ocorrências	4

Tabela 62: Entraves, Obstáculos ou Problemas na Adopção

Nos sete casos onde se observaram ocorrências no que concerne a entraves, obstáculos ou problemas na adopção da política, verifica-se que os mesmos são de dois tipos, conforme se apresenta na Tabela 63.

Tipo de Problemas na Adopção	Número
Resistência dos utilizadores	5
Desobediência dos utilizadores	2

Tabela 63: Tipo de Problemas na Adopção

Os entraves apontados anteriormente foram, segundo os inquiridos, superados rapidamente, pois os utilizadores compreenderam que a informação estava mais segura desta forma, e por outro lado desmistificou-se a ideia de eventualmente estarem a ser vigiados ou monitorizados.

Os factores apontados como críticos para se iniciar o processo de formulação e posterior implementação da política vão além da vontade e decisão política, tendo sido detectados um conjunto de factores que levaram à concretização efectiva de uma política de SSI. Esses aspectos foram divididos em verificação de falhas, uso indevido das TIC, falta de formação e informação dos utilizadores e falta de definição de regras. Seguidamente são apresentados alguns extractos ilustrativos dos diferentes aspectos.

Verificação de Falhas

> "Quando fazemos monitorização verificamos que há sempre grandes falhas. Felizmente o nosso antivírus consegue verificar tudo. Também temos *firewalls*, todo o sistema de segurança e de bloqueio de páginas implementado". [C1.3]

Uso Indevido das TIC

- **Uso indevido da Internet**
  "Foi adoptada para prevenir certos ataques e o uso indevido da internet …". [C1.30]
- **Uso indevido do Correio Electrónico**
  "Foi adoptada para prevenir certos ataques e o uso indevido …do e-mail". [C1.30]

Falta de Formação e Informação dos Utilizadores

- **Falta de formação**
  "Sentimos que existe também uma necessidade de formar, não só informar, provavelmente informadas estão, mas formadas não". [C1.3]
- **Não estar a ser cumprida a legislação**

"Fazemos chegar aos utilizadores legislação, para que tenham conhecimento do existente na área da segurança em termos legais. [C1.3]

Falta de Definição de Regras

- **Ser tudo permitido**
  "Tudo era permitido, porque nós começamos com dez computadores na Presidência e pouco mais". [C1.6]
- **Falta de regras devidamente definidas (ou seja escritas)**
  "Já existiam regras, já existiam procedimentos, tratou-se assim e apenas de uma formalidade, colocar no papel para haver precedentes de execução". [C1.20]
- **Falta de registo dos utilizadores**
  "Tivemos a necessidade de tentar limitar as pessoas e o acesso externo a determinados documentos confidenciais, alguns, outros não, mas o que acontecia era que a um utilizador bastava ter o computador ligado, e qualquer pessoa podia chegar ao computador e abrir os documentos, consultar e ter acesso a tudo aquilo que lá estava. Com os servidores, e estando tudo num servidor, é preciso um *login*, além do mais, ao fim de um "x" tempo, o computador bloqueia se estiver inactivo". [C1.29]
- ***Downloads* de software, filmes, música, etc.**
  "Tinhamos o caso dos eMules instalados, os utilizadores a fazerem *downloads* constantemente de filmes, músicas, etc. Também utilizavam os chats e outras situações com que tínhamos que acabar". [C1.6] e [C1.37]
- **Falta de segurança na rede**
  "A razão foi, por exemplo a utilização do emule, e outra razão foi a falta de segurança na rede". [C1.34]

Questionados sobre quem detectou realmente a falta de uma política de SSI, em nove (82%) casos foi o Departamento de Informática e em dois (18%) casos foi o Vereador responsável pela Informática.

Os factores fundamentais apontados pelos entrevistados para que uma política de SSI tenha sucesso, ou seja, para que os objectivos para o qual foi criada sejam atingidos, no âmbito de uma Câmara Municipal, são apresentados na Tabela 64.

Factores para o Sucesso da Política	Número
Formação dos utilizadores	4
Monitorização do cumprimento	3
Definição dos objectivos para a segurança	3
Empenho na Implementação	3
Ter aprovação do Executivo	2
Cumprimento pelos utilizadores	1
O documento não ser extenso	1
Definição de política	1

Tabela 64: Factores para o Sucesso da Política (*Cluster* 1)

A formação dos utilizadores

É dos aspectos mais mencionados, entende-se neste caso como a cultura e a forma de estar dos utilizadores perante a utilização das TIC no seu local de trabalho. Os utilizadores adquirindo formação, a sua cultura em relação à utilização das TIC

muda. “É tudo uma questão dos utilizadores estarem mentalizados para o que isto é e para o que têm que fazer”. [C1.30]

A monitorização do cumprimento

Alerta que não chega implementar uma política de SSI, o seu acompanhamento em permanência é fundamental para o sucesso da política. “O documento obriga-nos a nós internamente, define alguns aspectos que são necessários na implementação dos serviços, … aparece-nos um utilizador novo, nós temos que o caracterizar, temos que verificar quais são as medidas que vamos aplicar a essa pessoa…”. [C1.36]

A definição clara dos objectivos a atingir com a política de SSI

É fundamental para a sua formulação e, posteriormente, ir de encontro às verdadeiras necessidades de segurança do Município. “Primeiro, criar uma directriz. Depois de criar essa directriz, pô-la em prática, contornando, e além de contornar as dificuldades que vão surgindo no dia-a-dia, tentar tirar algumas ilações desses mesmos problemas que vão surgindo, para depois podermos melhorar a implementação desse mesmo sistema de segurança”. [C1.25]

O sucesso das políticas depende fortemente do empenho dos utilizadores e chefias

Na verdade, se as pessoas que estão a implementar a política se “empenharem e conseguirem chegar até às pessoas, explicar-lhes a importância de tudo o que estão a fazer sem impor, de forma que as pessoas consigam compreender o benefício que lhes vai trazer, é a melhor forma para se implementar uma política de SSI”. [C1.3] Segundo os inquiridos as restrições têm de ser percebidas pelos utilizadores e não impostas.

A aprovação pelo Executivo da política de SSI

Trata-se de outro factor crítico para o sucesso das políticas de SSI nas Câmaras Municipais. Segundo alguns inquiridos “uma coisa é a implementação e a aceitação pelos utilizadores se a ordem for do Executivo da Câmara outra completamente diferente é vinda dos colegas de informática”. [C1.20]

O cumprimento da política de SSI

É também um aspecto fundamental para que a mesma tenha sucesso, “porque não chega formular e implementá-la se depois a mesma não é cumprida pelos utilizadores. O cumprimento da política é o aspecto mais importante, depois basta os utilizadores terem a noção do que realmente podem ou não fazer”. [C1.6]

O documento deve ser de fácil leitura e compreensão, devendo também não ser muito extenso

Tem de ser um conteúdo rico e abrangente, mas resumido e legível para as pessoas o lerem e entenderem mais facilmente. Em relação à dimensão do documento, onde os inquiridos mencionam que não deve ser muito longo, está de acordo com as 25 políticas de SSI analisadas no capítulo anterior cuja média é de nove páginas, variando como número mínimo de uma página e número máximo de 26 páginas. Esta variação do número de páginas faz com que existam documentos demasiado simples e outros bastante pormenorizados. “…tem os pontos que para

nós são essenciais, tentamos explicar ao máximo, mas com o mínimo de texto possível… Optamos pelo essencial". [C1.6]

A definição de política

O que é para o município uma política de SSI é um aspecto importante para os passos subsequentes que são a formulação e implementação, porque conhecendo-se o que se pretende desde o início do processo, a homogeneização de todo o processo será mais fácil de alcançar. "Primeiro a definição de uma política. Todos os objectivos que são vistos. Acho que isso é mesmo o fundamental. Acho que cada caso é um caso, estudamos e vemos quais as nossas deficiências e depois elaboramos um documento". [C1.34]

7.3.2 Cluster 2

Nesta subsecção abordam-se aspectos contidos no guião que serviu de base para a realização das entrevistas às Câmaras Municipais que se enquadram no *Cluster* 2, tratando-se os seguintes tópicos: Benefícios das Políticas, Aprovação da Política, Processo – Formulação, Processo – Implementação, Contexto – Externo, Contexto – Interno, Conteúdo – Características e Conteúdo – Componentes.

Segue-se o primeiro tópico que diz respeito à dimensão "Benefícios", que aborda aspectos associados aos benefícios esperados com uma política.

Benefícios das Políticas

Uma vez que o Cluster 2 diz respeito a Câmaras que ainda não têm uma política de SSI, mas estão em processo de formulação ou adopção, os benefícios aqui abordados dizem sempre respeito ao que se espera com a política de SSI.

As respostas dos inquiridos sobre os benefícios esperados com a adopção da política de SSI puderam ser agrupadas conforme se observa na Tabela 65.

Benefícios Esperados de uma Política de SSI	Número
Maior segurança e atribuição de acesso às TIC	5
Diminuição da monitorização do departamento de informática	4
Utilizadores melhor informados	3
Normalização dos procedimentos	2
Maior produtividade	1

Tabela 65: Benefícios esperados com uma Política de SSI (*Cluster* 2)

A segurança da informação e a atribuição de acessos aos utilizadores que lhes permita aceder só a determinada informação é o benefício mais vezes citado.

"A política de segurança é útil na medida em que limita o acesso a esse tipo de situações (fuga de informação) …". [C2.28]

Diminuir a monitorização do departamento de informática devido à diminuição de erros cometidos pelos utilizadores é o segundo benefício mais citado.

> "Em temos do nosso trabalho, no dia a dia, penso que muitos dos problemas com que hoje somos confrontados, tenho quase a certeza que grande parte deles ficariam resolvidos". [C2.23]

O terceiro benefício é a informação dos utilizadores, ou seja, eles saberem o que podem e não podem fazer.

> "Para o departamento de informática é igualmente benéfico, deixando que as perdas de segurança sejam só da responsabilidade dos técnicos de informática e passarem a ser de qualquer funcionário porque está informado do que pode ou não fazer no seu computador e se não o fizer pode ser responsabilizado por isso". [C2.44]

A normalização dos procedimentos, ou seja, as restrições e as permissões estando escritas fazem com que todos tenham conhecimento dos mesmos.

> "… deve passar pela normalização e fazer sempre a mesma coisa, e sem excepções". [C2.16]

Por último, a maior produtividade é apontada por um dos inquiridos.

> "A protecção é verdade, não cabe tanto às pessoas, cabe mais a nós, direi que é uma situação que lhe será benéfica ao nível da produtividade". [C2.18]

Relativamente à questão se os restantes elementos da Câmara partilham que a política tem esses benefícios, em oito (73%) casos a resposta foi positiva, em dois (18%) casos esse assunto ainda não foi falado com ninguém e em um (9%) dos casos a resposta é não, sendo alegado que os outros elementos da Câmara vêem a parte da não divulgação de dados e partilham com o gabinete de informática, mas acham que o equilíbrio entre o risco de as pessoas terem acesso à informação versus a divulgação, a facilidade e as pessoas começarem a usar, é provável que ponderem num sentido um pouco diferente.

Aprovação da Política

Questionados se a política de SSI vai ser superiormente aprovada, a resposta foi unânime e todos responderam que sim. Em dois casos foi referido que se vai consultar o gabinete jurídico para saber se deve ser uma norma e assim ser aprovada em reunião de Câmara ou se deve ser um regulamento e assim ser aprovada em Assembleia Municipal.

A política de SSI, segundo os inquiridos, vai ser aprovada nos órgãos do Município conforme apontado na Tabela 66. Quando é referido que a aprovação vai depender da competência é porque ainda não sabem de que tipo de documento se vai tratar, logo não sabem quem o vai aprovar.

Quem Aprovará a Política	Número
Presidente da Câmara	4
De quem for a competência	3
Assembleia Municipal	2
Reunião de Câmara	2

Tabela 66: Quem Aprovará a Política (*Cluster* 2)

O porquê da política ser superiormente aprovada deve-se ao facto de ser mais vinculativa e ser melhor aceite pelos utilizadores, dar-lhe um carácter mais institucional e como se trata de uma ordem superior esta tem de ser aceite por todos, conforme se verifica nos extractos seguintes:

> "Acima de tudo por uma questão legal, nenhum documento pode ser circular ou ser aplicado se o Presidente não o aprovar. Por outro lado, ser aprovado em reunião de câmara para dar um carácter mais institucional ao documento". [C2.21]

> "Deve ser aprovada pelo Executivo para que essa política possa ser mais forte. Quando as coisas são feitas pelo início da pirâmide, regra geral, têm mais força". [C2.41]

Seguidamente trata-se outra perspectiva que diz respeito à dimensão "Processo", que aborda aspectos associados ao processo de formulação e implementação das políticas de SSI.

Processo – Formulação

Questionados sobre como está a ser formulada a política de SSI, as respostas dos inquiridos foram categorizadas conforme se indica na Tabela 67.

Formulação da Política	Número
Com base nas necessidades e crescimento tecnológico	5
Seguiram um modelo de outra Câmara	3
Escrevendo os procedimentos de segurança que utilizam no dia-a-dia	3
Com base em legislação existente	2
Em agrupamento com outras Câmaras	2
No âmbito de processo de certificação	1

Tabela 67: Formulação da Política (*Cluster* 2)

Como se observa na tabela, a formulação está a ser feita em quatro casos com base nas necessidades sentidas na Câmara no dia-a-dia e de acordo com o crescimento tecnológico sentido.

> "O documento está a ser formulado com base no crescimento tecnológico que a Câmara tem verificado nos últimos anos. É um parque informático cada vez mais alargado e então, temos que formular no papel, porque são muitos colaboradores, funcionários a entrar e a sair, e é necessário estabelecer alguma ordem em termos de segurança". [C2.11]

> "A sua formulação esta a ser feita conforme as nossas necessidades, e com o que aprendemos e vemos no dia-a-dia que tem de ficar definido". [C2.44]

Em três casos verifica-se que está a ser elaborada com base em documentos pedidos a outras Câmaras.

> "… estamos a recolher informação de outras Câmaras, de modo a seguir aquilo que de bom é feito". [C2.16]

Em três casos estão a escrever os procedimentos de segurança com base nos procedimentos já implementados na prática, mas não existentes em formato de papel.

"A maior parte destas políticas e destas directrizes já são conhecidas, ou seja, o que fizemos neste momento foi reunir realmente um conjunto de ideias, escrevê-las num documento ainda interno, só da unidade, e discuti-las entre as pessoas que melhor estão relacionas com essa área". [C2.18]

Em dois casos estão a verificar os requisitos legais na área da segurança que servirão de base para a escrita da política.

"Preocupei-me um bocado em ver o site da protecção de dados, vendo as restrições que eles impõem, …". [C2.21]

Em outros dois casos estão a ser escritas em agrupamento com outras Câmaras, tratando-se em um dos casos de um projecto de cidade digital.

"Neste momento estamos com o Projecto Cidades Digitais e estamos a tentar criar uma política comum, com todos os outros Municípios parceiros no Ave Digital". [C2.16]

Em um dos casos está a ser formulada por uma empresa externa no âmbito do processo de certificação dos serviços.

"…este documento surgiu da necessidade que nós tínhamos de documentar alguma informação. Aproveitamos também o facto da Câmara Municipal dar início a um processo de certificação". [C2.23]

Relativamente a quem está a elaborar a política de SSI, as respostas são observáveis na Tabela 68.

Autor da Política	Número
Gabinete de Informática	5
Gabinete de Informática e Gabinete Jurídico	3
Director de informática e Gabinete Jurídico	1
Projecto Cidades Digitais	1
Equipa da Certificação e Gabinete de Informática	1

Tabela 68: Autor da Política (*Cluster* 2)

Questionados sobre quem está a elaborar a política de SSI, o gabinete de informática está sempre presente, representado pelos seus directores ou técnicos, sendo que o apoio ao gabinete jurídico é mencionado em quatro casos. O que se verifica é que na sua maioria, a elaboração é interna à Câmara Municipal, não recorrendo os Municípios a empresas externas, com excepção de uma empresa de certificação, mas que trabalha em conjunto com o gabinete de informática.

Relativamente ao método que está a ser utilizado para a formulação da política, merecem destaque os seguintes aspectos:

- **Elaboração de uma política geral e depois compartimentar**
  "Nesta primeira análise não estou a seguir nenhum guião, estou a fazer … a política geral e depois compartimentar. Temos que ir ponto a ponto. … Portanto, estou a seguir baseando-me na nossa própria realidade". [C2.11]

- **Fazer recolha de modelos e adaptar à realidade da Câmara**

"Neste momento o que existe e, digamos que fizemos uma recolha, e tentamos adequar os elementos dessa recolha à especificidade básica, ou às especificidades que encontramos aqui na Câmara". [C2.18]

- **Observar as necessidades na prática e depois passar para o documento**
  "Observam-se no dia-a-dia as necessidades, na prática e depois passam-se para o documento...". [C2.21]

- **Consulta de informação no Instituto de Informática**
  "… consultei alguma informação, nomeadamente no Instituto de Informática e outra na internet". [C2.23]

- **Junção de sinergias e saberes das várias Câmaras**
  " … ver aquilo que já estava a ser bem feito, … aquilo que já nalgumas Câmaras está a ser implementado". [C2.23]

Processo – Implementação

No âmbito deste *cluster*, dado as Câmaras Municipais ainda não terem a política implementada, focar-se-ão aspectos de como está prevista ser implementada a política de SSI, conforme se observa na Tabela 69.

Implementação da Política	Número
As chefias fazem reuniões sectoriais	5
Disponibilização do documento na Intranet	4
Envio por Correio Electrónico	3
Acções de sensibilização dos utilizadores	2

Tabela 69: Implementação da Política (*Cluster* 2)

A política de SSI nestas Câmaras vai ser implementada em cinco casos com a distribuição através das chefias com as devidas instruções acerca da aplicação da política e estas por sua vez, fazem chegar a informação e a política a todos os utilizadores. Neste processo a distribuição da política normalmente é em papel. "Após aprovação o documento será entregue aos Directores de Departamento, que por sua vez fazem distribuição aos Chefes de Divisão, e estes vão fazer chegar a todos os funcionários". [C2.38]

Em quatro casos a implementação é feita através da disponibilização do documento na intranet para os utilizadores a poderem ver e estudar. "Numa primeira análise, como temos uma intranet a funcionar, a primeira informação há-de ser via intranet, onde iremos disponibilizar esse documento, para que cada funcionário no seu posto de trabalho possa ver, estudá-lo". [C2.11]

Em três desses casos é enviada também informação por correio electrónico. "Vai ser de duas formas, uma delas é de facto partir da intranet, estar lá e dar conhecimento através de e-mail, que toda a gente tem um endereço electrónico, dar-lhe conhecimento da entrada em vigor desse documento e que toda a gente deve respeitar". [C2.23]

Em dois casos há indicação que a implementação é feita através da comunicação do documento e sensibilização dos utilizadores para a vantagem da política, ou seja, fornecer aos utilizadores formação e educação adequadas acerca da utilização da política de segurança e procedimentos. "O que é importante para eles é que as medidas que são propostas e o que nós aconselhamos, lhes traga alguma vantagem. Se eu conseguir convencer que com aquelas medidas o trabalho deles será desempenhado de uma forma melhor, mais rápida, então eles de certeza que vão acompanhar-me". [C2.18]

Questionados sobre quem vai ser o responsável pela implementação da política de SSI, as respostas encontram-se sintetizadas na Tabela 70.

Responsável pela Implementação	Número
Gabinete de Informática	7
Gabinete de Informática e Chefes de Divisão	1
Gabinete de Informática e Vereador	1
Gabinete de Informática e Presidente da Câmara	1
Gabinete de Informática e Empresas Municipais	1

Tabela 70: Responsável pela Implementação (*Cluster* 2)

A responsabilidade da implementação é sempre do gabinete de informática, sozinho em sete casos, nos restantes é em conjunto com os Chefes de Divisão, Vereador, Presidente da Câmara e Empresas Municipais.

O local onde ficará depositada a política de SSI vai ser em seis casos na Intranet da Câmara Municipal, em três casos no Gabinete de Informática, nos restantes dois casos vai ficar em cada um deles na internet e no Gabinete de Informática e na Internet e na zona de relações públicas. A síntese dos locais onde deverá ficar a política encontra-se na Tabela 71.

Local de Depósito da Política	Número
Intranet	6
Gabinete de Informática	3
Intranet e Gabinete de Informática	1
Intranet e na zona de relações públicas	1

Tabela 71: Local de Depósito da Política (*Cluster* 2)

Segue-se outra perspectiva que diz respeito à dimensão "Contexto" que incide sobre os factores facilitadores e inibidores da adopção de políticas de SSI pelas Câmaras Municipais.

Contexto – Externo

Como factor fundamental externo para que uma política de SSI tenha sucesso no âmbito de uma Câmara não foi mencionado nenhum aspecto.

Como factor crítico para que tivesse sido possível iniciar-se o processo de formulação foi indicado em um caso que "a proliferação das TIC na sociedade actual, nomeadamente a Internet e o correio electrónico, levou a que fosse mais que pertinente a formulação de uma política para salvaguardar os SI da autarquia de uma

série de problemas de segurança que podem advir com a utilização das TIC no Município". [C2.40]

Contexto – Interno

Os factores estruturais, sociais e culturais que internamente condicionam o início do processo de adopção da política de SSI foram apontados pelos inquiridos como sendo os factores que se apresentam na Tabela 72.

Factores que Condicionam o Processo de Adopção	Número
Falta de tempo e de programação dessa acção	6
Expectativa de resistência da parte dos utilizadores	3
Falta de aprovação da política	2
Falta de percepção da necessidade por parte dos políticos	1
Falta de formação	1
Falta de funcionários de informática	1
O documento não estar de acordo com a lei	1

Tabela 72: Factores que Condicionam o Processo de Adopção (*Cluster* 2)

- **Falta de tempo e de programação dessa acção**
  A falta de tempo e de programação dessa acção foi apontada como o factor que mais condiciona o início do processo, ou seja, outras prioridades são definidas, ficando a adopção de uma política de SSI para segundo plano.

- **Factor Humano**
  O factor humano é também apontado "pelo facto de se saber existir resistência por parte dos utilizadores". [C2.21]

- **Aprovação da política**
  A aprovação da política em um caso foi inviabilizada na votação na Assembleia Municipal aquando da sua aprovação [C2.24] e em outro Município ainda está no Presidente da Câmara para ser aprovada [C2.40], é outro factor apontado como condicionador do processo de adopção de uma política.

- **Percepção da necessidade por parte dos políticos**
  Em um caso, a percepção da necessidade por parte dos políticos é apontada como condicionante, uma vez que "não é entendida como algo prioritário". [C2.28]

- **Falta de formação**
  A falta de formação dos utilizadores é também indicada. "Especialmente a falta de formação das pessoas na área da informática. Muitas vezes cometem erros sem saber, e no início pensavam que estavam a ser controlados, e não que estavam a ser protegidos". [C2.38]

- **Falta de funcionários de informática**
  A falta de funcionários afectos ao gabinete de informática inviabiliza que o trabalho seja todo feito. "… nesta Câmara Municipal só trabalham duas pessoas na informática. Temos diferentes edifícios e a responsabilidade das

escolas do 1º ciclo. Não nos podemos desdobrar e fazer tudo. E as solicitações são cada vez mais". [C2.44]

- **O documento não estar de acordo com a lei**
  Em outro caso a dificuldade consistiu em "articular a política para o correio electrónico com o articulado na lei vigente" para esse meio de comunicação. [C2.40]

Os factores que condicionam o processo de adopção de uma política de SSI anteriormente mencionados são todos factores condicionadores de natureza inibidora.

Questionados sobre quem detectou a falta de uma política de SSI, em nove (82%) casos foi o departamento de informática e nos restantes dois casos (18%), foi o director de departamento responsável pela informática.

Os factores fundamentais para que uma política de SSI tenha sucesso no âmbito de uma Câmara Municipal são apresentados na Tabela 73.

Factores para o Sucesso da Política	Número
Ter aprovação do Executivo	4
Existir vontade política	4
Os utilizadores terem formação	3
Os utilizadores entenderem as vantagens	3
Existir empenho na implementação	2
Monitorizar o cumprimento da política	1
Ter a componente tecnológica	1

Tabela 73: Factores para o Sucesso da Política (*Cluster* 2)

Conforme se observa na tabela anterior, o apoio político e a aprovação recolheram, no seu conjunto, oito citações.

"Que superiormente haja a sensibilidade e reconhecimento dos benefícios que podem advir da implementação de uma política de SSI, utilizando os meios com rigor e sem excepções". [C2.41]

Os utilizadores são mencionados logo a seguir com a indicação da importância da sua formação e o facto de eles entenderem as vantagens que vão advir da adopção de uma política.

" … perceberem que é importante este documento para eles e o cumprimento dessas regras". [C2.18]

O empenho e a monitorização do cumprimento por parte do gabinete de informática merecem o terceiro lugar nas citações.

" O pessoal na informática estar preparado e com vontade para que algo aconteça. Porque são sempre os principais visados e os principais interessados". [C2.21]

A componente tecnológica é também indicada como forma de apoiar a política de SSI.

"Em primeiro lugar, a estrutura tecnológica tem que estar preparada e salvaguardada das políticas que vamos aplicar. "O documento de que falamos é

importante, para primeiro verificarmos e fazer testes, e só depois disso é que a implementamos. Mas acho que a parte tecnológica é a mais importante para as políticas terem sucesso". [C2.38]

Relativamente a quem vai ter conhecimento da política de SSI, elenca-se na Tabela 74 as classes de destinatários.

Conhecimento da Política	Número
Todos os utilizadores	8
Todos os funcionários	1
Todos os utilizadores e chefias	1
Funcionários, Executivo e Gabinete de Apoio ao Executivo	1

Tabela 74: Conhecimento da Política (*Cluster* 2)

Em oito casos (73%) a política vai ser do conhecimento de todos os utilizadores, em um caso (9%) vai ser do conhecimento dos funcionários, em outro caso (9%) do conhecimento dos utilizadores e chefias e no caso restante (9%) vai ser do conhecimento de todos os funcionários, do Executivo e do gabinete de apoio ao Executivo da Câmara.

É de referir que em alguns casos os utilizadores podem coincidir com os funcionários, mas nem sempre isso se verifica. Os utilizadores são aqueles que vão utilizar o sistema de informação do Município, esses utilizadores são por norma funcionários, mas podem também ser pessoas externas, outra situação é que muitas vezes nem todos os funcionários são utilizadores.

Seguidamente são abordados aspectos relacionados com a perspectiva "Conteúdo", ou seja, as características e as componentes das políticas de SSI a adoptar por estas Câmaras Municipais.

Conteúdo – Características

Relativamente ao conteúdo de uma política de SSI no que diz respeito às suas características, mais concretamente a existência de uma única política global ou várias parciais, as respostas foram em 10 casos (91%) que vai haver um único documento que "irá englobar alíneas diferentes, compartimentado por capítulos" [C2.11]. Esta opção deve-se ao facto de acreditarem que é melhor quando se pretende transmitir uma mensagem a um utilizador ou a um colaborador um só documento com aquilo que pretendem e o que estão a implementar, do que terem de ler vários documentos. Entende-se que desta forma a informação está mais centralizada, o que poderá garantir que a divulgação seja mais eficaz. "Se forem muitos documentos a informação poder-se-á dispersar e não chegar como pretendido aos utilizadores" [C2.24].

Em um caso (9%) vão existir duas políticas parciais: "uma política para o "correio electrónico" e outra para a "protecção de dados, acesso à Internet, *passwords* e nomes de utilizadores". A justificação para a existência de duas políticas parciais, prende-se com o propósito de serem mais abrangentes e complexas. [C2.38].

Conteúdo – Componentes

Relativamente ao conteúdo de uma política de SSI, no que diz respeito às suas componentes, questionados sobre se devem estar definidos os papéis e as responsabilidades a resposta foi unânime e nos onze casos (100%) a resposta foi positiva. Os utilizadores têm de ter conhecimento daquilo que o gabinete de informática está forçosamente a implementar e têm de ter a noção de responsabilidade. A responsabilidade e papéis estão também definidos para o gabinete de informática de acordo com a sua hierarquia no gabinete.

Relativamente à definição de sanções para o não cumprimento da política de SSI, verifica-se na Tabela 75 que em seis casos estão previstas sanções, em três casos a sanção é a prevista na lei da função pública, designadamente a aplicação de um processo disciplinar. Em outros três casos essas sanções estão definidas no próprio documento e podem ser penas como o corte do acesso à Internet e o corte de alguns privilégios. Em três casos o documento não refere em parte alguma este aspecto das sanções. Nos restantes dois casos ainda não definiram se vão ou não incluir este ponto.

Definição de Sanções	Número
Sim	6
Não	3
Não está ainda definido	2

Tabela 75: Definição de Sanções (*Cluster* 2)

7.3.3 Cluster 3

Esta subsecção debruça-se sobre aspectos contidos no guião que serviu de base para a realização das entrevistas às Câmaras Municipais que se enquadram neste *Cluster*, para tal abordando os seguintes tópicos: Benefícios das Políticas, Contexto – Externo e Contexto – Interno.

Segue-se a primeira perspectiva que diz respeito à dimensão "Benefícios", focando-se aspectos associados aos benefícios esperados com uma política.

Benefícios das Políticas

Uma vez que o Cluster 3 diz respeito a Câmaras que não têm uma política de SSI, mas que têm intenção de adoptar uma política de SSI, os benefícios aqui abordados dizem sempre respeito ao que se espera com a política de SSI.

Questionados sobre se uma política de SSI trará benefícios no âmbito de uma Câmara Municipal, as respostas foram positivas em todos os casos (100%), mencionando os benefícios esperados. A utilidade esperada com a adopção de uma política de SSI pode ser observada na Tabela 76.

Benefícios Esperados de uma Política de SSI	Número
Utilizadores melhor informados	7
Maior controlo do acesso às TIC	5
Maior normalização dos procedimentos	3
Redução de ocorrência de incidentes	2

Tabela 76: Benefícios Esperados de uma Política de SSI (*Cluster* 3)

Informar os utilizadores foi mencionado sete vezes, sendo referido que o benefício será em primeiro lugar as pessoas saberem exactamente quais são as regras pelas quais se rege a utilização dos sistemas.

> "Uma política de segurança bem definida é sempre útil. É a mesma coisa que existir uma planta de emergência em qualquer edifício. Nunca ninguém vê que ela lá está, mas quando é preciso ela está lá. Penso que será essencial para as pessoas, as secções, os departamentos terem conhecimentos dos direitos e deveres e quanto às restrições explicar porque é que são assim". [C3.10]

A segurança e acesso às TIC refere-se ao sentido de proteger e salvaguardar os dados que os Municípios armazenam, bem como restringir os acessos dos utilizadores às TIC.

> "Poderá também ter uma definição mais clara da atribuição de login`s e de privilégios de utilização na rede, que muitas vezes é feita um bocadinho *ad-hoc*". [C3.9]

A normalização de procedimentos foi referida em três casos, tendo sido focadas as vantagens da definição formal dos processos e procedimentos relacionados com as TIC.

> "Um documento destes poderá fazer a definição destes processos". [C3.35]

A redução de ocorrências de incidentes é também referida como um benefício esperado com a adopção de uma política de SSI.

> "Reduzir a probabilidade de ocorrência de incidentes". [C3.5]

Segue-se outra dimensão "Contexto" que reflecte sobre os factores facilitadores e inibidores da adopção de políticas de SSI pelas Câmaras Municipais.

<u>Contexto – Externo</u>

As Câmaras incluídas neste *cluster* não têm uma política de segurança, mas têm intenção de adoptar uma, e isso deveu-se à influência externa em dois casos. No primeiro caso essa intenção surgiu inerente ao processo de certificação de qualidade que a Autarquia está a levar a cabo. No segundo caso a intenção surgiu aquando no âmbito deste trabalho foram contactados para responderam a um inquérito sobre a temática das políticas de SSI.

Foi referido em um caso que embora exista a intenção há bastante tempo ainda não foi iniciado o processo de formulação pelo facto de existir uma constante necessidade de se adaptarem às novas tecnologias, às novas ameaças e às novas formas de as combater, que lhes consome algum do tempo que seria necessário para elaborar um documento escrito.

Em outro caso justificam que ainda não iniciaram o processo de formulação porque aguardam que se inicie o processo de certificação de qualidade no Município.

Contexto – Interno

Os factores estruturais, sociais e culturais que influenciam a adopção ou aplicação de uma política de SSI no contexto interno, são relativamente à questão "Que factores são fundamentais para que uma política tenha sucesso no âmbito de uma Câmara Municipal?" e as respostas são as observadas na Tabela 77.

Factores para o Sucesso da Política	Número
Ter aprovação do Executivo	5
Formação dos utilizadores	4
Vontade política	3
Os utilizadores entenderem as vantagens	3
Formação dos técnicos	2
O documento não ser extenso	2
Actualização da política	1

Tabela 77: Factores para o Sucesso da Política (*Cluster* 3)

Conforme se observa na tabela anterior, a aprovação pelo Executivo da Câmara Municipal da política de SSI é o factor mais vezes apontado como fundamental para o sucesso de uma política, segue-se a formação dos utilizadores, e a vontade política aqui não em termos de aprovação, mas de incentivo para a sua formulação, em igual número surge a necessidade de os utilizadores entenderam os benefícios inerentes à política. A formação dos técnicos no âmbito da segurança dos SI é também fundamental para o sucesso da implementação da política. O documento não ser demasiado extenso, assim como a política estar actualizada são factores também mencionados.

Os factores explicativos do porquê de ainda não disporem uma política de SSI estão expostos na Tabela 78.

Factores para a Não Existência de uma Política	Número
Falta de tempo e de recursos humanos	6
Nunca existiu essa necessidade	2
Complexidade na criação e implementação	1
Início do processo de certificação pendente	1
Falta aprovar documento prévio	1
Falta de vontade política	1
Regulamentos deixados para segundo plano	1

Tabela 78: Factores para a Não Existência de uma Política (*Cluster* 3)

Com a indicação em seis casos é apontado como o principal factor explicativo do porquê de não terem ainda uma política de SSI a falta de tempo e de recursos humanos.

> "… a constante necessidade de nos adaptarmos a novas tecnologias, a novas ameaças e a novas formas de as combater, que nos consome algum do tempo que seria necessário para elaborar um documento escrito, com regras aprovadas pelo

executivo, e que realmente me parece trará algum benefício acrescido à própria componente tecnológica da segurança". [C3.4]

Segue-se a indicação em dois casos de nunca se ter sentido essa necessidade pelo facto de ser uma autarquia pequena e em outro caso por se desconhecer a existência deste tipo de documentos.

"Nós não temos porque não tínhamos ninguém especializado em informática, e nunca houve essa necessidade, nem sequer a noção dessa necessidade". [C3.10]

Segue-se com uma indicação a complexidade na sua criação e implementação.

"… a formulação de uma política envolve diversas etapas, vários intervenientes e exige resposta a muitas questões. A implementação também não é fácil pois nem todos têm consciência da sua importância sendo que nem sempre é bem aceite ter de seguir regras. Por outro lado, o desconhecimento da sua importância relega-a para um plano secundário. A pressão é para que sejam resolvidos os problemas do dia-a-dia e para a execução de projectos com resultados visíveis". [C3.5]

Em igual número com uma indicação está a espera enquanto não tem início o processo de certificação de qualidade.

"O projecto-piloto para a certificação da qualidade passava pelas áreas do Expediente e Licenciamento Urbanístico, aguardamos também posteriormente a certificação da qualidade da Divisão de Informática, porque a informática é transversal a todas as áreas". [C3.8]

A falta de aprovação pela Assembleia Municipal das normas que vão ser a base para a escrita da política.

"Esse documento ainda não foi aprovado pela Assembleia Municipal, e portanto, como ainda não está aprovado não deu até ao momento origem ao documento da política de SSI". [C3.13]

A falta de vontade política que impede que se inicie esse trabalho em detrimento de outros.

"… muitas vezes os políticos, ainda não estão convencidos, de que sem se adoptar uma política por escrito, não são cumpridas certas normas que são necessárias". [C3.17]

Em outro caso os regulamentos são considerados instrumentos para segundo plano em detrimento das tecnologias.

"Em primeiro lugar, a minha ideia de política de segurança, e eu tenho uma formação bastante técnica, tenho alguma tendência em deixar as questões relativas a Regulamentos e posturas um bocado para segundo plano, ou seja, do ponto de vista tecnológico não fazia sentido que a Câmara Municipal não tivesse os seus sistemas de informação com segurança, mas realmente em termos de regulamentação, de regras, não estamos ainda nesse patamar". [C3.4]

Os factores explicativos do porquê de ainda não se ter iniciado o processo de formulação encontram-se na Tabela 79.

Factores para Não se Ter Iniciado o Processo de Formulação	Número
Falta de tempo e de recursos humanos	7
Existência de tecnologia	2
Aguardar processo de certificação	1
Aguardar ordem do executivo	1
Complexidade na elaboração	1

Tabela 79: Factores para Não se ter Iniciado a Formulação (*Cluster* 3)

A falta de tempo, de recursos humanos, a existência de outras prioridades e a complexidade da tarefa foram adiando o processo. Por outro lado, a tranquilidade oferecida pelos diversos mecanismos de segurança implementados, também ajuda a protelar. A falta de vontade política é também aqui mencionada como uma condicionante, bem como a espera pelo processo de certificação de qualidade.

- **Falta de tempo e de recursos humanos**
  "Não foi iniciado por manifesta falta de tempo e de oportunidade. Falta capital humano". [C3.9]
  "Porque um dos grandes motivos é que eu sou o único informático, tenho de fazer de tudo". [C3.10]

- **Existência de tecnologia**
  "Por outro lado a tranquilidade oferecida pelos diversos mecanismos de segurança implementados, também ajuda a protelar". [C3.5]

- **Aguardar processo de certificação**
  "Ainda não foi iniciado esse processo porque estamos a aguardar, em velocidade cruzeiro, o processo de certificação, e a partir daí avançaremos". [C3.8]

- **Aguardar ordem do executivo**
  "Estamos à espera de luz verde do Executivo". [C3.17]

- **Complexidade na elaboração**
  "A existência de outras prioridades e a complexidade da tarefa foram adiando o processo". [C3.5]

Quem detectou a falta de uma política e posterior intenção de formular tal documento foi em seis casos o gabinete de informática, em quatro casos o director de informática e em um caso a resposta não teve a indicação de uma pessoa em particular, mas sim da necessidade que se foi sentindo para a resolução de alguns problemas.

O facto de quererem adoptar uma política, razão pela qual se enquadram no Cluster 3, deve-se a motivos diferenciados, entre eles destacam-se os seguintes:

- A necessidade de adoptar uma política foi aumentando com o crescimento do parque informático;
- A disseminação da informática neste momento é muito grande e as Câmaras estão muito mais sujeitas a ataques;

- A informação é considerada o principal activo de uma organização e simultaneamente está sob constante risco;
- Grande parte dos incidentes de segurança serem causados por falhas humanas e técnicas e que esses incidentes poderiam ser evitados se fossem seguidas regras e normas de conduta;
- Para o gabinete se salvaguardar de possíveis perdas de dados;
- Para salvaguardar as pessoas e os próprios funcionários em termos da segurança dos dados, em relação ao exterior e do exterior em relação à Câmara;
- Para se poderem responsabilizar os funcionários, de certos abusos que possam praticar.

7.3.4 Cluster 4

Esta subsecção versa sobre aspectos contidos no guião que serviu de base para a realização das entrevistas às Câmaras Municipais que se enquadram neste *Cluster*, e aborda os seguintes tópicos: Benefícios das Políticas, Contexto Externo e Contexto Interno.

Segue-se a primeira perspectiva que diz respeito à dimensão "Benefícios", que aborda aspectos associados aos benefícios esperados com uma política.

Benefícios das Políticas

Uma vez que o Cluster 4 diz respeito a Câmaras que não têm uma política de SSI e não têm intenção de adoptar uma política de SSI, os benefícios aqui abordados dizem sempre respeito ao que se espera com a política de SSI e as razões apontadas para não considerarem uma política útil.

Relativamente aos benefícios que se podem esperar com a implementação de uma política de SSI, os inquiridos responderam de acordo com os resultados elencados na Tabela 80.

Benefícios Esperados com uma Política de SSI	Número
Maior responsabilização dos utilizadores	2
Maior segurança e melhor acesso às TIC	1
Utilizadores melhor informados	1
Melhor complementação da parte tecnológica	1

Tabela 80: Benefícios Esperados com uma Política de SSI (*Cluster* 4)

A responsabilização dos utilizadores é um dos benefícios referidos. Maior segurança e melhor acesso às TIC também são indicados. O facto de os utilizadores estarem melhor informados com a existência de uma política e um melhor complemento da parte tecnológica são também apontados.

- **Maior responsabilização dos utilizadores**
  "Maior responsabilidade de cada utilizador". [C4.7]

- **Maior segurança e atribuição de acesso às TIC**
  "Digamos que com uma política de SSI implementada será mais fácil prevenir e controlar possíveis intrusões e erros que possam surgir na rede e base de dados da Câmara". [C4.39]

- **Utilizadores melhor informados**
  "Porque traz vantagens. Este é um exemplo que eu vou dar, chega uma pessoa nova, está escrito, é muito mais fácil adoptar as políticas e é muito mais fácil as pessoas que entram de novo saberem o que e que podem ou não fazer". [C4.26]

- **Melhor complementação da parte tecnológica**
  "Como documento é importante complementando a parte tecnológica". [C4.19]

Os outros seis entrevistados neste cluster consideram que uma política poderá ser útil, mas que as tecnologias utilizadas conseguem manter os SI livres de perigos, conseguindo assim garantir a SSI, não tendo estes seis casos sentindo ainda necessidade de formular uma política de SSI.

> " Temos vários mecanismos de defesa como anti-vírus, firewall, mecanismos activos de defesa da rede e até agora não tivemos essa necessidade. Existe uma série de procedimentos que no dia-a-dia são transmitidos aos utilizadores, mas sem estarem escritos". [C4.14]

Segue-se a perspectiva "Contexto" que incide sobre os factores facilitadores e inibidores da adopção de políticas de SSI pelas Câmaras Municipais.

<u>Contexto – Externo</u>

Os factores económicos, políticos, legais, etc., que influenciam a adopção de políticas de SSI no contexto externo só foram mencionados num dos casos como resultado do contacto efectuado aquando da realização do inquérito no âmbito deste trabalho de investigação a essa Autarquia. Inicialmente não tinham intenção de adoptar nenhuma política de SSI devido ao total desconhecimento da existência destes documentos. Este factor externo fez com que o inquirido se questionasse sobre a utilidade deste documento e ponderasse alterar a sua posição e considerasse formular uma política de SSI.

Um exemplo do desconhecimento da existência de políticas de SSI é referido no extracto seguinte.

> "… achei brilhante, nunca nos tinha ocorrido passar isto a escrito…". [C4.12]

<u>Contexto – Interno</u>

Questionados sobre que factores são fundamentais para que uma política tenha sucesso no âmbito de uma Câmara Municipal, os entrevistados responderam conforme se observa na Tabela 81.

Factores para o Sucesso da Política	Número
Maior investimento na aquisição de TIC	5
Monitorizar mais o cumprimento	3
Ser do conhecimento de todos os utilizadores	2
Ter aprovação do Executivo	1
Os utilizadores terem mais formação	1
Existir vontade política	1

Tabela 81: Factores para o Sucesso da Política (*Cluster* 4)

O investimento em TIC, como por exemplo, servidores, sistemas de *backup* e anti-vírus é apontado como o factor primordial para o sucesso de uma política em cinco casos.

> "O factor da actualização das novas tecnologias e o controlo que fazem, permitem proteger a informação". [C4.43]
>
> "Tem que haver uma actualização permanente do equipamento informático, que é muito importante, o equipamento físico também tem que ser actualizado, servidores, que guardam a informação, e outros componentes ligados ao servidor." [C4.7]

Monitorizar o cumprimento por parte do gabinete de informática é citado em três casos.

> "É necessário que as políticas sejam cumpridas". [C4.26]

Ser do conhecimento de todos os utilizadores mereceu menção em dois casos.

> "… sejam dados a conhecer aos utilizadores porque assim responsabiliza-os". [C4.14]

Ter aprovação do Executivo.

> "… os procedimentos estarem escritos e aprovados…". [C4.14]

Os utilizadores terem formação.

> "… alguma formação para todos os utilizadores". [C4.7]

Existir vontade política para aceitar a formulação e implementação de uma política é também um factor fundamental para o sucesso de uma política.

> "É importante a nossa força de vontade, neste caso do Gabinete de Informática, de conseguir que os políticos nos ouçam e ajudem à prossecução de políticas tão importantes como é o caso da política de SSI". [C4.1]

Questionados sobre as razões para a não adopção de uma política de SSI, as respostas podem ser observadas na Tabela 82.

Razões para Não Adoptar uma Política	Número
Satisfação com a protecção providenciada pelas TIC	6
Falta de autorização superior	1
Complexidade da formulação	1
Falta de tecnologia de suporte	1

Tabela 82: Razões para Não Adoptar uma Política (*Cluster* 4)

Em seis casos foi mencionado que a razão para não adoptarem uma política de SSI é terem TIC suficientes para manterem o sistema de informação seguro (é de referir que na sua maioria são Câmaras de média dimensão), apontando vários mecanismos de defesa como anti-vírus, *firewall*, mecanismos activos de defesa da rede informática até ao momento considerados suficientes. Mencionaram também que existe uma série de procedimentos (como e onde gravar ficheiros, fazer sempre *logout* ao sair do computador e procedimentos específicos para o envio de correio electrónico) que no dia-a-dia são transmitidos aos utilizadores, mas sem estarem escritos.

> "Temos vários mecanismos de defesa como anti-vírus, firewall, mecanismos activos de defesa da rede e até agora não tivemos essa necessidade. Existe uma série de procedimentos que no dia-a-dia são transmitidos aos utilizadores, mas sem estarem escritos". [C4.14]

Em um dos casos a razão mencionada é a falta de ordem superior para elaborarem a política.

> "… as decisões são emanadas pelos políticos, e como os políticos estão "de fora" não sentem essa necessidade. Dada a situação, o nosso Gabinete foi tomando medidas de forma a defender-se do exterior e até do interior. Neste momento, aguardamos decisão superior para elaborar e adoptar essa política SSI". [C4.1]

A complexidade da formulação é também referida.

> " … tentar ver quais são os procedimentos que temos que tomar aqui internamente, para conseguirmos obter esse documento". [C4.22]

Outra razão é a falta de tecnologias: não tendo *firewall*, nem servidor de *backups* e também não tendo a rede num servidor de domínio, não fará muito sentido criar regras sobre uma estrutura tão pouco apetrechada tecnologicamente.

> "Porque neste momento não temos ainda os meios tecnológicos suficientes para adoptar essa política. Mas no futuro, penso que será uma boa solução". [C4.26]

7.4 Análise Inter-Clusters

As entrevistas foram efectuadas com o apoio de quatro guiões antecipadamente elaborados (disponíveis no Capítulo 5), ou seja, tantos quantos os *clusters*. Por sua vez, cada um dos guiões é organizado tendo em conta a aplicabilidade a esse *cluster* de cada uma das perspectivas (conteúdo, processo e contexto).

O *Cluster* 1, que corresponde a Câmaras que têm uma política de SSI, está associado à primeira dimensão "processo", ou seja aos processos de formulação, implementação e revisão das políticas. Está também relacionado com a terceira dimensão "contexto", onde se pretende saber quais são os factores facilitadores e inibidores da adopção de políticas de SSI pelas Câmaras.

O *Cluster* 2, que corresponde a Câmaras que não têm implementada uma política de SSI, mas estão em processo de formulação ou adopção, está associado às três dimensões como o *Cluster 1*, com excepção da dimensão "processo" que só está parcialmente associada a este *cluster*, porque as políticas estão em processo de

formulação e questões como, por exemplo, a revisão da política ainda não podem obter resposta.

O *Cluster* 3 e o *Cluster* 4, que correspondem a Câmaras que não têm uma política de SSI, mas têm intenção de adoptar uma política de SSI e Câmaras que não têm uma política de SSI e não têm intenção de adoptar uma política de SSI, estão associadas à dimensão "contexto", onde se pretende saber quais são os factores facilitadores e inibidores da adopção de políticas de SSI pelas Câmaras.

Após a análise das entrevistas individualmente e intra-clusters, nesta secção será feita a análise da justaposição do *Cluster 1*, *Cluster 2*, *Cluster 3* e *Cluster 4*. Dada a contextualização e abrangência de cada Cluster ser ímpar, as questões conjuntas entre eles é diminuta. Em todos é abordada a questão dos benefícios que se podem esperar com a adopção da política e os factores fundamentais para que uma política tenha sucesso no âmbito de uma Câmara Municipal.

Relativamente aos benefícios esperados há aspectos comuns nas respostas dos quatro *clusters*, nomeadamente a "Segurança e acesso às TIC", "Diminuir a monitorização do departamento de informática" e "Informar os utilizadores" que estão presentes e listadas pela mesma ordem nos *Clusters* 1 e 2.

No *Cluster* 3 é também referida a "Normalização de procedimentos", o que se entende uma vez que a política ainda está a ser formulada, e que é com a sua adopção que todos os utilizadores devem ter os mesmos procedimentos, uma vez que todos recebem a política de SSI de igual forma.

No *Cluster* 3 o benefício apontado com maior destaque é o de "Informar os utilizadores", seguindo-se a "Segurança e acesso às TIC", a "Normalização de procedimentos" e a "Redução de incidentes" é também mencionado.

No *Cluster* 4 a "Responsabilidade dos utilizadores" merece o destaque.

O aspecto que diferencia mais estes quatro aglutinados de informação, é que os primeiros dois *clusters* identificam benefícios mais abrangentes e que dizem respeito à segurança da informação e ao gabinete de informática e só depois o foco vai para os utilizadores, no *Cluster* 3, e muito em particular no *Cluster* 4, as respostas são mais específicas e mais direccionadas, com foco principal nos utilizadores, normalização de procedimentos, redução de incidentes e complementação da parte tecnológica.

Em suma, à medida que descemos nos *clusters* o foco está mais no sentido das tecnologias e dos equipamentos informáticos que para os entrevistados é o suficiente para garantir a segurança sendo que aspectos como a segurança da informação não é mencionada no *Cluster* 4.

Os factores condicionantes para que uma política tenha sucesso no âmbito de uma Câmara Municipal podem ser observados no ponto anterior, contudo nota-se que conforme se desce nos *clusters*, o foco direcciona-se para a parte tecnológica, para a formação dos técnicos e para os utilizadores entenderem as vantagens inerentes à política de SSI. No *Cluster* 4, o factor mais focado foi a "Aquisição de tecnologia",

o que vem dar sustentação ao anteriormente escrito que à medida que se desce no *cluster* o foco nas tecnologias aumenta; nos *Clusters* 1, 2 e 3 a parte tecnológica nem é referida como factor para o sucesso de uma política. Por sua vez, no *Cluster 4* é referido com uma percentagem significativa, que as razões para não adoptarem uma política é estarem "Satisfeitos com as TIC".

Nesta análise inter-cluster, merece destaque o que faz certas Câmaras disporem de políticas, pelo entendido, poder-se-á dizer que é para garantir a segurança e acesso às TIC e para diminuir a monitorização do departamento de informática, e consequentemente libertar este gabinete para outras tarefas, uma vez que é referenciado várias vezes a falta de recursos humanos nesta área.

Outro aspecto pertinente é o que sugere que a maioria das Câmaras Municipais não disponha de uma política de SSI. O principal factor apontado é a falta de tempo e de programar esta acção, como já foi vincada as solicitações por diversos motivos ao gabinete de informática são constantes e por vezes este aspecto fica para segundo plano, uma vez que os recursos humanos são poucos. Em alguns casos, embora considerem que uma política de SSI pode trazer benefícios para a Câmara Municipal, ainda não foi notada uma necessidade basilar para se iniciar o processo de criação. Outro aspecto é a satisfação com as TIC, sentindo que é suficiente para a garantir a SSI. Estes factos indiciam que embora tenham conhecimento dos benefícios com a adopção de uma política de SSI, ainda não elegeram a adopção de uma política de SSI como primordial para garantir a segurança dos SSI da Autarquia.

Os aspectos que podem contribuir para que uma Câmara Municipal passe a ter uma política de SSI incluirão o aumento dos recursos humanos afectos à informática, os processos de certificação que estão a decorrer em vários Municípios e a existência de um modelo de política de SSI que possa ser adaptada a cada realidade Municipal.

Segundo a análise realizada podem ser apontados como factores que podem dificultar o processo de adopção de uma política de SSI numa Câmara Municipal os seguintes: falta de vontade política, complexidade na elaboração, falta de aprovação superior e falta de formação dos utilizadores que muitas vezes faz com que tenham atitudes desfavoráveis à mudança.

7.5 Conclusão

A contribuição fundamental deste capítulo foi a análise das 44 entrevistas que teve por base os quatro *Clusters* definidos, bem como a sua aplicabilidade conforme a perspectiva definida: Conteúdo das políticas, Processo associado às políticas de SSI e Contexto relativo às políticas de SSI.

Numa primeira fase foi feita a análise individual de cada uma das entrevistas, através da sua transcrição, leitura e codificação.

Numa segunda fase procedeu-se à análise intra-*cluster*, abordando-se tópicos como por exemplo, os benefícios das políticas, o processo (formulação, implementação e revisão), o contexto (interno e externo) e o conteúdo (características e componentes).

Na última fase foi feita a análise inter-*clusters* onde se teceram considerações relativas ao cruzamento dos dados entre o Cluster 1, Cluster 2, Cluster 3 e Cluster 4, nomeadamente nos pontos comum.

Findo este capítulo crêem-se reunidas as condições para se proceder à discussão dos resultados obtidos até ao momento, e que estão presentes neste trabalho na análise do inquérito, dos documentos e das entrevistas. A realização deste processo é o propósito do capítulo seguinte.

Capítulo 8

Discussão dos Resultados

8.1 Introdução

No primeiro capítulo deste trabalho de investigação efectuou-se uma sumária introdução, onde se explanaram as motivações, enquadramento e objectivos do presente trabalho, tendo-se seguido no segundo capítulo a revisão da literatura no âmbito das políticas de SSI. No terceiro capítulo foram caracterizadas as Câmaras Municipais seguindo-se o quarto capítulo onde foram apresentados os resultados do levantamento realizado sobre políticas de SSI nas Câmaras Municipais Portuguesas, ao que sucedeu um capítulo onde se descreveu o trabalho realizado, elaborando-se sobre o método e técnicas de investigação a utilizar neste estudo, discutindo-se as razões que levaram à sua selecção, as suas principais características e aspectos relacionados com o rigor, a validade e a generalização das conclusões que permitem obter. No capítulo seis foi apresentado o estudo dos dados resultantes da análise documental das políticas de SSI disponibilizadas pelos Municípios, seguindo-se o capítulo sete onde foi exposta a análise das entrevistas efectuadas nas Câmaras Municipais. No presente capítulo é apresentada a discussão dos resultados deste trabalho de investigação.

No plano deste projecto de doutoramento, a tarefa que requeria um esforço mais intensivo e demorado dizia respeito à realização dos inquéritos via telefónica à totalidade dos Municípios Portugueses, a recolha do maior número de políticas de SSI e por fim a realização das 44 entrevistas efectuadas em todos os Distritos de Portugal Continental e na Região Autónoma dos Açores.

Na posse dos dados recolhidos procedeu-se à sua análise. Tratando-se o inquérito de dados de carácter mais quantitativo a análise foi feita através de uma folha simples do Excel. Quanto à análise dos documentos das políticas e das entrevistas que são dados puramente qualitativos, a análise foi feita com a ajuda de um software apropriado para esse tipo de análise, o Atlas.ti.

Este trabalho de análise foi descrito nos capítulos 4, 6 e 7, pelo que neste capítulo é feita a interpretação dos resultados provenientes das análises efectuadas, dando-se resposta às questões de investigação propostas neste trabalho de investigação.

Com este trabalho procurou-se contribuir para o conhecimento da realidade em Portugal no que diz respeito à adopção de políticas de SSI e para o enriquecimento da literatura de SI, deficitária em estudos empíricos sobre a temática versada.

Os resultados do levantamento efectuado deram origem a diversas interrogações, as quais se fundaram na reduzida adopção de políticas de SSI por parte dos Municípios em Portugal. Na investigação subsequente, ou seja, na realização das entrevistas, e

indo beber directamente aos resultados do inquérito efectuado, julgou-se útil organizar o fenómeno em análise em quatro *clusters,* mencionados na subsecção 5.6.2 deste trabalho.

Antes de se iniciar o novo trabalho de campo, foi necessário planear devidamente a abordagem de recolha de dados a utilizar, bem como definir os tipos de dados que se pretendiam gerar e quais os procedimentos a utilizar.

Uma vez que o método de investigação empregue neste estudo é qualitativo e que a perspectiva filosófica implícita é a interpretivista, foi necessário definir a técnica de análise de dados que melhor se enquadre neste trabalho tendo em conta o seu âmbito e objectivos.

Lacity e Janson [2001] consideram que um investigador de matriz interpretivista não pode analisar objectivamente um texto, uma vez que as abordagens interpretivistas relacionam-se com as circunstâncias contextuais que influenciam os investigadores, assim como com as circunstâncias contextuais que influenciam as próprias interpretações dos investigadores.

A técnica de análise de texto interpretivista considera que a análise dos dados de texto é subjectiva, uma vez que tem de se ter sempre em consideração a época, cultura e experiências pessoais tanto do investigador como do entrevistado/orador [Lee 1991]. Este facto condiciona as interpretações literais do texto, sendo necessário interpretar os dados tendo em conta estas condicionantes.

Procurando atenuar os potenciais reflexos daquelas condicionantes na análise de conteúdo realizada, designadamente nos domínios da validade e fiabilidade dos resultados alcançados, procedeu-se à codificação dos documentos com intervenção de dois investigadores (a autora do presente trabalho e um outro investigador externo) aplicando-se os códigos utilizados nas referidas operações e enunciados no *Codebook* (elaborado por um terceiro elemento), já anteriormente mencionado.

De forma a se atingirem os objectivos acima estabelecidos, este capítulo encontra-se organizado em cinco secções.

Após a introdução do capítulo, na secção 8.2 procede-se à apresentação da interpretação dos resultados da análise das políticas e das entrevistas. Na secção 8.3 é feita uma análise crítica face à literatura sobre políticas de SSI. No seguimento desta discussão dos resultados, na secção 8.4 é apresentado um conjunto de recomendações que possam contribuir para a adopção de políticas de SSI na Administração Local Portuguesa, terminando com a secção 8.5 onde se expõem as conclusões.

8.2 Interpretação dos Resultados

Nesta secção é apresentada a interpretação dos resultados obtidos com a análise efectuada nos capítulos: Levantamento sobre Políticas de SSI nas Câmaras Municipais em Portugal, Análise das Políticas de Segurança e Análise das Entrevistas.

Com vista a uma melhor estruturação e articulação desta interpretação, recorreu-se ao já apresentado enquadramento para a análise da mudança proposto por Walsham [1993], tendo-se organizado a interpretação nas vertentes do Conteúdo, Processo e Contexto das políticas de SSI.

8.2.1 Conteúdo

Analisados os documentos autárquicos que contêm as políticas de SSI, constatou-se que dos mesmos resulta um particular e especial enfoque em torno de questões que têm o propósito de salvaguardar os recursos informáticos (numa óptica mais global), acesso à internet e aos sistemas de correio electrónico, activos e tecnologias de informação e optimização de recursos.

No âmbito do presente trabalho foram consideradas várias componentes, seguindo as posições preponderantes no domínio da literatura sobre as políticas de SSI, tendo-se escolhido as enumeradas na Tabela 26.

Conforme já anteriormente mencionado, todas as componentes referidas no âmbito da Tabela 26 estiveram presentes, denotando-se, no entanto, uma variação muito significativa no que se refere às respectivas frequências de surgimento, conforme aliás se observa pelas colunas com os resultados absolutos e percentuais, e que variam num intervalo entre 1 – 25, constatando-se a existência de uma relação evidente entre a intensidade da frequência das componentes da política de SSI e um âmbito mais ou menos alargado da sua parametrização. Assim, poder-se-á afirmar que quanto maior for a amplitude ou abrangência dos parâmetros da componente, maior será a probabilidade de ser integrada na política de SSI da Câmara Municipal.

Da supra referida análise constatou-se, ainda, uma grande diversidade ou variedade de abordagens, sendo que, apesar de uma posição consolidada dos principais académicos ou investigadores, em torno das componentes que devem integrar uma política de SSI, na verdade, conforme resulta da análise da Tabela 26 (Componentes Presentes nas Políticas de SSI), deste trabalho de investigação, não existe uma convergência absoluta de todos os documentos acerca das componentes que são tratadas, dando-se mesmo o caso de algumas das componentes tidas pela literatura como recomendáveis para uma efectiva política de SSI, não constarem de nenhum dos documentos sujeitos a apreciação, designadamente: Monitorização do cumprimento, Crenças, Importância da segurança da informação, Nível de segurança pretendido, Entidade responsável pela política de SSI, Definição da Segurança da Informação, Compromisso da gestão e Controlos imprescindíveis.

Pese embora se possa compreender a desconsideração de algumas componentes, como seja o caso da “Crença”, não se pode deixar de considerar como absolutamente angulares numa efectiva política de SSI a presença e consideração das demais componentes citadas, sem as quais não será possível aferir da efectividade e eficácia da política que se pretende levar a cabo.

Sublinha-se, ainda, a notória ausência, em todos documentos analisados, no âmbito da componente “Definição da Segurança da Informação”, de uma densificação do conceito de Segurança da Informação, elemento central para a definição de qualquer política de SSI, assim, a consolidação de um conceito de “Segurança da Informação”

é uma mais-valia para a elaboração de políticas de SSI consistentes, completas e mais convergentes no plano nacional, sem prejuízo dos exercícios de modulação às especificidades de cada edilidade, fazendo constar dos documentos de uma política de SSI o entendimento mais consensual acerca do mesmo.

Embora se verifique um número considerável de políticas de SSI aprovadas pelo executivo das Câmaras Municipais, o compromisso da gestão não se verifica em nenhum dos 25 documentos. Por "compromisso da gestão" entende-se uma declaração de compromisso da gestão para a segurança da informação. Nessa declaração espera-se ver manifestado o apoio e empenho dos executivos na realização dos objectivos da segurança da informação e em conformidade com o estabelecimento de normas de protecção da informação.

O facto de esta componente não ser mencionada poderá ser entendido que essa ausência se deve ao facto de considerarem suficiente a aprovação do documento e que essa aprovação poderá ser entendida pelos utilizadores como um compromisso da gestão para com a segurança da informação.

Os documentos analisados, procurando seguir de perto as posições dominantes da literatura que se debruça sobre as questões da SSI, são, no entanto, omissos em algumas das componentes tidas por relevantes para que estas sejam eficazes. Assim, pese embora as lacunas ou omissões já referidas, os documentos analisados servem de ponto de partida ou base para o desenvolvimento ou sustentação de uma proposta de modelo de política SSI, que se pretende apresentar, nomeadamente na Secção 8.4 deste capítulo, para as Administrações Municipais, desde logo porque se revela alinhamento, não apenas entre as componentes referidas na literatura e os documentos autárquicos de SSI, mas também destes últimos entre si.

As políticas de SSI assumem um âmbito multifacetado, compreendendo vários aspectos, dos quais se destacam por ordem decrescente a preocupação em torno das pessoas, funcionários e utilizadores que acedem aos sistemas informáticos, a preocupação em torno do sistema informático, em si mesmo, e das unidades organizacionais que a ele acedem. Evidencia-se, através da ordem previamente referida, uma preocupação preponderante acerca dos riscos advenientes do factor humano, acolhendo-se o entendimento de que o erro humano poderá constituir, pelo seu grau de probabilidade de ocorrência, o maior desafio para a política de SSI.

As recomendações que as políticas de SSI contêm variam conforme o tipo de utilizador a que se reportam. Para um utilizador genérico verificam-se por ordem decrescente da sua frequência os seguintes: Procedimentos e Responsabilidades Operacionais; *Backups*; Manipulação de Suportes Informáticos e Segurança de Ficheiros de Sistema. Para os Técnicos de SI/TI a recomendação que as políticas contêm é sobre o Controlo de Acesso às Aplicações e à Informação. Para a Unidade de SI/TI a recomendação refere-se à temática Política de Segurança da Informação. Constata-se pois, que os documentos de política de SSI procuram ajustar os seus dispositivos à natureza e preparação dos seus destinatários. Assim, pode afirmar-se que o número, profundidade e variedade das recomendações destinadas aos utilizadores com menor grau de conhecimento e preparação em questões de informática é superior àqueles que se destinam aos técnicos com preparação mais avançada nestas temáticas.

Do teor dos documentos municipais de política de SSI resulta evidente uma tendência para um carácter mais impositivo ou imperativo na adopção ou abstenção de comportamentos quanto a todos os que acedem aos sistemas de informação, evidenciando-se um número pouco relevante de recomendações (28), face ao número de proibições (207), obrigações (179) ou deveres (148).

As políticas de SSI, reflectidas nos documentos apreciados para o presente trabalho de investigação, revelam um elevado grau de imposição ou de prescrição de comportamentos ou condutas, tendo um carácter inegavelmente prescritivo, porém, atento o elevado nível de detalhe ou minúcia com que, algumas das políticas, são abordadas, estes assumem um carácter também descritivo.

No que se refere à natureza assumida pelos documentos autárquicos de SSI, observa-se que na maior parte dos casos esta varia em função do perfil do utilizador, ou seja, verifica-se que sempre que há um acesso mais alargado aos sistemas de informação, designadamente por parte dos particulares, esse acesso é disciplinado por regulamento, que para ter eficácia externa terá que ser aprovado pela Assembleia Municipal; sempre que o acesso aos sistemas de informação local se realiza, apenas, no âmbito e pelos recursos humanos da Câmara Municipal, a disciplina é estabelecida por normas, instrução de trabalho, política ou regras que emanam do executivo municipal para os seus trabalhadores.

Constata-se, da análise dos documentos que reflectem as políticas locais de SSI, que subsistem incidências que se podem dizer transversais à generalidade dos documentos, tal como se resume na Tabela 83.

Temáticas Existentes nas Políticas	Número Políticas
Utilização do correio electrónico	14
Utilização da Internet	11
Utilização do equipamento informático	10
Atribuições dos utilizadores	10
Segurança informática e dos sistemas de informação	8
Software protegido por direitos de autor	6
Utilização da rede interna da Câmara	6
Penalidades	6
Disposições gerais	6
Atribuições do gabinete de informática	6
Responsabilidades	6

Tabela 83: Temáticas Existentes nas Políticas

No entanto, resulta clara a preocupação preponderante revelada, pela generalidade dos documentos apreciados, em torno das questões atinentes às matérias tecnológicas e informáticas (regras para a utilização do correio electrónico, da Internet e utilização do equipamento informático), em detrimento daquelas que se relacionam com os respectivos enquadramentos normativos e componente humana, embora como já referido anteriormente a preocupação acerca dos riscos sucedidos do factor humano mereça destaque.

Sublinha-se neste domínio, a circunstância de em pelo menos oito dos documentos analisados surgir o título " Segurança Informática e dos sistemas de informação", o qual integra matérias, também, tratadas noutras temáticas presentes na tabela. Porém, decidiu-se incluir na Tabela 83 todas as temáticas, para garantir a correspondência com todos os documentos analisados.

Relativamente às características das políticas de SSI disponibilizadas pelas Câmaras Municipais aqui analisadas, e dando resposta à questão de investigação número dois, podem-se descrever na sua maioria como documentos de fácil leitura e compreensão, devidamente estruturados e escritos com bastante rigor e com uma linguagem clara e fluida. Contudo, três dos documentos são demasiado sucintos e restritos nos aspectos abordados, em contrapartida, sete dos documentos são demasiado longos, pecando por excesso de tamanho.

O tamanho dos documentos varia entre o máximo de 26 páginas e o mínimo de uma página, sendo o tamanho médio desses documentos de nove páginas.

Ainda relativamente às características das políticas de SSI, no que se refere à aprovação dos documentos, verifica-se que só é referido em 52% dos casos onde ou por quem foi aprovado. A aprovação é na sua maioria em reunião de Câmara, ficando as restantes aprovações a cargo do Presidente e Vice-Presidente de Câmara, Vereador, chefe de divisão e Assembleia Municipal.

Quanto à indicação no documento do intervalo de tempo em que a política deverá ser revista é mencionado em poucos casos. Só um caso se refere a esse período de tempo, daqui decorrendo um potencial desfasamento entre as políticas de SSI e os riscos que vão surgindo com a evolução tecnológica. A consignação de um período máximo de vigência ou de um determinado ciclo de revisão ou actualização é fundamental para assegurar a actualidade e eficiência das políticas de SSI, pelo que a sua inclusão expressa nos respectivos documentos é altamente recomendável.

Quanto às componentes compreendidas nas políticas de SSI das Câmaras Municipais, analisadas no âmbito da presente investigação, assumem um número e frequência variável encontrando-se presentes na enumeração a que se procedeu na Tabela 26. A variedade e frequência tão oscilante das referidas componentes podem decorrer da ausência de modelos claros e coerentes de políticas de SSI que possam ser adoptados pelas Câmaras Municipais em função das características e utilidades dos respectivos sistemas de informação. Os importantes contributos para a definição de políticas de SSI, prestado pela literatura, normas ou legislação, na prática são avulsamente tidos em consideração, sem a presença de quaisquer preocupações de continuidade ou coerência.

As características e componentes de uma política de SSI foram abordadas em Câmaras que não têm política de SSI, mas que estão em formulação ou adopção. Relativamente à questão se vão ter uma política global ou várias políticas parciais, a resposta com excepção de uma Câmara é que vai existir uma única política global de SSI.

Relativamente às componentes que vão estar presentes na política de SSI, as que mereceram maior destaque, ou seja, consideradas fundamentais é estarem

devidamente definidos os papéis e as responsabilidades dos utilizadores e as sanções para os utilizadores que não cumpram o estipulado estarem devidamente determinadas no documento.

8.2.2 Processo

O capítulo "Levantamento sobre Políticas de SSI nas Câmaras Municipais em Portugal" teve como base a elaboração de um inquérito às 308 Câmaras Municipais em Portugal sobre políticas de SSI, tendo-se alcançado uma taxa de resposta de 100%.

A questão principal do inquérito prendia-se com o apuramento da existência de políticas de SSI nas Câmaras Municipais em Portugal, cujo resultado foi que das 308 Câmaras Municipais, 38 (12%) indicaram dispor de políticas de SSI e 270 (88%) indicaram não terem adoptado qualquer política.

Apesar do grande número de Câmaras Municipais que não possuem uma política de SSI, muitas foram aquelas que em resposta ao inquérito afirmaram ponderar a formulação de uma política de SSI. De acordo com o que se conseguiu apurar ao longo dos contactos telefónicos, tal facto ficar-se-á a dever à necessidade de certificação de serviços, no âmbito da certificação da qualidade (ISO 9001) e da adesão a projectos de redes de cidades digitais em Portugal. Parece, assim, que em muitos dos casos, a adopção das políticas de SSI funda-se num processo reactivo por via de factores exógenos às Câmaras que têm que ver com a certificação e participação em projectos de informatização regionais.

Com base nos resultados, observa-se que 66% (177) dos inquiridos sem políticas de SSI estão a ponderar formular uma política, contra os 34% (93) que neste momento não pensam em formular nenhuma política. Face a esta resposta, estes 93 participantes foram inquiridos sobre se entendem a SSI como uma preocupação. A resposta foi invariavelmente afirmativa, ou seja, os respondentes, apesar de não estarem a pensar formular uma política, consideram a SSI como uma preocupação, justificada pelo valor que reconhecem à informação. Numa tentativa de se encontrar uma explicação para esta incongruência foram avançadas explicações pelos inquiridos que se fundam na utilização de diversas tecnologias de SSI, o que, na óptica dos respondentes, dispensa a existência de uma política de SSI sob a forma de um documento escrito.

Quanto à autoria dos documentos que são o repositório das políticas locais de SSI constata-se que apenas em 36% dos mesmos se refere ou identifica os responsáveis pela respectiva formulação, sendo que destes resulta uma preferência pela utilização dos recursos endógenos da administração autárquica, nomeadamente pelos Gabinetes de Informática e, em menor número, pelos serviços ou Departamentos de Administração, pelo que se concluirá que as políticas de segurança da informação são construídas, em regra, considerando os potenciais riscos locais e conhecidos para o SSI e não de forma a considerar riscos potenciais e que surjam para lá da realidade concreta de cada município. Sempre se dirá que a transversalidade do trabalho dos gabinetes de informática identificará e aprofundará os riscos que em concreto podem surgir para o sistema de informação da Câmara Municipal, contudo a participação de

agentes do meio académico na construção de modelos de política de SSI poderá revelar-se da maior importância na medida em que, de alguma forma, garante a actualidade das opções técnicas vertidas nos documentos directores das políticas de SSI.

Relativamente ao processo, ou seja, ao modo como as políticas são formuladas, implementadas e revistas e analisando os dados retirados directamente das entrevistas realizadas constata-se o presente na Tabela 84.

Cluster	Formulação	Implementação	Revisão
Cluster 1	Com base nas necessidades; Apoiada em políticas de outras Câmaras e Pesquisa na Internet	Distribuída em papel; via internet e correio electrónico	Nunca foi revista na maioria dos casos
Cluster 2	Com base nas necessidades e crescimento tecnológico; Seguiram um modelo de outras Câmaras e Escrevendo os procedimentos de segurança que utilizam no dia-a-dia	As chefias fazem reuniões sectoriais; Distribuída na Internet e via correio electrónico	n/a

Tabela 84: Processo das Políticas de SSI

A formulação da política de SSI nas Câmaras Municipais inseridas no *Cluster* 1 e *Cluster* 2 é feita com base nas necessidades detectadas no dia-a-dia e seguindo o modelo de outras Câmaras ou através de pesquisas feitas na Internet, nestes dois últimos casos trata-se de um mecanismo de isomorfismo institucional do tipo mimético, ou seja, consiste em copiar as melhores práticas, ocorrendo este mecanismo de isomorfismo quando uma organização por razões diversas (neste caso por falta de um modelo institucionalizado de uma política de SSI), adopta os procedimentos e práticas que já foram desenvolvidos e provados em outras organizações que pertencem ao seu ambiente específico.

A implementação, segundo as respostas a essa questão efectuada aquando das entrevistas, é feita através da distribuição do documento em papel, via Internet ou correio electrónico. Para as Câmaras entrevistadas pertencentes ao *Cluster* 2 a implementação é feita através de reuniões sectoriais promovidas pelas chefias junto dos utilizadores.

Relativamente à revisão da política, na maior parte dos casos a política de SSI nunca sofreu qualquer tipo de revisão. Esta informação é só referente ao *Cluster* 1, pois só as Câmaras pertencentes a este grupo têm uma política adoptada.

Os problemas experimentados na formulação são mencionados em dois casos, sendo eles a falta de um modelo de política de SSI a adoptar, bem como a pouca informação sobre este assunto.

Relativamente aos problemas detectados aquando da implementação da política, aponta-se a unanimidade encontrada em torno do factor cepticismo dos utilizadores, o qual pode considerar-se inerente à introdução de qualquer processo novo.

Ainda referente ao processo há um aspecto que merece ser destacado que é a responsabilidade pela observância ou cumprimento da política, essa atribuição não merece unanimidade, as respostas variam entre o gabinete de informática e o vereador responsável pela informática, embora na maioria dos casos essa responsabilidade seja do gabinete de informática.

8.2.3 Contexto

A média dos anos de existência da política no total das 38 Câmaras é só de três anos, o que indica que a sensibilidade para a adopção de políticas de SSI é recente.

A síntese dos dados recolhidos nas entrevistas tem por base o Capítulo 7 (Análise das Entrevistas), onde foi feita a análise das entrevistas efectuadas aos 44 Municípios. Constata-se, da análise das entrevistas, e dando resposta à questão de investigação número um, que os factores facilitadores na adopção de uma política de SSI numa Câmara Municipal, e que podem garantir que uma política tenha sucesso, assumem diferentes naturezas, que permitem que se agrupem da seguinte forma:

Políticos

- Definir os objectivos para a segurança
- Existir vontade política
- Ter aprovação do executivo
- Ser do conhecimento de todos os utilizadores

Humanos

- O documento não ser extenso
- Existir formação dos utilizadores
- Monitorizar o cumprimento da política
- Existir empenho na implementação
- Os utilizadores entenderem as vantagens
- Existir formação dos técnicos

Tecnológicos

- Aquisição de TIC

Por outro lado, dessa análise resulta que os factores inibidores na adopção de uma política de SSI numa Câmara Municipal são agrupados nas seguintes categorias:

Políticos

- A política não ser aprovada

Humanos

- Falta de tempo e de recursos humanos
- Resistência dos utilizadores
- Falta de tempo e programação dessa acção
- Desobediência dos utilizadores

Tecnológicos

- Satisfação com as TIC que estão a ser utilizadas
- Existência de tecnologia suficiente para garantir a segurança

Relativamente a factores inibidores para a adopção de políticas de SSI nas Câmaras Municipais destacam-se dois: a resistência dos utilizadores e desobediência dos utilizadores. A resistência à mudança é sempre grande quando há alterações às rotinas de trabalhos dos utilizadores e a adopção das políticas não é excepção, assim, a conversão das meras recomendações em actos normativos de carácter imperativo e com a adopção de sanções ou restrições para quem desrespeite as políticas de SSI poderá revelar-se como um forte instrumento inibidor da concretização de verdadeiras políticas de SSI, que desejavelmente deverão ser complementadas com uma forte aposta na divulgação da importância de cumprir as regras de SSI e na formação dos utilizadores.

Dando resposta à questão de investigação número três, constata-se a presença de uma relação inibidora de vários factores para a adopção de políticas de SSI por parte das Câmaras Municipais. Com efeito, verifica-se que a satisfação com as tecnologias de informação acaba por desmotivar a realização de novos investimentos com novas tecnologias, ou novas formas de operar, já que os hábitos criados e enraizados por parte dos utilizadores desmotiva a realização de novas acções de formação, com vista à alteração de comportamentos, mais consentâneos com a SSI e, por essa via, potencialmente geradores de conflitos e tensões nos serviços.

Refira-se, ainda, que a especificidade das matérias, bem como o investimento na formação e valorização de políticas de SSI, acaba por constituir um móbil de desmotivação dos decisores políticos, com uma margem reduzida no que se refere a gastos e gestão de recursos humanos, sempre parcos face às exigências com que o Poder Local hoje se confronta.

Como forma de potenciar a adopção de uma política de SSI em uma Câmara Municipal, pode-se avançar com o seguinte: Formação dos utilizadores, monitorizar o cumprimento da política, definir os objectivos para a segurança, o responsável pela implementação empenhar-se para que seja bem sucedida, ter aprovação do executivo, os utilizadores entenderem as vantagens inerentes a estas medidas, haver vontade política para que uma política seja formulada.

Constatou-se nesta análise que os factores facilitadores para a adopção de uma política de SSI nas Câmaras Municipais é que o documento tenha aprovação superior, seja pelo executivo em Reunião de Câmara ou pela Assembleia Municipal, não seja demasiado extenso, que os utilizadores sejam formados não com acções de formação sobre nenhum software, mas sim eticamente, para assim poderem compreender os objectivos pelos quais se adopta uma política no Município.

Relativamente ao contexto que afecta as políticas de SSI, ou seja, nos factores pertencentes ao contexto externo e ao contexto interno das Câmaras Municipais e analisando os dados retirados directamente das entrevistas realizadas constata-se o presente na Tabela 85.

Contexto	Externo	Interno
Cluster 1	Formação dos utilizadores	Resistência dos utilizadores
Cluster 2	n/a	Falta de tempo e de programação dessa acção
Cluster 3	Processo de certificação de qualidade e Aquando da realização do inquérito deste trabalho	Falta de tempo e de recursos humanos
Cluster 4	Aquando da realização do inquérito deste trabalho	Satisfação com a protecção providenciada pelas TIC

Tabela 85: Contexto das Políticas de SSI

Relativamente aos factores facilitadores e inibidores da adopção de políticas de SSI pelas Câmaras Municipais Portuguesas, destacam-se os seguintes:

- As Câmaras com política indicam como factor externo facilitador a formação dos utilizadores promovida pela administração central e como factor inibidor interno a resistência dos utilizadores.

- As Câmaras que não têm política de SSI, mas que estão em formulação ou adopção indicam como factor interno inibidor a falta de tempo e de programação dessa acção.

- As Câmaras que não têm política de SSI, mas que têm intenção de adoptar uma, referem como factores externos facilitadores o processo de certificação de qualidade e aquando da realização do inquérito deste trabalho de investigação e como factor interno inibidor a falta de tempo e de recursos humanos.

- As Câmaras que não têm política de SSI e não tem intenção de adoptar uma, referem como factor externo que os poderá eventualmente pensar no assunto foi aquando da realização do inquérito deste trabalho e como factor interno que inibe essa possibilidade a satisfação com a protecção providenciada pelas TIC.

Em suma, os factores que precipitam a adopção de uma política podem ser articulados em termos de contexto interno e externo, se internamente os políticos e os utilizadores tiverem a noção real dos benefícios de uma política, para a poderem pôr em execução e os utilizadores para a aceitarem e se externamente existirem modelos de políticas de SSI que possam ser adaptadas por uma Câmara e também externamente, a nível da Administração Central, apostarem em programas de certificação dos serviços e em formações específicas dirigidas aos técnicos e aos utilizadores, são factores que se forem articulados facilitam a adopção por parte de uma Autarquia de uma política de SSI.

Por outro lado, os factores externos e internos que obstam à adopção de uma política, são, ao nível externo, a falta de um modelo de política de SSI e ao nível interno a satisfação com a protecção providenciada pelas TIC, a falta de tempo e de recursos humanos para a formulação do documento e a resistência dos utilizadores.

8.3 Análise Crítica Face à Literatura

Nesta secção é apresentada a análise crítica dos resultados obtidos face à literatura.

8.3.1 Conteúdo

Face ao estudo realizado e para o universo considerado, constata-se uma diferença entre aquilo que é defendido na literatura e o que se verifica na prática. Apesar de autores como Baskerville e Siponen [2002, p. 337] afirmarem ser "muito consensual que uma boa política de segurança da informação constitui a base da segurança da informação das organizações", os respondentes parecem ainda não estar suficientemente alertas ou convencidos para o fundamento dessa observação.

Os documentos analisados retratam decisões no âmbito da gestão e utilização da informação e recursos informáticos nas Câmaras Municipais, com incidência na vertente da SSI.

Da análise das políticas de SSI verifica-se que as Câmaras Municipais abordam a questão da segurança de forma diversificada, contudo partilham certas preocupações e processos de actuação neste âmbito.

O tamanho das 25 políticas analisadas, cuja média é de nove páginas excede um pouco o definido como óptimo, por investigadores destas temática e já indicado neste trabalho de investigação, que descrevem que uma política não deve ser demasiado grande, definindo o tamanho de cinco páginas como o mais indicado.

Para Höne e Eloff [2002b], uma política deve ser de fácil leitura e compreensão, não contendo demasiado texto, ou seja, apresentar-se resumida, e de elevado nível de abstracção. Esta constatação difere dos documentos analisados, uma vez que alguns são demasiado longos, não sendo de modo nenhum resumidos nem de elevado nível de abstracção. Relativamente à compreensão do seu conteúdo e à sua fácil leitura poder-se-á dizer que respeitam a constatação do autor mencionado.

Existe igualmente simultaneidade em relação ao carácter prescritivo ou descritivo das políticas de SSI. As políticas de SSI, reflectidas nos documentos apreciados para o presente trabalho de investigação, revelam um elevado grau de imposição ou de prescrição de comportamentos ou condutas, tendo um carácter inegavelmente prescritivo, característica apontada por Siponen [2000a] para estes documentos.

O carácter normativo e regulamentar das muitas disposições analisadas nos documentos que servem de base ao presente trabalho revela uma ausência de uniformidade das designações dos referidos documentos que se intitulam desde regulamentos a normas, passando por manuais e instruções ou regras de trabalho, surgindo um único título com referência a "política", mas de uso de computador, programas de software e internet.

A situação descrita releva o facto de não se encontrar inculcada na administração local, a ideia de que esta matéria constitui objecto de uma verdadeira política, considerando-se desejável a adopção de um modelo uniforme para as autarquias locais, eventualmente concebido sob a égide da Associação Nacional de Municípios

Portugueses e que contemple todas as componentes reconhecidas como importantes pela melhor literatura desta área do conhecimento.

8.3.2 Processo

Conforme referido por Höne e Eloff [2002a] nem sempre é fácil redigir o documento da política, verificando-se que muitas vezes se fazem cópias de minutas disponíveis, não reflectindo a verdadeira cultura da organização, ou seja, não resultando assim num documento efectivo orientado para a SSI. Essa constatação é também verificada neste trabalho de investigação, uma vez que a formulação de uma política resulta em alguns casos de pesquisa na Internet e apoiada em políticas de outras Câmaras, nos dois casos pode-se encontrar tanto bons como maus exemplos de uma política de SSI, mas independentemente disso o ajustamento desse documento à realidade da Câmara onde se vai implementar é impreterível.

No que respeita à sua durabilidade, e ainda segundo os autores anteriormente citados, as revisões do articulado da política devem ser efectuadas periodicamente, mas não constantemente. O que se verifica nas políticas analisadas é que com excepção de um caso, nunca foram feitas revisões no documento. Segundo Kee [2001], as políticas deveriam ser escritas utilizando a regra SMART (*Specific, Measurable, Agreeable, Realistic and Time-bound*), ou seja, devem ser escritas de uma forma Específica, Mensurável, Agradável, Realista e Delimitada no tempo.

Uma política de SSI deve demonstrar comprometimento, contudo o que se observa nos documentos analisados é que os mesmos nem sempre são aprovados superiormente e em alguns casos não está referenciado se foram ou não aprovados por uma chefia ou pelo executivo.

Para ter aceitação, é preciso que a cúpula do Município apoie e participe do processo de implantação. É de suma importância o aval do executivo para que todos aceitem, respeitem as normas e procedimentos vinculados na política de segurança da informação.

Relativamente ao facto de uma política ser disseminada em toda a organização, há simultaneidade entre a literatura e o referido pelos entrevistados, que referenciam que a implementação é sempre feita com a difusão a todos os utilizadores e colaboradores do Município da política que está a ser promovida. Para a implementação adequada de uma política é necessária a sua correcta divulgação junto dos utilizadores da mesma.

É de referir que um aspecto tão relevante como é a responsabilidade do dono da política perante o desenvolvimento, revisão, avaliação e manutenção da política de SSI só seja referido em três documentos. A monitorização por um responsável deve incluir acções de avaliação e reavaliação com vista a garantir que os procedimentos em utilização vão ao encontro dos requisitos originalmente especificados.

Para além destes aspectos, o processo de adopção de uma política é também essencial, sendo considerado o processo efectivo da política, é aqui que se verifica a sua verdadeira aceitação, por isso é um processo que tem início em simultâneo com

a sua implementação tendo como resultado a verdadeira consciencialização da importância da política e consequente cultura organizacional. As fases pelas quais deve passar o processo de adopção de uma política não são praticamente mencionadas nas diferentes análises de dados efectuadas no presente trabalho. O processo de adopção segundo Karyda et al. [2005] tem como *inputs* a avaliação efectuada à política aquando da sua implementação, os procedimentos e práticas de trabalho que implementam a política de segurança e os processos de formação e educação dos utilizadores. Com base nestes dados, o processo vertente inclui a resolução de possíveis conflitos e dificuldades detectadas na aplicação de certos parâmetros contidos na política, bem como manter os utilizadores e gestores informados acerca da agenda da SSI.

8.3.3 Contexto

Um aspecto que é considerado factor crítico de sucesso para uma boa implementação é a definição de penalizações para os utilizadores que não cumprem o estipulado pela política. Este aspecto não foi evidenciado pelos inquiridos nas entrevistas realizadas como factor crítico de sucesso para a adopção ou implementação de uma política de SSI numa Câmara Municipal. Tal facto poder-se-á explicar pela circunstância de os inquiridos, com formação maioritariamente na área de informática, evidenciarem uma fraca sensibilidade para as questões de ordem jurídica ou formal, bem como pelo facto de reconhecerem a limitada preparação dos utilizadores na compreensão e manuseamento dos mecanismos de segurança de informação.

Whitman e Mattord [2005] indicam que as políticas de segurança são as directivas mais baratas de formular, mas as mais difíceis de implementar adequadamente, pelo que face aos resultados se questiona se os respondentes entenderão as dificuldades da aplicação concreta das políticas de SSI como um dos travões à sua adopção. Eventualmente, o problema poderá encontrar-se a montante, nomeadamente na falta de um modelo para a formulação das políticas de SSI, com a indicação clara das suas características e componentes, adequado à realidade organizacional e institucional da Administração Pública Local.

A literatura sobre esta temática denuncia a contradição existente no facto de, apesar de diminuto o investimento a efectuar com a formulação de políticas SSI, poucas serem as Câmaras Municipais que adoptaram tais políticas, considerando que a relação custo/benefício favorece a adopção de políticas SSI, não sendo este, verdadeiramente, o factor decisivo e inibidor de tal aprovação.

A mudança institucional proposta vai variar conforme o *Cluster* em que a Câmara Municipal se incluiu. Com excepção do *Cluster* 4, onde a institucionalização do modelo proposto tem de ter acompanhamento de formação e esclarecimento dos benefícios inerentes à adopção de uma política de SSI, as restantes podem formular ou adaptar a existente ao modelo proposto.

O trabalho realizado por Karyda et al. [2005], que se debruçou sobre aspectos de contexto, explorando o processo de formulação, implementação e adopção de uma política de segurança em duas organizações diferentes, isolou um conjunto de

factores de natureza contextual que poderiam influenciar a aplicação das políticas. Alguns desses factores são similares e outros diferentes dos observados neste trabalho de investigação.

Relativamente ao factor relacionado com a estrutura organizacional, verifica-se uma simultaneidade com este estudo, uma vez que se observa a preocupação com uma organização flexível e não uma estrutura rígida que possa constituir um obstáculo para a gestão da SSI.

Comparativamente em termos de cultura organizacional, verifica-se que os responsáveis de informática nas Câmaras municipais têm implementado aos seus utilizadores um código de práticas ou de ética, verificando-se com este estudo que as políticas de SSI em muitos dos casos são a passagem para papel do que se faz no dia-a-dia.

Em relação à contribuição para as metas dos utilizadores, o sincronismo não é tão evidente neste estudo, embora se verifique claramente que se os utilizadores entenderem que as medidas e restrições impostas na política são necessárias para garantir a segurança da informação, a sua adopção poderá ser bem sucedida. É de referanciar aqui que a resistência dos utilizadores foi um dos factores mais mencionados como inibidor para a implementação de uma política de SSI e que a formação desses utilizadores seria a forma de ultrapassar esse obstáculo.

No que diz respeito à participação dos utilizadores no processo de formulação, não se verificou neste estudo um envolvimento destes neste processo. Note-se que indirectamente os utilizadores estão a participar, uma vez que para formular uma política é necessário, para além de outros aspectos, ter em conta as linhas de orientação das normas de gestão da segurança e melhores práticas.

Relativamente à formação e educação, a sintonia entre os dois estudos não é evidente, embora se mencione e seja claro que a formação dos utilizadores seja um dos factores críticos para o sucesso de uma política, o acompanhamento da avaliação da eficácia da política de segurança para a implementação e adopção bem sucedidas das políticas de segurança da informação não se registam no presente estudo.

O apoio da gestão como factor de máxima importância para o sucesso de uma política de SSI é um factor comum aos dois estudos. O empenho e envolvimento do executivo da Autarquia para com a SSI terão um impacto substancial na aplicação prática das provisões da política.

A definição do responsável pela segurança é mencionada nos dois estudos, embora nos documentos das políticas analisados não seja demais referido de quem é a responsabilidade de conduzir a formulação e implementação da política de segurança. Nas entrevistas realizadas ficou mais claro que o responsável pela segurança e que possa contribuir para a implementação e adopção bem sucedida da política de SSI é o gabinete de informática.

8.4 Recomendações

Nesta secção são feitas recomendações com vista à melhoria dos níveis de adopção de políticas de SSI por parte das Câmaras Municipais Portuguesas.

8.4.1 Conteúdo

A análise dos documentos que serviram de base ao presente trabalho permite operar o diagnóstico da situação, evidenciado um número diminuto de autarquias que se municiaram de documentos que têm a Segurança dos Sistemas de Informação como temática, 38 em 308, das quais foram analisadas 25 que revelaram um tratamento díspar destas matérias.

Com efeito, constata-se que enquanto os documentos produzidos por algumas das Câmaras Municipais acentuam as suas preocupações na criação de normas relativas à utilização de programas, utilização de internet, acessos físicos e lógicos, bloqueio de sites, utilização do correio electrónico e de outros recursos tecnológicos (tratando alguns dos documentos, apenas, uma ou algumas destas temáticas), outros documentos reflectem a sua preocupação, apenas, com as regras de comportamento dos utilizadores.

Conclui-se, assim, pela necessidade e utilidade da recomendação de concepção de dois modelos de políticas de SSI, moduladas em função da natureza dos sistemas de informação a preservar e da dimensão da própria autarquia. Os modelos a conceber devem, assim, ser susceptíveis de uma adaptação às estruturas em que serão implementados, dando uma resposta adequada e eficaz à segurança de informação.

A opção por dois modelos, em vez de um único, tem em consideração as diferentes naturezas de utilização dos SSI, reconhecendo as diferenciadas responsabilidades e habilitações dos respectivos utilizadores e os potenciais riscos que os mesmos representam para os sistemas.

Avança-se, assim, com a concepção de dois modelos de política de SSI, designadamente um dirigido aos dirigentes e técnicos informáticos do Município – Proposta A e outro vocacionado para questões relativas aos modelos de conduta/procedimentos dos diferentes utilizadores – Proposta B (cf. Apêndice I).

Estes modelos não são mais que metapolíticas, isto é são directrizes para a criação e manutenção das políticas, ou seja, que indicam como a organização poderá criar e manter a sua política de segurança. Entre suas atribuições, definirá quem são os responsáveis pela elaboração e modificação das políticas de segurança e em quais momentos este processo deve ser iniciado. Conforme proposto por Baskerville e Siponen [2002] as políticas de SSI devem desenvolver-se com a ajuda das normas e linhas de orientação gerais da gestão da SSI, e seguir o mais possível as directivas e normas de segurança existentes.

Pese embora a diferente natureza dos serviços e das respostas que cada uma das Administrações Públicas deve dar à sua demanda, na verdade, vigora uma grande uniformidade de procedimentos por parte das várias administrações públicas, as quais devem observar o Código do Procedimento Administrativo, o qual serve de

referência base ao trabalho desenvolvido pela generalidade das administrações. Por outro lado, existe uma relação de intercomunicação entre as várias administrações, verificando-se, não raras vezes, a necessidade de os sistemas de informação se interpenetrarem. Assim, observando-se as mesmas regras de procedimento nas administrações e verificando-se a interconexão dos sistemas das várias administrações públicas, fará sentido a concepção de um modelo geral que lhes seja aplicável, sem prejuízo da sua capacidade de adaptação e ajustamento.

No caso vertente, e atenta à dimensão da Administração Pública Portuguesa e o propósito deste trabalho de investigação, procurar-se-á desenvolver e reflectir acerca de um modelo comum para as autarquias locais, de cariz municipal, com as condicionantes e particularidades que previamente se referiram.

Os elementos de uma política de SSI, presentes nos modelos propostos como Proposta A e Proposta B, ou seja, o modelo direccionado para o gabinete de informática e para o respectivo pelouro (Proposta A) e o modelo direccionado para os diferentes utilizadores (Proposta B), encontram-se indicados na Tabela 86.

Elementos de uma Política de Segurança	Proposta A	Proposta B
l – Propósito	x	x
2 – Âmbito	x	x
3 – Definições	x	x
4 – Requisitos	x	x
5 – Directivas	x	x
6 – Responsabilidade	x	x
7 – Comunicação de Incidentes	x	x
8 – Compromisso de gestão		x
9 – Punições		x
10 – Procedimento de comunicação		x
11 – Alvo de comunicação da política		x
12 – Declaração de conhecimento		x
13 – Localização da política		x
14 – Autor da política	x	x
15 – Data de elaboração/aprovação e entrada em vigor	x	x
16 – Aprovação da política	x	x
17 – Programa de revisão	x	x
18 – Aprovação das revisões	x	x
19 – Entidade responsável pela política		x

Tabela 86: Elementos de uma Política de Segurança – Proposta A e Proposta B

Uma explicação breve das componentes e características propostas anteriormente para os dois modelos é apresentada de forma a complementar e clarificar os diferentes elementos mencionados.

1 – Propósito da política

A definição do propósito da política de SSI é crucial. O propósito do documento tem de ser definido indicando o porquê da sua formulação, bem como o que se pretende atingir com essa política de SSI.

2 – Âmbito da política
A definição da abrangência da política, ou seja, as unidades organizacionais às quais se aplica a política, a que indivíduos, a que sistemas ou a que informação.

3 – Definições
É essencial que a política contenha um conjunto de definições, que de forma sucinta sejam delimitadas definições inerentes à segurança da informação de forma a assegurar uma compreensão uniforme e sem ambiguidades por todos os destinatários do documento.

4 – Requisitos
Uma exigência para os esforços de segurança da informação empreendida pela organização. Um requisito implica geralmente um tipo e nível de protecção necessário para assegurar um certo nível de segurança para o sistema de informação.

5 – Directivas
A definição das directivas diz respeito às decisões para a implementação da segurança da informação.

6 – Responsabilidade
A componente responsabilidade é a mais presente nas políticas de SSI, pois define as responsabilidades específicas de um utilizador, indicando os comportamentos que devem ter, bem como os comportamentos proibidos.

7 – Comunicação de Incidentes
É a indicação dos procedimentos que um utilizador deve ter para comunicar ameaças identificadas ou suspeitas, anomalias e incidentes detectados.

8 – Compromisso de gestão
É crucial o compromisso por parte do Executivo Municipal ou pela Assembleia Municipal, transmitindo assim vontade política para com a SSI. Esse comprometimento potencia que a aceitação do documento pelos utilizadores seja mais séria.

9 – Punições
As consequências a aplicar caso os utilizadores não cumpram o estipulado na política é muito importante para o rigor na sua aplicabilidade.

10 – Procedimento de comunicação
A definição dos mecanismos ou meios de comunicação da política de SSI aos seus destinatários é fulcral para não existirem falhas nesse processo.

11 – Alvo de comunicação da política
O alvo de comunicação da política incide sobre os destinatários ou público da política, ou seja, a quem a política deve ser comunicada (funcionários, grupos organizacionais, munícipes).

12 – Declaração de conhecimento
Esta componente é também muito importante pois diz respeito a uma declaração assinada por todos os destinatários da política em como leram e tiveram conhecimento deste documento.

13 – Localização da política
A indicação do local onde vai ser colocada a política é também importante ser mencionado no documento, para tornar mais ágil a sua consulta quando necessário.

14 – Autor da política
Refere-se à indicação do nome ou função da pessoa que elaborou a política de SSI.

15 – Data de elaboração/aprovação e entrada em vigor
Refere-se à indicação da data em que a política foi elaborada, aprovada e quando entra em vigor.

16 – Aprovação da política
É de crucial importância a indicação da aprovação da política de SSI, por quem foi e devidamente rubricada.

17 – Programa de revisão
O processo definido para a revisão da política compreende a definição da data ou período em que grandes alterações para a política devem ser feitas. A indicação pode revestir a forma de uma data precisa ou pode apontar para um intervalo de tempo após o qual deverá ser revisto.

18 – Aprovação das revisões
Refere-se a uma declaração do Executivo, que aprova a versão revista da política. Esta componente só se aplica em políticas que foram submetidas a um processo de revisão.

19 – Entidade responsável pela política
É a indicação do nome ou da função da pessoa ou a designação da entidade responsável pela política.

Crê-se que estes dois modelos de metapolítica são suficientes para a maior parte das Câmaras Municipais, contudo um terceiro modelo ou um aditamento à Proposta B poderia ser feito, no que concerne aos utilizadores externos à Autarquia, como é o caso dos Munícipes e Fornecedores, entre outros.

8.4.2 Processo

Relativamente à questão de investigação número quatro, que se refere às recomendações que poderão ser avançadas de forma a potenciar a adopção de políticas de SSI nas Câmaras Municipais Portuguesas, podem ser sintetizadas em seis pontos fulcrais:

- Definida
- Aprovada
- Publicada
- Comunicada
- Entendida
- Avaliada

A política de SSI deve ser devidamente definida e redigida indo de encontro às características da Câmara Municipal para a qual se destina, tendo por base então a sua natureza e público-alvo sem deixar de ter em conta as normas existentes para a SSI. Antes de se formular uma política, é necessário ter em linha de conta os objectivos da Câmara Municipal para esta área, bem como os seus processos e cultura organizacional.

A aprovação superior é fundamental para demonstrar comprometimento superior tornando dessa forma a sua implementação mais eficaz. Este sinal adicional de compromisso do Executivo para com a segurança da informação provoca nos utilizadores a que é dirigida outro tipo de acolhimento.

O documento deve ser publicado e posteriormente comunicado a todos os utilizadores do sistema de informação da Câmara Municipal, podendo os mesmos serem internos ou externos à edilidade. É facilmente entendível que todos os actores organizacionais devem ter conhecimento da política de segurança, embora a forma de dar conhecimento possa variar (circular interna, disponibilização da política na Internet da Câmara ou outros mecanismo de publicação).

A mesma tem de ser entendida, ou seja, não deve ser demasiado longa, deve estar devidamente estruturada e deve estar escrita numa linguagem de fácil leitura e entendimento. De pouco ou nada servirá ter uma política de SSI se a sua compreensão e exequibilidade se revelarem impossíveis.

Por fim, a política de segurança da informação deve ser sempre revista, nunca devendo apresentar-se desactualizada.

8.4.3 Contexto

A proposta dos elementos apresentada no ponto 8.4.1 é um possível modelo a seguir pelas Câmaras Municipais Portuguesas. Esta proposta emerge do facto da conclusão iminente a este estudo ser que a adopção de uma política de SSI ainda não está institucionalizada, ou seja, não exista ainda um conjunto de regras e de normas que integrem uma política e que sejam compartilhadas por todas as Câmaras Municipais Portuguesas.

A institucionalização poderá ser a melhor forma para que a existência de políticas de SSI seja uma realidade nas Autarquias em Portugal.

A problemática do processo de institucionalização tem sido, há já alguns anos, alvo de investigação e atenção de vários investigadores, que se debruçam sobre esta temática, constituindo um dos elementos estudados e abordados no âmbito da teoria

institucional, a qual perspectiva e explica, segundo de Sá-Soares [2009, p. 524] "o modo como determinadas estruturas ou mecanismos de natureza reguladora, normativa ou cultural-cognitiva, que sejam fundamentais para a institucionalização de um fenómeno, podem ser criadas, mantidas, alteradas e destruídas".

Segundo Scott [2004], a teoria institucional trata dos mais profundos aspectos da estrutura social, considerando os processos pelos quais as estruturas (tais como, esquemas, regras, normas e rotinas) se estabelecem como linhas orientadoras e confiáveis para o comportamento social e investigando a forma como estes componentes são criados, difundidos, adoptados e adaptados ao longo do tempo e do espaço; e a forma como eles caem em declínio e desuso.

As estruturas institucionais consistem nas pressões de natureza reguladora, normativa e cultural-cognitiva, aceites no campo organizacional.

O pilar regulador constrange e regula o comportamento por meio de regras, sanções e punições de natureza formal. Assim sendo, no presente trabalho corresponde á institucionalização de uma política de SSI, podendo as Câmaras seguir os modelos propostos, mas para isso têm primeiro que ser superiormente aprovados.

No pilar normativo a ênfase é colocada numa base moral, mais profunda de legitimação, em que se enfatizam os valores e normas, como elementos capazes de pressionar a acção organizacional, transformando-se, pela utilização quotidiana, em uma obrigação social. Na presente proposta inclui a influência exercida nos Municípios para a política de SSI ser efectivamente implementada.

O terceiro pilar, as estruturas culturais-cognitivas, também sustenta significados que são partilhados entre os actores acerca das estruturas reguladoras e normativas, ou seja, da realidade que cerca os actores, que constroem e continuamente negoceiam a realidade social, num contexto que contempla estruturas simbólicas, objectivas e externas que oferecem orientação. No presente trabalho a orientação vai para a formação dos utilizadores e consequente interiorização nos mesmos dos benefícios desta mudança.

À luz da teoria institucional, no que respeita à agência e estruturação, relativamente às intenções de ter realizado ou vir a realizar determinada acção, a indicação de intenção colectiva de se ter realizado ou de se vir a realizar determinada acção é muito superior à intenção individual. Esses aspectos recolhidos da análise das entrevistas, são focados em questões como quem detectou a falta de uma política de SSI, quem está a elaborar a política, por quem é feita a observância e cumprimento da política, sobre quem vai recair a responsabilidade da sua implementação, quem vai ter conhecimento da política e se a política vai ser superiormente aprovada.

No modelo proposto de institucionalizar um modelo de política de SSI considera-se que esse processo deva ser também colectivo, nomeadamente na aprovação da política que depois de elaborada deverá ter o despacho do director de departamento responsável pela divisão de informática, para posteriormente ser aprovada pelo executivo municipal. Relativamente à elaboração da política é desejável que seja executada colectivamente, com apoio de outras divisões da autarquia se necessário.

Esta proposta pelo facto de não se encontrar incutida na administração local, a ideia de que esta matéria constitui objecto prioritário, como forma de inverter esta situação, considerando-se desejável a adopção de um modelo uniforme para as Câmaras Municipais o possam seguir, eventualmente concebido sob a égide da Associação Nacional de Municípios Portugueses e que contemple todas as componentes reconhecidas como importantes pela melhor literatura desta área do conhecimento.

A teoria institucional é absolutamente crucial, quer como lente interpretativa, quer como lente projectiva, uma vez que as pressões miméticas, coercivas e normativas que existem num ambiente institucionalizado podem influenciar a predisposição para a adopção de novas regras e procedimentos.

A institucionalização para que uma política seja uma realidade nas Câmaras Municipais Portuguesas tem de seguir alguns processos. O processo de institucionalização tem o seu início pela "Inovação" e ocorre em virtude de forças externas, tais como: mudanças tecnológicas, legislação ou forças de mercado. Neste caso, o factor inovação significa a solução para o problema da segurança da informação nas Câmaras Municipais, com a implementação de uma política de SSI.

Segue-se a "Habituação" que se trata de um estágio de pré-institucionalização, ou seja, arranjos estruturais em resposta a esses problemas de segurança da informação, que podem passar pela comparação com outros organismos.

Gerada a solução para o problema, o deslocamento em direcção a um estado mais permanente baseia-se no processo de "Objectivação", que acompanha a difusão da política de segurança, ampliando a sua utilização.

O estádio em que a institucionalização é total é denominado de "Sedimentação" e caracteriza-se pela adopção da política de SSI por todos os utilizadores da Câmara por um período considerado longo no tempo.

De acordo com Scott [2008], o processo de institucionalização pode ocorrer essencialmente em dois formatos: de uma forma naturalista ou com base na actuação de agentes.

O primeiro formato corresponde a uma situação em que o fenómeno se vai institucionalizando de forma natural e gradual, constituindo normalmente um processo lento e moroso. O segundo formato, com base na actuação de agentes, ao contrário da forma naturalista introduz um elemento catalizador, denominado agente, que permite acelerar o processo de institucionalização. Este segundo formato destaca a importância de identificar um conjunto particular de agentes capazes de exercer determinados tipos de acções [Scott 2008].

Ao contrário do que sucede na forma naturalista, a institucionalização com base da actuação de agentes, "os enquadramentos normativos são racionalmente arquitectados, criados e modificados através de processos conscientes e deliberados, o mesmo sucedendo com elementos cultural-cognitivos que, neste caso, tendem também a ser conscientemente concebidos e disseminados por determinados agentes." [de Sá-Soares 2009]

Esta estratégia baseada em agentes pode ser uma das alternativas a seguir para implementar políticas de SSI nas Câmaras Municipais. Os principais agentes que podem ter um papel activo neste processo é a Associação Nacional de Municípios Portugueses, o Executivo da Câmara Municipal, a Assembleia Municipal e os responsáveis pelas unidades ou subunidades orgânicas de informática/SI.

O primeiro agente mencionado parece ser a nível nacional aquele que mais directamente interage com os Municípios. Embora esta associação não tenha um poder impositor de normas ou regulamentos é aquela que mais facilmente comunica com as Câmaras Municipais e assim pode sensibilizar para a importância da implementação de políticas de SSI, bem como sugerir modelos que podem ser adaptados aos diferentes municípios Portugueses.

Os dois agentes seguintes têm também um papel fundamental na adopção de uma política de SSI, sem o envolvimento do Executivo da Câmara Municipal no processo de implementação de uma política, desde a formulação até à revisão a sua adopção não será certamente uma realidade. A aprovação da política tem de ter aprovação da Assembleia Municipal, caso a política se trate de um Regulamento Municipal, por isso o seu papel como agente para a institucionalização de uma política.

Por fim, a realidade portuguesa, claramente evidenciado pelo levantamento e entrevistas levadas a cabo, no decurso deste trabalho, deixa claro que os responsáveis pelas unidades ou subunidades orgânicas de informática/SI têm sido os verdadeiros *pivots* na elaboração das políticas de SSI actualmente existentes.

Garantidos estes elementos, julga-se que estar criada a conjuntura elementar para que as Câmaras Municipais institucionalizem uma política de SSI.

8.5 Conclusão

Apesar da realidade, constatada junto das Câmaras Municipais Portuguesas, parecer evidenciar o inverso, é hoje incontestável, designadamente nos meios académicos, a relevância e utilidade das Políticas de SSI como salvaguarda dos activos da informação numa Câmara Municipal. A importância das políticas foi neste trabalho de investigação mencionada com sustentação teórica e citações de investigadores sobre esta temática.

Ao longo deste capítulo procurou-se abordar as questões de investigação cuja resposta ainda se encontrava pendente, nomeadamente identificar que factores condicionam, positiva ou negativamente, a adopção de políticas de SSI nas Câmaras Municipais Portuguesas.

Tendo-se completado a resposta às questões de investigação que orientaram a realização deste trabalho de investigação, torna-se possível sistematizar as contribuições do presente capítulo em mais dois níveis.

Primeiramente, contemplou-se a resposta a questões que foram colocadas aquando da codificação e análise dos documentos disponibilizados pelas Autarquias,

respostas que complementaram as principais questões de investigação deste trabalho de investigação.

A síntese dos resultados que saiu em grande parte da análise das políticas de SSI e das entrevistas culmina com as respostas ao enquadramento proposto com base no Processo, Conteúdo e Contexto.

Em seguida, perspectivaram-se os resultados alcançados neste trabalho de investigação à luz do conhecimento que se encontra acumulado na literatura sobre políticas de SSI.

Por último, apresentam-se recomendações em forma de proposta com os elementos que uma política de SSI poderá conter, com o intuito de poder inverter os números incipientes de políticas existentes nas Câmaras Municipais Portuguesas, servindo de potencial modelo a seguir. No decurso desta explanação emergiram duas propostas de metapolíticas orientadoras para a formulação de políticas de SSI.

Capítulo 9

Conclusão

9.1 Introdução

No capítulo final desta tese de doutoramento procede-se a um balanço do trabalho de investigação desenvolvido. As conclusões estruturam-se em quatro secções.

Primeiramente resumem-se as principais contribuições da investigação realizada no âmbito das políticas de segurança dos sistemas de informação nas Câmaras Municipais Portuguesas.

Seguidamente, identificam-se e discutem-se as limitações do estudo apresentado, adoptando-se uma organização similar à empregue na apresentação das contribuições.

O capítulo prossegue com a identificação de trabalhos futuros. Uma investigação conducente a um doutoramento, onde uma série de ramificações do assunto central surgem e que por uma série de constrangimentos de tempo ou âmbito, não é possível abranger, são aqui apresentados como pontos promissores para trabalhos futuros.

Finalmente, na última secção, apresentam-se as considerações finais deste projecto de investigação.

9.2 Contribuições

Nesta secção sintetizam-se as principais contribuições que resultam do estudo realizado para o conhecimento do domínio das políticas de segurança dos sistemas de informação nas Câmaras Municipais Portuguesas.

Uma das principais contribuições que este trabalho produziu resulta fundamentalmente no facto de contribuir para colmatar a lacuna existente na falta de uma teoria coerente sobre políticas de segurança e para mitigar a inexistência ou reduzida expressão de estudos empíricos sobre a adopção, conteúdo e implementação de políticas de segurança de sistemas de informação.

Com este trabalho de investigação contribui-se para apresentar um estudo empírico nesta temática, comparando assim o que advoga a literatura sobre políticas de segurança e aquilo que sucede na prática para o campo organizacional em estudo.

O trabalho de análise envolveu um número diversificado de métodos e técnicas de investigação empregues bem como base teórica para essa análise e software apropriado para a codificação das políticas de segurança e das entrevistas. Essa diversidade deveu-se ao facto de se terem efectuado três tipos de análise, iniciando-se o estudo dos dados resultantes do levantamento à totalidade das Câmaras

Municipais, seguiu-se a análise dos 25 documentos das políticas de segurança, terminando com a análise das 44 entrevistas realizadas em Portugal Continental e na Região Autónoma dos Açores.

Pode-se destacar como contributo deste trabalho o facto de sensibilizar um grande número de dirigentes para a problemática da segurança dos sistemas de informação, pelo facto de se ter contactado directamente por telefone com um elevado número de pessoas e posteriormente em número mais reduzido, mas não menos importante, o contacto para a realização das 44 entrevistas.

Outro contributo foi a clarificação sobre o conceito de política de SSI, verificou-se a falta de um entendimento claro e universal por parte dos respondentes aquando do levantamento, para o conceito de política de SSI. Foi com alguma dificuldade que diversos respondentes associaram esse conceito ao conjunto de regras que estabelecem o regime de utilização dos SI das autarquias. Para tal, poderá contribuir a enorme profusão de "roupagens" formais de normas e regras de procedimento existentes nas Câmaras, em virtude das mesmas se acharem vertidas por uma disparidade de documentos, tais como regulamentos internos, normas, despachos e até mesmo sob a forma de avisos no espaço de trabalho.

A identificação das componentes e características das políticas de SSI existentes na Administração Pública Local foi feito com a análise dos 25 documentos, trabalho indubitável para se conhecer a composição dessas políticas de SSI.

A identificação e classificação de factores condicionadores da adopção de políticas de SSI por parte das Câmaras Municipais considera-se ser uma contribuição deste trabalho, prestação que poderá servir para melhor formular e implementar políticas de SSI, uma vez que são conhecidas as fraquezas, bem como os factores que potenciam a sua adopção.

Destaca-se, de igual modo, a proposta de modelos de políticas de SSI. Estes modelos, depois de moldados à realidade de cada Município, podem contribuir para que a institucionalização da adopção de políticas de SSI na Administração Pública Local em Portugal seja uma realidade.

9.3 Limitações

Nesta secção são identificadas e discutidas as limitações deste trabalho e dos seus resultados.

Uma limitação deste trabalho de investigação diz respeito ao número de entrevistas que foram efectuadas. Embora se creia que com base nas 44 entrevistas se tenham gerado dados suficientes para os propósitos deste trabalho, facilmente se aceitará que um maior número poderia resultar num conjunto de dados mais rico e mais sustentado.

Outra limitação refere-se ao facto de um dos aspectos a ter em conta durante a selecção da recolha de dados com o método de investigação "Estudo de Casos", é usar a triangulação para garantir a precisão dos dados obtidos no âmbito das entrevistas realizadas, ou seja, entrevistar mais do que uma pessoa por Município. A

adopção desta técnica teria permitido maior segurança e fiabilidade das informações obtidas junto dos entrevistados e uma maior aproximação à realidade concreta das Câmaras Municipais.

No entanto, a necessidade de gravar em suporte sonoro digital e posterior transcrição das entrevistas realizadas, com acentuado dispêndio de tempo, bem como a dimensão territorial do estudo, de âmbito nacional, com acentuado dispêndio económico, inviabilizaram a aplicação daquela técnica.

Outra limitação deste trabalho de investigação prende-se com a delimitação do estudo ao território nacional, pelo que sob o ponto de vista de eventuais diferenças culturais ou de diferenças ao nível das missões e do funcionamento de entidades similares às Câmaras em outros países ou em outras culturas nada se poder concluir.

9.4 Investigação Futura

No decorrer da elaboração deste trabalho de investigação foi possível identificar algumas linhas orientadoras para possíveis trabalhos a desenvolver. Nesta sequência identificam-se alguns pontos promissores de partida para trabalhos futuros.

1. Proposta de um enquadramento legal e distribuído por todos os organismos que auxilie os Municípios e outros na formulação e implementação das políticas de segurança dos sistemas de informação.

2. Como organizações diferentes têm problemas de segurança comuns, comparar políticas de segurança dos sistemas de informação de organizações diferentes poderá ser uma boa proposta de investigação. Este trabalho permitiria avaliar diferentes políticas de segurança de forma objectiva e por outro lado, fomentar-se uma cultura global de segurança dos sistemas de informação.

3. Um dos maiores entraves à implementação e adopção de uma política de segurança poder-se-á considerar a falta de sensibilização dos dirigentes para as questões da segurança. Uma proposta de investigação é estudar a forma de sensibilizar eficazmente os gestores de topo para esta problemática.

4. Por fim, mas não menos importante, a quantificação da adopção de políticas de segurança de sistemas de informação em outro tipo de organizações tanto públicas como privadas, bem como a identificação dos factores facilitadores e inibidores da sua adopção e se há diferenciação entre empresas públicas e privadas quando a quantificação da adopção dessas políticas.

9.5 Considerações Finais

A implementação de um sistema de protecção da informação deve transpor as fronteiras da implementação de dispositivos de hardware ou software, que protegem o que está armazenado nas bases de dados e ficheiros da organização e que muitas vezes não oferecem a segurança necessária ou esperada devido a falhas de funcionamento ou de parametrização e instalação [Peltier 2002].

O elemento humano pode ser considerado o ponto fraco dentro do processo que compõe a segurança da informação. Por essa razão, para muitas organizações a SSI é um dos aspectos mais difíceis e trabalhosos da sua gestão.

Quanto às responsabilidades dos utilizadores e dos responsáveis da política de SSI, embora se elabore em relação à importância do cumprimento das políticas e aos problemas que poderão advir da sua inobservância, nas políticas analisadas não se explicita a possibilidade da organização tomar medidas face a esses incumprimentos.

Como anteriormente mencionado, o aspecto humano é o factor crítico da segurança da informação, para essa gestão ser efectiva, as organizações devem formular e implementar uma política de SSI. Nas Câmaras Municipais Portuguesas a adopção de uma política de SSI ainda não está institucionalizada.

Essa política deve incluir um conjunto de directrizes, normas e procedimentos que devem ser seguidos e que visam consciencializar e orientar os funcionários para o uso seguro das tecnologias, com a informação sobre como gerir, guardar e proteger um dos seus principais activos que é a informação.

Para uma política de SSI ser institucionalizada nas Câmaras Municipais, a existência de um modelo padrão base poderá ser um meio facilitador da institucionalização de políticas de SSI nas Câmaras Municipais.

Realizado este trabalho, conclui-se com a esperança de se ter contribuído para o enriquecimento do conhecimento no domínio dos sistemas de informação e, em particular, para o despertar e entendimento da importância das políticas de segurança dos sistemas de informação nas organizações, através dos resultados deste projecto de investigação.

Apêndice A – Municípios e Dimensão

Este apêndice inclui uma tabela que identifica os municípios pertencentes a cada Distrito, a respectiva população residente (dados que tiveram como fonte a página da Associação Nacional de Municípios Portugueses – ANMP [2007]) e a dimensão e número de eleitores por Concelho (dados originários do Secretariado Técnico dos Assuntos para o Processo Eleitoral – STAPE [2008b]).

A dimensão que tem por base o número de eleitores é definida pelas letras A, B, C e D, dependendo a sua atribuição conforme o intervalo populacional em que se enquadre. A Classe A compreende Municípios com mais de 100.000 eleitores e são consideradas "Autarquias muito grandes". A Classe B corresponde aos Municípios com a população eleitoral compreendida entre 50.000 e 100.000 e são consideradas "Autarquias grandes". Na Classe C estão os Municípios com a população eleitoral compreendida entre 10.000 a 50.000 e são denominadas "Autarquias médias". A Classe D é atribuída aos Municípios cujo número de eleitores é no máximo 10.000 e são consideradas "Autarquias pequenas".

Estes dados são referentes ao ano de 2007 e 2008, pelo facto de, na altura, terem contextuado o levantamento efectuado junto das Câmaras Municipais.

Distritos	Municípios	População Residente	Dimensão Eleitores
Aveiro (19 Municípios)	Águeda	49 691	C (41711)
	Albergaria-a-Velha	25 497	C (20224)
	Anadia	31 671	C (26786)
	Arouca	24 019	C (20417)
	Aveiro	73 626	B (62480)
	Castelo de Paiva	17 089	C (14191)
	Espinho	31 703	C (30154)
	Estarreja	28 279	C (23079)
	Ílhavo	39 247	C (30070)
	Mealhada	21 500	C (17613)
	Murtosa	9 657	D (8668)
	Oliveira de Azeméis	70 699	B (57423)
	Oliveira do Bairro	22 365	C (18038)
	Ovar	56 715	C (44787)
	Santa Maria da Feira	142 295	A (113978)
	São João da Madeira	21 538	C (19196)
	Sever do Vouga	13 186	C (11268)
	Vagos	23 205	C (17983)
	Vale de Cambra	24 761	C (21572)
Beja	Aljustrel	10 567	D (8908)

(14 Municípios)	Almodôvar	7 650	D (7306)
	Alvito	2 708	D (2113)
	Barrancos	1 825	D (1570)
	Beja	34 970	C (29694)
	Castro Verde	7 702	D (6273)
	Cuba	4 775	D (3971)
	Ferreira do Alentejo	8 505	D (7774)
	Mértola	8 712	D (7504)
	Moura	16 411	C (13695)
	Odemira	25 738	C (21746)
	Ourique	5 842	D (5146)
	Serpa	16 072	C (14054)
	Vidigueira	6 019	D (5184)
Braga (14 Municípios)	Amares	19 290	C (17299)
	Barcelos	123 831	B (98757)
	Braga	170 858	A (135872)
	Cabeceiras de Basto	17 775	C (15856)
	Celorico de Basto	20 128	C (18381)
	Esposende	34 625	C (28859)
	Fafe	53 528	C (46151)
	Guimarães	161 876	A (132027)
	Póvoa de Lanhoso	23 657	C (21022)
	Terras de Bouro	7 955	D (8081)
	Vieira do Minho	14 474	C (14326)
	Vila Nova de Famalicão	131 690	A (107525)
	Vila Verde	48 122	C (41065)
	Vizela	23 528	C (18691)
Bragança (12 Municípios)	Alfândega da Fé	5 688	D (5922)
	Bragança	34 774	C (33525)
	Carrazeda de Ansiães	7 220	D (7434)
	Freixo de Espada à Cinta	4 014	D (3824)
	Macedo de Cavaleiros	17 210	C (17673)
	Miranda do Douro	8 085	D (7955)
	Mirandela	25 780	C (23806)
	Mogadouro	10 792	C (11214)
	Moncorvo	9 920	D (9683)
	Vila Flor	7 737	D (7560)
	Vimioso	5 105	D (6060)
	Vinhais	10 051	C (11743)
Castelo Branco (11 Municípios)	Belmonte	7 662	D (6042)
	Castelo Branco	55 034	C (47478)
	Covilhã	53 501	C (48611)
	Fundão	31 297	C (28375)
	Idanha-a-Nova	10 929	C (10377)
	Oleiros	6 212	D (6552)

	Penamacôr	6 160	D (5990)
	Proença-a-Nova	9 267	D (8479)
	Sertã	16 208	C (15068)
	Vila de Rei	3 242	D (3118)
	Vila Velha de Ródão	3 802	D (3603)
Coimbra (17 Municípios)	Arganil	13 187	C (11552)
	Cantanhede	38 590	C (33197)
	Coimbra	142 408	A (122248)
	Condeixa-a-Nova	16 459	C (11381)
	Figueira da Foz	63 144	B (55475)
	Góis	4 606	D (4155)
	Lousã	17 252	C (13641)
	Mira	13 146	C (11814)
	Miranda do Corvo	13 400	C (10519)
	Montemor-o-Velho	25 084	C (21414)
	Oliveira do Hospital	21 901	C (19089)
	Pampilhosa da Serra	4 756	D (4723)
	Penacova	16 850	C (14129)
	Penela	6 421	D (5378)
	Soure	20 695	C (18028)
	Tábua	12 452	C (10291)
	Vila Nova de Poiares	7 291	D (5916)
Évora (14 Municípios)	Alandroal	6 293	D (5563)
	Arraiolos	7 382	D (6251)
	Borba	7 545	D (6510)
	Estremoz	15 064	C (13153)
	Évora	55 619	C (45900)
	Montemor-o-Novo	18 540	C (15215)
	Mora	5 470	D (5129)
	Mourão	3 348	D (2506)
	Portel	7 078	D (5976)
	Redondo	6 990	D (6158)
	Reguengos de Monsaraz	11 460	D (8980)
	Vendas Novas	11 957	C (10262)
	Viana do Alentejo	5 639	D (4749)
	Vila Viçosa	8 745	D (7423)
Faro (16 Municípios)	Albufeira	35 281	C (25207)
	Alcoutim	3 411	D (3242)
	Aljezur	5 322	D (4188)
	Castro Marim	6 495	D (5813)
	Faro	58 305	C (49901)
	Lagoa	22 658	C (15869)
	Lagos	27 041	C (20711)
	Loulé	62 295	C (48360)
	Monchique	6 441	D (5694)

	Olhão	42 272	C (32723)
	Portimão	47 189	C (39454)
	São Brás de Alportel	11 205	D (7929)
	Silves	34 909	C (27597)
	Tavira	25 105	C (21385)
	Vila do Bispo	5 381	D (4050)
	Vila Real de Santo António	18 158	C (15048)
Guarda (14 Municípios)	Aguiar da Beira	6 247	D (6084)
	Almeida	7 784	D (8343)
	Celorico da Beira	8 752	D (8441)
	Figueira de Castelo Rodrigo	6 884	D (6368)
	Fornos de Algodres	5 435	D (5246)
	Gouveia	15 792	C (15071)
	Guarda	44 149	C (37038)
	Manteigas	4 094	D (3834)
	Mêda	6 000	D (6164)
	Pinhel	10 436	C (10783)
	Sabugal	14 222	C (14724)
	Seia	27 574	C (25376)
	Trancoso	10 639	C (10310)
	Vila Nova de Foz Côa	8 249	D (8347)
Leiria (16 Municípios)	Alcobaça	55 269	C (46784)
	Alvaiázere	8 112	D (7082)
	Ansião	13 673	C (11817)
	Batalha	15 542	C (12377)
	Bombarral	13 712	C (11712)
	Caldas da Rainha	51 403	C (40221)
	Castanheira de Pera	3 464	D (3244)
	Figueiró dos Vinhos	7 080	D (6328)
	Leiria	124 701	A (100681)
	Marinha Grande	38 030	C (29701)
	Nazaré	14 904	C (13130)
	Óbidos	11 187	C (10091)
	Pedrogão Grande	4 262	D (3825)
	Peniche	28 164	C (22826)
	Pombal	58 617	C (47127)
	Porto de Mós	24 271	C (19771)
Lisboa (16 Municípios)	Alenquer	42 932	C (31570)
	Amadora	176 239	A (138568)
	Arruda dos Vinhos	11 210	D (8840)
	Azambuja	21 508	C (16749)
	Cadaval	14 385	C (12228)
	Cascais	181 444	A (147323)
	Lisboa	529 485	A (513931)
	Loures	199 231	A (156850)

	Lourinhã	24 601	C (20557)
	Mafra	62 009	C (46088)
	Odivelas	143 995	A (110144)
	Oeiras	168 475	A (136199)
	Sintra	409 482	A (265475)
	Sobral de Monte Agraço	9 789	D (7269)
	Torres Vedras	75 494	B (60658)
	Vila Franca de Xira	133 224	B (99709)
Portalegre (15 Municípios)	Alter do Chão	3 666	D (3295)
	Arronches	3 278	D (2814)
	Avis	5 197	D (4072)
	Campo Maior	8 359	D (6953)
	Castelo de Vide	3 780	D (3110)
	Crato	3 995	D (3617)
	Elvas	22 691	C (19519)
	Fronteira	3 422	D (3255)
	Gavião	4 453	D (4150)
	Marvão	3 739	D (3401)
	Monforte	3 241	D (2845)
	Nisa	8 047	D (7268)
	Ponte de Sôr	17 593	C (15122)
	Portalegre	24 756	C (21776)
	Sousel	5 579	D (4726)
Porto (18 Municípios)	Amarante	61 029	B (50157)
	Baião	21 564	C (18583)
	Felgueiras	58 553	C (45674)
	Gondomar	169 239	A (134226)
	Lousada	46 322	C (33966)
	Maia	130 254	B (98650)
	Marco de Canaveses	53 961	C (41503)
	Matosinhos	168 451	A (136043)
	Paços de Ferreira	54 801	C (41011)
	Paredes	85 428	B (66241)
	Penafiel	72 095	B (57083)
	Porto	263 131	A (227713)
	Póvoa do Varzim	65 452	B (53021)
	Santo Tirso	71 623	B (61297)
	Trofa	39 166	C (30765)
	Valongo	86 005	B (71998)
	Vila do Conde	74 391	B (61400)
	Vila Nova de Gaia	300 868	A (236429)
Santarém (21 Municípios)	Abrantes	42 436	C (36516)
	Alcanena	14 763	C (12300)
	Almeirim	22 617	C (18723)
	Alpiarça	8 198	D (6298)

	Benavente	25 837	C (19466)
	Cartaxo	24 465	C (19650)
	Chamusca	11 313	D (9527)
	Constância	3 796	D (3386)
	Coruche	20 629	C (18566)
	Entroncamento	20 065	C (16054)
	Ferreira do Zêzere	9 345	D (7931)
	Golegã	5 629	D (4691)
	Mação	7 763	D (7543)
	Ourém	49 269	C (38016)
	Rio Maior	21 621	C (17804)
	Salvaterra de Magos	20 908	C (17013)
	Santarém	64 124	B (52247)
	Sardoal	3 992	D (3649)
	Tomar	42 983	C (37824)
	Torres Novas	37 155	C (31418)
	Vila Nova da Barquinha	7 878	D (6541)
Setúbal (13 Municípios)	Alcácer do Sal	13 624	C (11829)
	Alcochete	14 966	C (11463)
	Almada	165 363	A (139166)
	Barreiros	79 012	B (70391)
	Grândola	14 454	C (12402)
	Moita	70 226	B (56295)
	Montijo	39 168	C (35703)
	Palmela	58 222	C (43339)
	Santiago do Cacém	30 203	C (25972)
	Seixal	164 715	A (116788)
	Sesimbra	44 046	C (34441)
	Setúbal	120 117	B (94161)
	Sines	13 613	C (10938)
Viana do Castelo (10 Municípios)	Arcos de Valdevez	24 635	C (25823)
	Caminha	16 926	C (15222)
	Melgaço	9 739	C (10200)
	Monção	19 842	C (19961)
	Paredes de Coura	9 409	D (9177)
	Ponte da Barca	13 026	C (12429)
	Ponte de Lima	44 609	C (38915)
	Valença	14 284	C (12876)
	Viana do Castelo	90 654	B (79392)
	Vila Nova de Cerveira	8 813	D (8218)
Vila Real (14 Municípios)	Alijó	13 942	C (13282)
	Boticas	6 116	D (6907)
	Chaves	44 186	C (42565)
	Mesão Frio	4 652	D (4497)
	Mondim de Basto	8 470	D (8137)

	Montalegre	12 150	C (14543)
	Murça	6 476	D (7024)
	Peso da Régua	17 987	C (16417)
	Ribeira de Pena	7 251	D (8118)
	Sabrosa	6 835	D (6825)
	Santa Marta de Penaguião	8 400	D (8398)
	Valpaços	19 154	C (20599)
	Vila Pouca de Aguiar	15 100	C (16503)
	Vila Real	50 499	C (44276)
Viseu (24 Municípios)	Armamar	7 318	D (6810)
	Carregal do Sal	10 411	D (9592)
	Castro Daire	16 846	C (15509)
	Cinfães	21 318	C (18388)
	Lamego	27 054	C (25673)
	Mangualde	21 158	C (19278)
	Moimenta da Beira	11 053	C (10650)
	Mortágua	10 365	D (9373)
	Nelas	14 504	C (12899)
	Oliveira de Frades	10 597	D (8921)
	Penalva do Castelo	9 019	D (8344)
	Penedono	3 378	D (3284)
	Resende	11 978	C (11218)
	Santa Comba Dão	12 393	C (11171)
	São João da Pesqueira	8 367	D (7620)
	São Pedro do Sul	19 215	C (16613)
	Sátão	13 419	C (12201)
	Sernancelhe	6 150	D (6266)
	Tabuaço	6 501	D (6196)
	Tarouca	8 303	D (7524)
	Tondela	31 026	C (28091)
	Vila Nova de Paiva	6 141	D (5606)
	Viseu	97 601	B (82843)
	Vouzela	11 807	C (10299)
R. Autónomas			
Açores (19 Municípios)	Angra do Heroísmo	35 581	C (28434)
	Calheta (Açores)	3 972	D (3533)
	Corvo	451	D (337)
	Horta	15 224	C (11450)
	Lagoa (Açores)	14 698	C (10980)
	Lajes das Flores	1 491	D (1266)
	Lajes do Pico	4 840	D (4184)
	Madalena	6 184	D (4647)
	Nordeste	5 254	D (4745)
	Ponta Delgada	65 718	B (51348)
	Povoação	6 696	D (5559)

	Praia da Vitória	20 342	C (16877)
	Ribeira Grande	29 318	C (21042)
	Santa Cruz da Graciosa	4 777	D (3790)
	Santa Cruz das Flores	2 500	D (1975)
	São Roque do Pico	3 705	D (2840)
	Velas	5 585	D (4556)
	Vila do Porto	5 511	D (4535)
	Vila Franca do Campo	11 039	D (8558)
Madeira (11 Municípios)	Calheta (Madeira)	11 856	C (11233)
	Câmara de Lobos	35 150	C (27261)
	Funchal	100 847	A (100218)
	Machico	21 321	C (19811)
	Ponta do Sol	8 189	D (8207)
	Porto Moniz	2 762	D (3141)
	Porto Santo	4 388	D (4407)
	Ribeira Brava	12 523	C (12214)
	Santa Cruz	32 696	C (31040)
	Santana	8 491	D (8657)
	São Vicente	6 063	D (6227)

Apêndice B – Normas de Segurança de Sistemas de Informação

Neste apêndice focam-se as normas de SSI geralmente conotadas com a temática da gestão da segurança da informação. Não se querendo abordar de forma exaustiva todas as normas existentes, e tendo-se presente que, por vezes, as normas diferem de país para país, listam-se neste apêndice aquelas que se julgam como as principais normas para a gestão da SSI.

Control Objectives for Information and related Technology (COBIT), publicada pelo IT Governance Institute, representa um conjunto de documentos que podem ser classificados como padrões e enquadramentos, geralmente aceites para gestão de tecnologias de informação, segurança e controlo.

ISSO/IEC 21827 – IT – Systems Security Engineering – Capability Maturity Model (SSE-CMM) é um guia para os conceitos e aplicação de um modelo para aperfeiçoar e avaliar a capacidade da engenharia de segurança.

Generally Accepted Information Security Principles (GAISP) é um conjunto de princípios de segurança que foi definido e produzido como um esforço colectivo por membros das organizações envolvidas.

The Information Security Forum's (ISF's) *Standard of Good Practice for Information Security* é um conjunto de princípios e práticas de segurança da informação.

ISO/TR 13569 *Financial Services—Information Security Guidelines*, lançado pelo International Organisation for Standardisation, é um conjunto de conceitos de segurança e objectivos de controlo sugeridos e soluções para o sector financeiro das organizações.

ISO/IEC 15408 *Security Techniques – Evaluation Criteria for IT Security* baseia-se nos *Common Criteria for Information Technology Security Evaluation 2.0* (CC). ISO/IEC 15408 é usado como referência para avaliar e certificar a segurança dos produtos e sistemas de tecnologias de informação.

The IT Infrastructure Library's (ITIL's) Security Management é um método que descreve como os processos de gestão de segurança de tecnologias de informação se ligam a outros processos de gestão de infra-estruturas de tecnologias de informação.

NIST SP 800-12 *An Introduction to Computer Security—The NIST Handbook*, lançado por US National Institute of Standards and Technology (NIST), descreve os requisitos comuns para gerir e implementar um programa de segurança informática e alguma orientação acerca dos tipos de controlos necessários.

NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* é um conjunto de princípios e práticas para estabelecer e manter a segurança de um sistema.

NIST SP 800-18 *Guide for Developing Security Plans for Information Technology Systems* fornece uma formatação e orientação para desenvolver um plano de segurança de sistema.

NIST SP 800-100 *Information Security Handbook: A Guide for Managers* cobre um vasto leque de aspectos de Segurança da Informação.

NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* fornece um conjunto de controlos de segurança básicos.

Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE) é um conjunto de princípios, atributos e resultados para avaliação de riscos.

Organisation for Economic Co-operation and Development (OECD) *Guidelines for the Security of Information Systems and Networks* fornece um conjunto de nove princípios de segurança da informação para encorajar uma "cultura de segurança".

Open Group's *Manager's Guide to Information Security* é um folheto que fornece orientação geral aos gestores de tecnologias de informação na aquisição de produtos e sistemas de tecnologias de informação.

ISO 27000 – Esta norma é composta pelo vocabulário e definições a serem utilizadas pelas restantes normas.

ISO 27001 – Esta norma define os requisitos para a implementação de um sistema de gestão de segurança da informação.

ISO 27002 – Esta norma define boas práticas para a gestão de segurança da informação.

ISO 27003 – Esta norma é um guia para a definição e implementação de um sistema de gestão de segurança da informação.

ISO 27004 – Esta norma define métricas e meios de medição para avaliar a eficácia de um sistema de gestão de segurança da informação.

ISO 27005 – Esta norma define linhas de orientação para a gestão do risco de segurança da informação.

ISO 27006 – Esta norma é um guia para o processo de acreditação de entidades certificadas.

BSI 100-1 1.5 – BSI *Standard* 100-1 *Information Security Management Systems* – Esta norma descreve como um sistema de gestão da segurança da informação pode ser concebido.

BSI 100-2 2.0 – BSI Standard 100-2: *IT-Grundschutz Methodology* – Presta assistência específica sobre a forma de introduzir um sistema de gestão da segurança da informação.

Apêndice C – Normas com Provisões sobre Políticas de SSI

Neste apêndice são apresentadas normas que directamente dizem respeito às políticas de SSI.

Para de Sá-Soares [2005, p. 21], o interesse na revisão das principais normas de segurança de sistemas de informação explica-se por se "entenderem estes documentos como prescrições extra-organizacionais para a acção das organizações e dos seus membros na área da segurança de sistemas de informação. Quanto às políticas, está subjacente um raciocínio semelhante, na medida em que são entendidas como prescrições intra-organizacionais para a acção no domínio da SSI".

Não há dúvidas que estes documentos podem ser uma boa base de trabalho a considerar na formulação e implementação de políticas de SSI, contudo é necessário ter em conta a natureza, cultura e outras variáveis da organização onde a política vai ser implementada.

Devido ao grande número de normas existentes no domínio da SSI, e dada a natureza do presente trabalho de investigação, as normas a apresentar são aquelas que directamente abordam a temática das políticas de SSI. Após a pesquisa efectuada, resultou um conjunto de seis normas principais que abordam a temática em discussão, e que se apresentam seguidamente.

COBIT 4.1

A norma COBIT, do inglês *Control Objectives for Information and Related Tecnology*, foi desenvolvida como uma norma para as boas práticas de controlo da informação, das TI e dos riscos que lhes estão associados, ou seja, é considerada um guia para a gestão das TI.

A primeira versão do COBIT remonta a 1996 e focava-se no controlo e análise dos sistemas de informação. A segunda edição surge em 1998 e passou a incluir a base de recursos mais o guia prático de implementação e execução. A edição actual, COBIT 4.1, é coordenada pelo *IT Governance Institute* e introduziu as recomendações de gestão de ambientes de TI dentro do modelo de maturidade da organização.

Esta norma difere das outras pelo facto de ter uma enorme abrangência. No que diz respeito às políticas de SSI, a sua abordagem é pouco explícita, considerando que as políticas, planos e procedimentos devem ser documentados, revistos, mantidos, aprovados, armazenados e comunicados aos colaboradores da organização, bem como podem ser utilizados para efeitos de formação dos colaboradores. Estabelece responsabilidades para cada uma destas actividades conexas àqueles documentos e, em momentos apropriados, verifica se os mesmos são executados correctamente.

Assegura que a política, planos e procedimentos são acessíveis, correctos, compreendidos pelos envolvidos e actualizados [COBIT 2007].

GAISP

A versão 3.0 da norma GAISP, do inglês *Generally Accepted Information Security Principles*, foi publicada em 2004, tendo sido elaborada pela ISSA (Information Systems Security Association) [ISSA 2004].

A norma GAISP é a sucessora da norma GASSP — *Generally Accepted System Security Principles*, que foi publicada em 1992, 1995 e 1999. A alteração do nome e consequentemente das siglas, resultou da substituição da palavra "*System*" por "*Information*", tendo assim o vocábulo informação assumido um destaque e diferenciação superiores.

Relativamente às políticas de SSI, esta norma defende que a gestão deve assegurar que as políticas, procedimentos e linhas de orientação são desenvolvidos e mantidos para envolver todos os aspectos da segurança da informação. Tal orientação deve determinar responsabilidades, o nível de discrição e da magnitude de risco que cada entidade organizacional ou individual está autorizada a assumir [ISSA 2004].

Tendo em vista assegurar que os princípios de informação sejam efectiva e uniformemente seguros, coerentes com o seu valor e os factores de risco, a gestão deve articular claramente a sua estratégia de segurança e expectativas associadas. Na falta desta clareza, alguns recursos vão ficar sem protecção, isto é, ineficazes e outros ficarão sobre-seguros de forma ineficiente [ISSA 2004].

Segundo estas normas as políticas devem reflectir a missão da organização, assim como o valor da confidencialidade, disponibilidade e integridade dos princípios da informação para a organização e outras partes relevantes. As políticas devem também reflectir alterações da missão organizacional, assim como avanços tecnológicos e outras alterações que poderiam, se não reconhecidas ou não dirigidas, comprometer a segurança da informação.

ISF - THE STANDARD OF GOOD PRACTICE FOR INFORMATION SECURITY

A norma de boas práticas para a segurança da informação foi produzida pelo Fórum de Segurança da informação (ISF), uma associação internacional com mais de 300 organizações, que fundaram e cooperam no desenvolvimento de um programa de investigação prático em segurança da informação [ISF 2007].

Esta norma apresenta no âmbito das políticas de SSI um conjunto de recomendações em relação à gestão da segurança, considerando como princípio que uma política de segurança da informação documentada e concisa deverá ser produzida e comunicada a todos os indivíduos com acesso aos sistemas de informação da empresa. O documentar de uma política "obriga", de algum modo, a gestão de topo a comprometer-se com o esforço de protecção do activo informação.

Esta norma defende a existência de uma política de segurança documentada, ratificada em todo a sua extensão, aplicada a toda a organização. Deve haver um funcionário ou grupo de funcionários responsáveis por manter a política.

A política de SSI deve exigir que:

a) A informação seja classificada de forma a indicar a sua importância na empresa.
b) Os donos (tipicamente as pessoas responsáveis pelos processos de negócio dependentes dos sistemas de informação) são nomeados para toda a informação e sistemas considerados críticos.
c) A informação e sistemas importantes sejam sujeitos regularmente a uma análise de risco da informação.
d) O pessoal seja avisado acerca da segurança da informação.
e) A organização respeite licenças de software e outras obrigações legislatórias e contratuais.
f) Sejam relatadas falhas na política de segurança da informação e suspeitas de fraquezas na segurança da informação.
g) A informação seja protegida relativamente aos seus requisitos de confidencialidade, integridade e disponibilidade.

Uma política de SSI deve ser:

a) Alinhada com outras políticas de alto nível (por exemplo, as que se relacionam com recursos humanos, finanças e tecnologias de informação).
b) Comunicada a todo o pessoal e indivíduos externos com acesso à informação ou sistemas da empresa.
c) Revista regularmente de acordo com um processo de revisão definido.
d) Revista para ter em conta a alteração de circunstâncias (por exemplo, novas ameaças, vulnerabilidades e riscos, reorganização da empresa, alterações aos requisitos contratuais legais e regulatórios, ou alterações à infra-estrutura de TI)

A política de SSI deve ainda:

a) Ser suportada por métodos que avaliam o compromisso (por exemplo, verificar se as análises de risco da informação têm sido feitas, adesão a processos de gestão de ajustamento e verificar a configuração de controlos de segurança que foram aplicados a aplicações e sistemas).
b) Estabelecer que acções disciplinares devem tomar-se contra os funcionários ou indivíduos que violaram o seu cumprimento.

Uma política de alto nível (isto é, a Política de SSI) deveria instruir os utilizadores a:

a) Encerrar os dados sensíveis ou documentação.

b) Desligar ou bloquear o sistema se um terminal ficar sem ninguém (por exemplo, durante uma reunião, almoço ou durante a noite).

Uma política de alto nível (por exemplo, a política de SSI) deveria proibir:

a) A utilização não autorizada da informação e sistemas da empresa.
b) Utilizar informação e sistemas para assuntos que não estão relacionados com o trabalho.
c) Fazer declarações ofensivas e impróprias (por exemplo, quando se utiliza o correio electrónico, mensagens instantâneas, internet ou telefone).
d) Fazer declarações obscenas, discriminatórias ou assédio.
e) O *download* de material ilegal.
f) O transporte de informação ou equipamento para fora da organização sem autorização.
g) De usar recursos de informação ou equipamentos não autorizados (por exemplo, software não autorizado de outras pessoas, *pens,* ou modems).
h) Copiar sem autorização informação ou software.
i) Comprometer *passwords* (por exemplo, escrevendo-as ou disponibilizando-as a outros)
j) Utilizar informação identificável pessoalmente a não ser que tal seja explicitamente autorizado.
k) Discutir informação relativa ao negócio em locais públicos.
l) Alterar provas no caso de incidentes de segurança de informação que possam requerer investigação forense.

NIST SP800-12 – AN INTRODUCTION TO COMPUTER SECURITY

O National Institute of Standards and Technology (NIST) é um dos órgãos norte americanos responsáveis pela emissão de normas técnicas e de testes de homologação. Dos documentos produzidos pelo NIST pode-se destacar An Introduction to Computer Security: The NIST Handbook. Este guia, além de explicar vários conceitos relacionados com segurança e os inter-relacionamentos dos controlos de segurança, ajuda o leitor a entender as necessidades de segurança e a determinar que controlos devem ser usados para alcançar o nível de protecção desejado.

A norma descreve os requisitos comuns para gerir e implementar um programa de segurança de computadores e fornece orientação acerca dos tipos de controlos necessários. No ponto das políticas de segurança, é referido que as decisões de gestão de assuntos de segurança de sistemas computacionais variam imenso. Para as distinguir entre os vários tipos de política, neste ponto são categorizadas em três tipos básicos:

- (*Program policy*) Utiliza-se a *política de programa* para criar um programa de segurança informática para uma empresa.

- (*Issue-specific policies*) As políticas de assuntos específicos dirigem-se a assuntos específicos de cada empresa.
- (*System-specific policies*) As políticas de sistemas específicos centram-se nas tomadas de decisão pela direcção para proteger um determinado sistema.

Procedimentos, padrões e linhas de orientação são utilizados para descrever como estas políticas serão implementadas dentro da empresa.

Como a política é escrita (elaborada, desenhada) a um nível geral, as organizações desenvolvem também normas, directivas e procedimentos que oferecem aos utilizadores, gestores e outros, uma abordagem mais clara para implementar a política e ir de encontro aos objectivos da empresa. As normas e directivas especificam métodos e tecnologias a serem utilizadas para tornar os sistemas seguros. Os procedimentos são passos ainda mais detalhados a ser seguidos para alcançar determinadas tarefas relacionadas com a segurança. As normas, directivas e procedimentos podem ser divulgados na empresa através de *handbooks*, regulamentos ou manuais [NIST 1995].

Algumas empresas desenvolvem manuais, regulamentos, *handbooks* ou outros documentos semelhantes sobre segurança informática. Estes podem misturar políticas, directivas, normas e procedimentos uma vez que estão intimamente relacionados. Enquanto os manuais e os regulamentos podem servir como importantes ferramentas é frequentemente útil distinguir claramente uma política da sua implementação. Isto pode ajudar a promover flexibilidade e custo efectivo oferecendo abordagens alternativas de implementação para atingir os objectivos da política [NIST 1995].

NIST SP800-100 – INFORMATION SECURITY HANDBOOK

Os relatórios do *National Institute of Standards and Technology* (NIST) dos EUA cobrem um vasto leque de aspectos de Segurança da Informação, alguns de índole geral, outros extremamente específicos e detalhados. Aquele que será agora alvo de atenção consiste num guia de gestão para a segurança da informação.

No que diz respeito às políticas de SSI, para além da sua definição, tem também indicação do que uma política deverá incluir. Nesta norma ou relatório é definido uma política de SSI como um conjunto de directivas, regras e práticas que regula a forma como uma organização gere, protege e distribui a informação [NIST 2006, 2007].

Segundo a norma, uma política de SSI é um componente essencial de gestão da SSI. Sem uma política, a gestão não tem substância nem regras para fazer cumprir.

A política de SSI de uma organização deve dirigir os fundamentos da estrutura de gestão da segurança da informação, mediante a identificação de:

- Papéis e responsabilidades no âmbito da segurança da informação;

- Definição da *baseline*[9] dos controlos de segurança e regras para exceder a *baseline*;
- Regras de comportamentos que se espera que os utilizadores da empresa sigam e as repercursões para não cumprimento.

As empresas devem assegurar que as suas políticas de SSI sejam suficientemente actuais para acomodar o ambiente de segurança da informação e a missão da empresa, bem como os requisitos operacionais. Para assegurar que os esforços de protecção da informação não se tornem obsoletos, as empresas devem implementar uma revisão da política e estabelecer um ciclo de revisão [NIST 2007].

NIST SP800-53 – RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS

A Publicação Especial 800-53, do *National Institute of Standards and Technology* (NIST), fornece uma estrutura unificada para obter segurança de informação e um sistema de análise de risco eficaz em todo o governo federal dos Estados Unidos.

No que diz respeito às políticas de segurança, este documento aborda a política de identificação e autenticação e procedimentos.

a) Uma política de identificação e autenticação formal e documentada, que refira propósitos, alcance, papéis, responsabilidades, compromisso de gestão, coordenação entre as entidades organizacionais e conformidade.

b) Procedimentos formais e documentados que facilitem a implementação da política de identificação e autenticação, bem como os controlos de identificação e autenticação que lhe estão associados.

Este controlo pretende produzir a política e os procedimentos necessários para a implementação efectiva dos controlos de segurança seleccionados e os aumentos de controlo na família da identificação e autenticação. A política e os procedimentos são coerentes com as leis federais aplicáveis, Ordens Executivas, políticas, regulamentos, normas e orientação. As políticas e os procedimentos organizacionais existentes podem tornar a necessidade de políticas específicas adicionais desnecessária. A política de identificação e autenticação pode ser incluída como parte da política geral de segurança de informação. Podem ser desenvolvidos procedimentos de identificação e autenticação para o programa de segurança geral e para um sistema de informação específico, quando necessário. A estratégia de gestão do risco organizacional é um factor chave no desenvolvimento da política de identificação e autenticação [NIST 2009].

ISO/IEC 27002

Na última década, a norma ISO/IEC 27002 assumiu-se como uma das principais normas na área da gestão da segurança da informação. A aplicação e utilização desta norma tem sido adoptada por diferentes organizações, de dimensão pequena, média e

[9] Entendida como um conjunto de controlos de segurança comummente usados, experimentados e testados por organizações bem geridas que podem ser prontamente aplicados pelas organizações [Humphreys 2000].

grande, e em inúmeros países do globo, sendo utilizada como "linguagem comum" em termos de boas práticas em segurança da informação. Em termos concretos, esta norma consiste num código de boas práticas para a implementação de um sistema de gestão da segurança da informação.

Face à relevância e impacto desta norma, providenciar-se-á de seguida uma revisão mais detalhada do seu conteúdo.

Esta norma internacional possui como pilares fundamentais dez matérias essenciais a abordar por qualquer organização que pretenda estabelecer uma postura de minimização dos riscos que pairam sobre a segurança da sua informação, nomeadamente:

1. Política de segurança - Demonstração de suporte e compromisso da gestão de topo em implementar uma gestão eficaz do risco sobre a informação de negócio. Inclui, entre outras, a abordagem da organização para as diversas práticas e posturas a tomar por todos os seus recursos humanos.

2. Organização da segurança - Existência de um fórum ou comissão de segurança da informação com a participação da gestão de topo, especialistas de segurança e responsáveis pelas diversas áreas de negócio existentes na organização para debater e planear proactivamente que acções empreender, bem como traçar as políticas de segurança a aplicar em toda a organização, definir as responsabilidades de segurança dos diversos elementos humanos e definir as condições de segurança da informação a incluir em contratos com terceiros.

3. Controlo e classificação de recursos - Existência de um sistema de gestão de inventário de recursos críticos e não críticos da organização, identificação de responsáveis para assegurar uma efectiva protecção ao longo do tempo de vida útil do recurso, entre outras matérias.

4. Segurança dos recursos humanos - Desenvolvimento de acções de formação e sensibilização para a problemática da segurança da informação para todos os recursos humanos da organização. Atribuição de responsabilidades e papéis a desempenhar por cada um dos elementos humanos face a uma situação de quebra de segurança ou catástrofe. Provisões relativas aos colaboradores da organização no período de recrutamento e selecção, emprego e terminação do vínculo contratual.

5. Segurança física e ambiental - Definição concreta e concisa do modelo de segurança física e ambiental a implementar, com base em requisitos identificados para controlo e segurança de locais e pessoas.

6. Gestão de operações e comunicações – Elaboração de um plano para o desenvolvimento de uma postura comunicativa eficaz que optimize a gestão das operações de sistemas e redes de comunicações. Definição de procedimentos de operação e de segurança dos equipamentos, gestão de alterações, segregação de ambientes de desenvolvimento e produção, planeamento e gestão de capacidades, cópias de segurança, entre outros itens.

7. Controlo de acessos - Definição de controlos que permitam assegurar que determinada informação só é acessível por aqueles que possuam as devidas credenciais.

8. Desenvolvimento e manutenção de sistemas - Assegurar que os projectos de tecnologias de informação e as actividades de suporte são conduzidos, desde o seu início, tendo em conta a segurança da informação e respeitando as políticas em vigor na organização.

9. Gestão da continuidade do negócio - Desenvolvimento de processos que permitam a gestão continuada e a melhoria contínua de planos de contingência que protejam os processos críticos do negócio contra os riscos existentes.

10. Conformidade - Capacidade de demonstração a todos os recursos humanos da organização, clientes, fornecedores e autoridades externas do compromisso relativamente ao cumprimento das normas legais e outras (internas ou externas) relacionadas com a informação.

A ISO/IEC 27002, no que diz respeito às políticas de SSI, pretende promover uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Na secção das políticas de SSI, esta norma foca dois controlos, um respeitante ao documento da política e outro à revisão da política [ISO/IEC 27002]. Esses controlos já foram abordados no Capítulo 2.

ISO/IEC 27001

A norma ISO/IEC 27001 – *Information security management systems* estabelece determinações sobre sistemas de gestão de segurança da informação. Uma das características distintivas desta norma prende-se com a possibilidade das organizações obterem a certificação dos seus sistemas de gestão de segurança da informação face ao estipulado nessa norma.

Em relação às Políticas de SSI, esta norma aponta um conjunto de objectivos de controlo e controlos relativamente às políticas de segurança, os quais são identificados na Tabela 88.

Política de Segurança	
Políticas de segurança da informação **Objectivo:** Fornecer à gestão directrizes e apoio para a segurança da informação, de acordo com os requisitos do negócio, leis e regulamentações relevantes.	
Documento da política de segurança da informação	Controlo – O documento da política de segurança da informação será aprovado pela gestão e publicado e comunicado a todos os funcionários e partes externas relevantes.
Revisão da política de segurança da informação	Controlo – A política de segurança da informação será revista em intervalos planeados ou se ocorrerem alterações significativas para assegurar que continua a servir e a ser adequada e efectiva.

Tabela 87: Norma 27001 – Objectivos do Controlo e Controlos
Adaptado de ISO/IEC [27001, 2005]

BSI 100-1 1.5 – BSI STANDARD 100-1 INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

BSI, cujas siglas correspondem a *Bundesamt für Sicherheit in der Informationstechnik*, é uma organização cuja origem se baseia na criação de normas para a padronização de processos.

Relativamente às políticas de segurança da informação, a norma BSI 100-1 1.5, intitulada *Information Security Management Systems*, aborda o tema das políticas com algum destaque.

Este documento estabelece que no processo de segurança da informação os gestores devem ter consciência de todas as condições existentes relevantes e deve especificar metas para a segurança da informação baseados nos objectivos de negócio da empresa ou no mandato da organização pública, devendo, ainda, criar os pré-requisitos necessários para a sua implementação. O procedimento é planeado em conjunto com a estratégia de segurança para estabelecer um processo contínuo de segurança de informação. A estratégia de segurança é implementada com a ajuda de um conceito de segurança e uma organização da segurança de informação [BSI 2008a].

Segundo descreve este documento, devem ser definidos objectivos da segurança de informação e devem ser estipuladas estratégias em relação à forma como os objectivos deveriam ser atingidos. As declarações nucleares são documentadas numa política de segurança de informação. Esta política deverá ser aprovada pela gestão e tornada pública na organização, devendo indicar:

- Objectivos da segurança de informação da instituição pública ou da empresa.
- Relação entre os objectivos da segurança de informação e os objectivos de negócio ou funções da instituição.
- Nível de segurança de informação pretendido.
- Documentos orientadores sobre a forma como o nível de segurança de informação deve ser atingido
- Documentos orientadores sobre se e como o nível de segurança de informação deve ser verificado

O planeamento de uma organização de segurança de informação pressupõe a especificação das estruturas organizacionais (e.g., departamentos, grupos, centros de competência), bem como a definição de papéis e deveres. Devem ser atribuídas responsabilidades na segurança de informação a um gestor do nível mais elevado da gestão, como um membro do conselho de gestão. Para além disso, deve ser nomeado um agente da segurança de informação. O agente da segurança de informação deve poder arquivar relatórios regulares e fazê-lo independentemente do nível mais elevado da gestão [BSI 2008a].

O desempenho do processo de segurança de informação deve ser revisto regularmente. Se e quando a necessidade surgir (por exemplo, se estiverem a ocorrer incidentes na segurança de informação com crescente frequência ou se houver grandes mudanças nas condições existentes), devem fazer-se reuniões entre as datas agendadas. Todos os resultados e decisões devem ser claramente documentados [BSI 2008a].

As questões seguintes, entre outras coisas, deveriam ser tidas em conta nas discussões sobre o desempenho no processo de segurança de informação:

- Houve mudança das condições existentes que resulte na necessidade de mudar o procedimento relativamente à segurança das TI?
- Os objectivos da segurança de informação ainda são adequados?
- A política de segurança de informação ainda está actualizada?

BSI 100-2 2.0 – BSI STANDARD 100-2: IT-GRUNDSCHUTZ METHODOLOGY

A BSI 100-2 2.0, intitulada *IT-Grundschutz Methodology*, aborda também a temática das políticas de segurança com algum destaque. Enquanto a BSI Standard 100-1 descreve os métodos gerais para a gestão de segurança da informação numa organização, a IT-Grundschutz Methodology presta assistência específica sobre a forma de introduzir um sistema de gestão de segurança da informação passo a passo, abordando também diferentes fases desse processo e apresenta soluções práticas e modelos (abordagens por melhores práticas), para realizar as tarefas.

A política de segurança de informação descreve, em linhas gerais, a forma como a segurança de informação deve ser estabelecida dentro da organização, para que propósitos e com que recursos e estruturas. Esse documento contém os objectivos da segurança de informação desejados pela organização e a estratégia de segurança a ser seguida. [BSI 2008b].

A política de segurança é criada de acordo com os seguintes passos [BSI 2008b]:

1 – Responsabilidade da gestão pela política de segurança
A política para a segurança da informação documenta a posição estratégica tomada pela gestão da organização a fim de atingir os objectivos de segurança de informação em todos os níveis da organização.

Já que a política de segurança representa um papel central para a segurança da informação dentro de uma organização, ela deve ser concebida de modo a que todas as unidades organizacionais se possam identificar com os seus conteúdos. Logo, deveriam estar envolvidos na sua preparação tantos departamentos quanto possíveis. Note-se, no entanto, que cada organização deve, por si própria, decidir quais os departamentos e os níveis hierárquicos que estarão envolvidos na formulação da política de segurança.

Aquando da criação da política de segurança, é recomendável o uso do domínio disponível nas seguintes unidades organizacionais: especialistas responsáveis pelas aplicações importantes, pelas operações TI e pela segurança (informação, TI, e segurança infra-estrutural); Agente de Protecção de dados; departamento de pessoal, conselho de pessoal e quadro supervisor; auditoria; representantes do departamento de finanças e departamento legal.

2 – Especificação da abrangência e dos conteúdos da política de segurança
A política de segurança de informação deve mencionar a que áreas se aplica. A abrangência pode incluir toda a organização ou apenas partes da organização. No entanto, é importante que a abrangência inclua na sua totalidade as tarefas de negócio e os processos examinados. A especificação da abrangência nem sempre é uma tarefa fácil, especialmente para grandes organizações. Pode ser útil especificar a abrangência de acordo com as áreas de responsabilidade.

A política de segurança deve ser formulada de forma clara e breve porque os documentos de política com mais de vinte páginas não têm tido sucesso na prática. O documento da política deve conter, pelo menos, a seguinte informação:

- O valor dado à segurança de informação e a importância, quer da principal informação, quer das TI para realizar as tarefas.
- A relação entre os objectivos da segurança de informação e os objectivos de negócio ou tarefas da organização.
- Os objectivos da segurança e os elementos nucleares da estratégia de segurança usada para as TI.
- Uma garantia de que a política de segurança é implementada pela gestão da organização em conjunto com declarações chave sobre o sucesso da monitorização.
- Uma descrição da estrutura organizacional estabelecida para a implementação do processo de segurança de informação.
- Por razões de motivação, algumas das principais ameaças aos processos de negócio podem ser realçadas, e as mais importantes regulamentações legais, bem como outras condições importantes (como acordos contratuais) podem ser mencionadas.
- Devem ser assinaladas as tarefas e responsabilidades chave no processo de segurança (principalmente as da equipa de gestão da SI, o Agente de Segurança das TI, os utilizadores das TI e os administradores das TI). Para além disso, também devem ser mencionadas as unidades ou papéis organizacionais que irão agir como pessoas de contacto para as questões de segurança.
- Podem também ser anunciados programas para promover a segurança de informação através de formação e actividades de consciencialização.

3 – Nomeação de uma equipa de desenvolvimento para a política de segurança
Se já existe na organização uma equipa de gestão da Segurança da Informação, então esta equipa deve ser responsável pelo desenvolvimento, pela verificação e revisão da política de segurança de informação. O documento é depois submetido à administração e gestão, respectivamente, para aprovação.

Se a equipa de gestão da segurança de informação ainda estiver a ser constituída, deve estabelecer-se um grupo de desenvolvimento para delinear a política de segurança de informação. Este grupo pode assumir a função da equipa de gestão da Segurança da Informação enquanto o processo de segurança continua. É aconselhável que este grupo de desenvolvimento inclua representantes dos utilizadores das TI, do pessoal operador das TI e um ou mais funcionários que tenham suficiente formação em segurança de informação. O ideal seria que também fosse incluído na equipa, por algum tempo, um membro da gestão que possa avaliar a importância do processamento da informação para a organização.

4 – Publicação da política de segurança

É importante que a administração ou a gestão sublinhem os seus objectivos e as suas expectativas através da publicação da política de segurança, e que realcem o valor da importância da segurança de informação em toda a organização. Por isso, todos os funcionários devem conhecer e entender os conteúdos da política de segurança. A política de segurança deve ser explicada aos novos funcionários antes que lhes seja dado acesso aos sistemas de processamento de informação.

Já que a administração é responsável em último grau pela política de segurança de informação, a política deve ser especificada por escrito. A política de segurança deve ser formalmente aprovada pela administração ou pela gestão. Os conteúdos da política de segurança devem não só ser conhecidos dentro da organização, mas também estar acessíveis tão facilmente quanto possível, como por exemplo através da Intranet da organização. Se contiverem informação confidencial, essa informação deve ser colocada num Apêndice que esteja claramente identificado como "confidencial".

5 – Actualização da política de segurança

A política para a segurança de informação deve ser verificada e actualizada em intervalos regulares. Quer devido aos rápidos desenvolvimentos no campo das TI, quer devido à situação da segurança, é recomendável que a política de segurança seja revista pelo menos cada dois anos.

As normas anteriormente apontadas contribuem para a formulação de uma política de SSI. A utilidade das normas resulta segundo de Sá-Soares [2005, p. 34], fundamentalmente, "do seu conteúdo regulador ou prescritivo ser reconhecido e aceite, de forma generalizada, pelos interessados nos assuntos versados nessas normas".

Apêndice D – Competências das Câmaras Municipais

Este apêndice inclui o Artigo 64.º da Lei n.º 169/99, de 18 de Setembro, com as alterações introduzidas pela Lei n.º 5-A/2002, de 11 de Janeiro. Esta Lei é, fundamentalmente, um diploma organizador, através do qual se estabelece o quadro de competências dos órgãos das freguesias e dos municípios com destaque, naturalmente, para a Assembleia Municipal e para a Câmara Municipal. O Artigo 64.º apresenta as competências atribuídas por esta Lei às Câmaras Municipais.

Artigo 64.º
Competências

1 — Compete à câmara municipal no âmbito da organização e funcionamento dos seus serviços e no da gestão corrente:

a) Elaborar e aprovar o regimento;

b) Executar e velar pelo cumprimento das deliberações da assembleia municipal;

c) Proceder à marcação e justificação das faltas dos seus membros;

d) Deliberar sobre a locação e aquisição de bens móveis e serviços, nos termos da lei;

e) Alienar os bens móveis que se tornem dispensáveis, nos termos da lei;

f) Adquirir e alienar ou onerar bens imóveis de valor até 1000 vezes o índice 100 das carreiras do regime geral do sistema remuneratório da função pública;

g) Alienar em hasta pública, independentemente de autorização do órgão deliberativo, bens imóveis de valor superior ao da alínea anterior, desde que a alienação decorra da execução das opções do plano e a respectiva deliberação seja aprovada por maioria de dois terços dos membros em efectividade de funções;

h) Aceitar doações, legados e heranças a benefício de inventário;

i) Nomear e exonerar o conselho de administração dos serviços municipalizados e das empresas públicas municipais, assim como os representantes do município nos órgãos de outras empresas, cooperativas, fundações ou entidades em que o mesmo detenha alguma participação no respectivo capital social ou equiparado;

j) Fixar as tarifas e os preços da prestação de serviços ao público pelos serviços municipais ou municipalizados;

l) Apoiar ou comparticipar no apoio à acção social escolar e às actividades complementares no âmbito de projectos educativos, nos termos da lei;

m) Organizar e gerir os transportes escolares;

n) Resolver, no prazo máximo de 30 dias, sobre os recursos hierárquicos impróprios que lhe sejam apresentados de todas as deliberações do conselho de administração dos serviços municipalizados;

o) Deliberar sobre a concessão de apoio financeiro, ou outro, a instituições legalmente constituídas pelos funcionários do município, tendo por objecto o desenvolvimento de actividades culturais, recreativas e desportivas;

p) Deliberar sobre a atribuição de subsídios a instituições legalmente existentes, criadas ou participadas pelo município ou criadas pelos seus funcionários, visando a concessão de benefícios sociais aos mesmos e respectivos familiares;

q) Aprovar os projectos, programas de concurso, caderno de encargos e a adjudicação relativamente a obras e aquisição de bens e serviços;

r) Dar cumprimento, no que lhe diz respeito, ao Estatuto do Direito de Oposição;

s) Deliberar sobre a administração de águas públicas sob sua jurisdição;

t) Promover a publicação de documentos, anais ou boletins que interessem à história do município;

u) Deliberar sobre o estacionamento de veículos nas ruas e demais lugares públicos;

v) Estabelecer a denominação das ruas e praças das povoações e estabelecer as regras de numeração dos edifícios;

x) Proceder à captura, alojamento e abate de canídeos e gatídeos, nos termos da legislação aplicável;

z) Deliberar sobre a deambulação e extinção de animais nocivos;

aa) Declarar prescritos a favor do município, nos termos e prazos fixados na lei geral e após publicação de avisos, os jazigos, mausoléus ou outras obras, assim como sepulturas perpétuas instaladas nos cemitérios propriedade municipal, quando não sejam conhecidos os seus proprietários ou relativamente aos quais se mostre que, após notificação judicial, se mantém desinteresse na sua conservação e manutenção, de forma inequívoca e duradoura;

bb) Remeter ao Tribunal de Contas, nos termos da lei, as contas do município.

2 — Compete à câmara municipal no âmbito do planeamento e do desenvolvimento:

a) Elaborar e submeter à aprovação da assembleia municipal os planos necessários à realização das atribuições municipais;

b) Participar, com outras entidades, no planeamento que directamente se relacione com as atribuições e competências municipais, emitindo parecer para submissão a deliberação da assembleia municipal;

c) Elaborar e submeter a aprovação da assembleia municipal as opções do plano e a proposta de orçamento e as respectivas revisões;

d) Executar as opções do plano e o orçamento aprovados;

e) Elaborar e aprovar o relatório de actividades e os documentos de prestação de contas a submeter à apreciação do órgão deliberativo;

f) Criar, construir e gerir instalações, equipamentos, serviços, redes de circulação, de transportes, de energia, de distribuição de bens e recursos físicos integrados no património municipal ou colocados, por lei, sob a administração municipal;

g) Participar em órgãos de gestão de entidades da administração central, nos casos, nos termos e para os efeitos estabelecidos por lei;

h) Colaborar no apoio a programas e projectos de interesse municipal, em parceria com outras entidades da administração central;

i) Designar os representantes do município nos conselhos locais, nos termos da lei;

j) Criar ou participar em associações de desenvolvimento regional e de desenvolvimento do meio rural;

l) Promover e apoiar o desenvolvimento de actividades artesanais, de manifestações etnográficas e a realização de eventos relacionados com a actividade económica de interesse municipal;

m) Assegurar, em parceria ou não com outras entidades públicas ou privadas, nos termos da lei, o levantamento, classificação, administração, manutenção, recuperação e divulgação do património natural, cultural, paisagístico e urbanístico do município, incluindo a construção de monumentos de interesse municipal.

3 — Compete à câmara municipal no âmbito consultivo:

a) Emitir parecer, nos casos e nos termos previstos na lei, sobre projectos de obras não sujeitas a licenciamento municipal;

b) Participar em órgãos consultivos de entidades da administração central, nos casos estabelecidos por lei.

4 — Compete à câmara municipal no âmbito do apoio a actividades de interesse municipal:

a) Deliberar sobre as formas de apoio a entidades e organismos legalmente existentes, nomeadamente com vista à prossecução de obras ou eventos de interesse municipal, bem como à informação e defesa dos direitos dos cidadãos;

b) Apoiar ou comparticipar, pelos meios adequados, no apoio a actividades de interesse municipal, de natureza social, cultural, desportiva, recreativa ou outra;

c) Participar na prestação de serviços a extratos sociais desfavorecidos ou dependentes, em parceria com as entidades competentes da administração central, e prestar apoio aos referidos extratos sociais, pelos meios adequados e nas condições constantes de regulamento municipal;

d) Deliberar em matéria de acção social escolar, designadamente no que respeita a alimentação, alojamento e atribuição de auxílios económicos a estudantes;

e) Assegurar o apoio adequado ao exercício de competências por parte do Estado, nos termos definidos por lei;

f) Deliberar sobre a participação do município em projectos e acções de cooperação descentralizada, designadamente no âmbito da União Europeia e da Comunidade de Países de Língua Portuguesa.

5 — Compete à câmara municipal, em matéria de licenciamento e fiscalização:

a) Conceder licenças nos casos e nos termos estabelecidos por lei, designadamente para construção, reedificação, utilização, conservação ou demolição de edifícios, assim como para estabelecimentos insalubres, incómodos, perigosos ou tóxicos;

b) Realizar vistorias e executar, de forma exclusiva ou participada, a actividade fiscalizadora atribuída por lei, nos termos por esta definidos;

c) Ordenar, precedendo vistoria, a demolição total ou parcial ou a beneficiação de construções que ameacem ruína ou constituam perigo para a saúde ou segurança das pessoas;

d) Emitir licenças, matrículas, livretes e transferências de propriedade e respectivos averbamentos e proceder a exames, registos e fixação de contingentes relativamente a veículos, nos casos legalmente previstos.

6 — Compete à câmara municipal, no que respeita às suas relações com outros órgãos autárquicos:

a) Apresentar à assembleia municipal propostas e pedidos de autorização, designadamente em relação às matérias constantes dos n.º 2 a 4 do artigo 53.º;

b) Deliberar sobre formas de apoio às freguesias;

c) Propor à assembleia municipal a concretização de delegação de parte das competências da câmara nas freguesias que nisso tenham interesse, de acordo com o disposto no artigo 66.º

7 — Compete ainda à câmara municipal:

a) Elaborar e aprovar posturas e regulamentos em matérias da sua competência exclusiva;

b) Administrar o domínio público municipal, nos termos da lei;

c) Propor, nos termos da lei, a declaração de utilidade pública, para efeitos de expropriação;

d) Exercer as demais competências legalmente conferidas, tendo em vista o prosseguimento normal das atribuições do município.

8 — As nomeações a que se refere a alínea *i*) do n.º 1 são feitas de entre membros da câmara municipal ou de entre cidadãos que não sejam membros dos órgãos municipais.

9 — A alienação de bens e valores artísticos do património do município é objecto de legislação especial.

Apêndice E – Fundos Municipais – Indicadores e Aplicação

Este apêndice inclui os valores do Fundo de Base Municipal (FBM), do Fundo de Coesão Municipal (FCM) e do Fundo Geral Municipal (FGM), atribuídos a cada um dos municípios, ordenados por distritos e referentes ao ano de 2006 (Total1) e os Fundos Municipais referentes ao ano de 2010 (Total2) disponíveis no portal da Associação Nacional de Municípios Portugueses.

Distrito: Aveiro

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Águeda	1 080 268	1 899 157	6 164 288	9 143 713	10 830 521
Albergaria-a-Velha	1 080 268	1 404 472	3 067 045	5 551 785	6 575 963
Anadia	1 080 268	2 798 525	3 928 791	7 807 584	9 247 905
Arouca	1 080 268	2 690 536	4 248 368	8 019 172	9 192 414
Aveiro	1 080 268	0	7 897 412	8 977 680	9 725 935
Castelo de Paiva	1 080 268	1 871 565	2 314 078	5 265 911	6 222 206
Espinho	1 080 268	359 618	4 136 869	5 576 755	6 294 396
Estarreja	1 080 268	2 102 833	3 380 577	6 563 678	7 730 501
Ílhavo	1 080 268	214 435	4 027 983	5 322 686	6 222 022
Mealhada	1 080 268	1 284 167	2 822 651	5 187 086	6 034 730
Murtosa	1 080 268	613 019	1 824 142	3 517 429	4 071 863
Oliveira de Azeméis	1 080 268	5 069 672	5 646 267	11 796 207	13 972 340
Oliveira do Bairro	1 080 268	1 657 400	3 593 913	6 331 581	7 329 596
Ovar	1 080 268	2 144 642	4 620 619	7 845 529	9 292 852
Santa Maria da Feira	1 080 268	4 771 271	10 906 306	16 757 845	19 849 286
São João da Madeira	1 080 268	0	3 094 186	4 174 454	4 711 642
Sever do Vouga	1 080 268	1 189 404	2 508 109	4 777 781	5 530 879
Vagos	1 080 268	1 860 779	2 500 302	5 441 349	6 445 153
Vale de Cambra	1 080 268	2 040 793	3 294 524	6 415 585	7 509 306

Distrito: Beja

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Aljust\rel	1 080 268	884 726	3 471 785	5 436 779	6 293 751
Almodôvar	1 080 268	950 156	5 792 096	7 822 520	9 055 544
Alvito	1 080 268	228 799	1 735 671	3 044 738	3 524 665
Barrancos	1 080 268	251 636	1 719 275	3 051 179	3 532 121
Beja	1 080 268	1 865 237	7 583 166	10 528 671	11 883 546
Castro Verde	1 080 268	763 059	3 563 547	5 406 874	6 259 133
Cuba	1 080 268	520 238	1 434 204	3 034 710	3 513 056
Ferreira do Alentejo	1 080 268	555 956	4 508 301	6 144 525	7 113 056
Mértola	1 080 268	956 968	7 979 670	10 016 906	11 595 821
Moura	1 080 268	1 290 102	6 678 905	9 049 275	10 475 667
Odemira	1 080 268	1 110 793	11 114 623	13 305 684	15 531 701
Ourique	1 080 268	463 905	4 405 750	5 949 923	6 887 780
Serpa	1 080 268	1 283 157	7 387 759	9 751 184	11 288 214
Vidigueira	1 080 268	410 926	2 414 780	3 905 974	4 521 654

Distrito: Braga

Fundos	Valores em Euros				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Amares	1 080 268	1 470 237	2 739 999	5 290 504	6 132 845
Barcelos	1 080 268	7 388 428	14 050 794	22 519 490	26 673 824
Braga	1 080 268	3 604 372	15 726 730	20 411 370	23 860 132
Cabeceiras de Basto	1 080 268	2 200 786	3 155 771	6 436 825	7 541 346
Celorico de Basto	1 080 268	2 202 992	3 786 221	7 069 481	8 327 784
Esposende	1 080 268	1 088 718	3 944 124	6 113 110	7 145 999
Fafe	1 080 268	4 266 217	6 595 032	11 941 517	13 833 768
Guimarães	1 080 268	4 217 463	17 441 453	22 739 184	26 934 047
Póvoa de Lanhoso	1 080 268	2 242 699	3 420 808	6 743 775	7 927 142
Terras de Bouro	1 080 268	957 087	3 349 434	5 386 789	6 194 058
Vieira do Minho	1 080 268	1 897 056	3 259 966	6 237 290	7 220 444
Vila Nova de Famalicão	1 080 268	5 515 648	11 600 682	18 196 598	21 553 456
Vila Verde	1 080 268	4 959 536	5 680 044	11 719 848	13 881 893
Vizela	1 080 268	1 069 117	2 385 085	4 534 470	5 370 978

Distrito: Bragança

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Alfândega da Fé	1 080 268	680 722	3 510 420	5 271 410	6 025 584
Bragança	1 080 268	899 988	11 481 514	13 461 770	15 583 682
Carrazeda de Ansiães	1 080 268	776 486	3 879 773	5 736 527	6 640 747
Freixo de Espada à Cinta	1 080 268	511 447	2 983 261	4 574 976	5 296 107
Macedo de Cavaleiros	1 080 268	1 714 940	6 713 321	9 508 529	11 007 311
Miranda do Douro	1 080 268	966 990	4 388 638	6 435 896	7 450 355
Mirandela	1 080 268	2 205 567	6 735 597	10 021 432	11 601 060
Mogadouro	1 080 268	1 368 989	6 088 230	8 537 487	9 883 208
Moncorvo	1 080 268	1 167 488	4 704 628	6 952 384	8 048 253
Vila Flor	1 080 268	776 876	3 567 435	5 424 579	6 219 162
Vimioso	1 080 268	687 350	4 021 925	5 789 543	6 702 120
Vinhais	1 080 268	1 291 822	6 198 714	8 570 804	9 873 133

Distrito: Castelo Branco

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Belmonte	1 080 268	631 063	2 069 757	3 781 088	4 269 381
Castelo Branco	1 080 268	1 944 423	13 000 807	16 025 498	18 087 729
Covilhã	1 080 268	2 756 699	7 874 321	11 711 288	13 871 755
Fundão	1 080 268	2 270 933	7 009 478	10 360 679	11 666 705
Idanha-a-Nova	1 080 268	1 279 125	8 804 544	11 163 937	12 923 653
Oleiros	1 080 268	819 423	4 093 789	5 993 480	6 871 051
Penamacôr	1 080 268	708 203	4 381 008	6 169 479	7 141 944
Proença-a-Nova	1 080 268	1 111 110	3 774 235	5 965 613	6 905 943
Sertã	1 080 268	1 975 666	4 416 586	7 472 520	8 650 376
Vila de Rei	1 080 268	313 149	2 250 923	3 644 340	4 202 068
Vila Velha de Ródão	1 080 268	393 861	2 792 898	4 267 027	4 939 617

Distrito: Coimbra

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Arganil	1 080 268	919 511	3 980 108	5 979 887	6 922 466
Cantanhede	1 080 268	2 690 985	4 974 603	8 745 856	10 124 421
Coimbra	1 080 268	0	16 697 677	17 777 945	19 551 184
Condeixa-a-Nova	1 080 268	1 094 369	1 761 191	3 935 828	4 661 898
Figueira da Foz	1 080 268	168 714	8 264 501	9 513 483	10 737 719
Góis	1 080 268	552 530	2 714 839	4 347 637	5 032 934
Lousã	1 080 268	671 931	2 569 159	4 321 358	5 002 512
Mira	1 080 268	710 871	2 240 492	4 031 631	4 775 375
Miranda do Corvo	1 080 268	1 183 393	1 759 614	4 023 275	4 719 197
Montemor-o-Velho	1 080 268	2 862 921	3 316 027	7 259 216	8 403 450
Oliveira do Hospital	1 080 268	672 972	4 936 784	6 690 024	7 744 539
Pampilhosa da Serra	1 080 268	581 126	3 866 847	5 528 241	6 399 630
Penacova	1 080 268	2 031 693	2 770 917	5 882 878	6 710 470
Penela	1 080 268	767 805	1 885 021	3 733 094	4 321 523
Soure	1 080 268	2 424 858	3 262 976	6 768 102	7 855 545
Tábua	1 080 268	1 250 155	2 970 861	5 301 284	6 136 898
Vila Nova de Poiares	1 080 268	442 818	2 058 563	3 581 649	4 146 206

Distrito: Évora

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Alandroal	1 080 268	526 624	3 794 324	5 401 216	6 252 583
Arraiolos	1 080 268	673 476	4 188 883	5 942 627	6 879 333
Borba	1 080 268	737 710	1 673 272	3 491 250	4 016 848
Estremoz	1 080 268	1 500 593	4 153 834	6 734 695	7 796 252
Évora	1 080 268	965 613	11 433 010	13 478 891	7 796 252
Montemor-o-Novo	1 080 268	975 211	7 951 431	10 006 910	11 584 250
Mora	1 080 268	481 300	2 795 015	4 356 583	5 043 290
Mourão	1 080 268	248 322	2 009 266	3 337 856	3 863 985
Portel	1 080 268	706 816	4 099 699	5 886 783	6 814 687
Redondo	1 080 268	431 235	2 949 953	4 461 456	5 164 693
Reguengos de Monsaraz	1 080 268	689 984	3 335 764	5 106 016	5 910 852
Vendas Novas	1 080 268	669 635	1 754 808	3 504 711	4 069 298
Viana do Alentejo	1 080 268	585 197	2 388 288	4 053 753	4 692 726
Vila Viçosa	1 080 268	602 222	2 145 974	3 828 464	4 431 925

Distrito: Faro

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Albufeira	1 080 268	0	6 707 815	7 788 083	4 952 965
Alcoutim	1 080 268	351 734	4 340 019	5 772 021	6 644 888
Aljezur	1 080 268	104 242	3 982 212	5 166 722	5 053 293
Castro Marim	1 080 268	126 278	3 617 479	4 824 025	3 765 309
Faro	1 080 268	0	6 258 386	7 338 654	7 731 570
Lagoa (Algarve)	1 080 268	421 595	3 712 820	5 214 683	4 247 392
Lagos	1 080 268	0	4 040 957	5 121 225	3 769 368
Loulé	1 080 268	1 165 852	8 915 530	11 161 650	9 578 452
Monchique	1 080 268	237 878	4 822 922	6 141 068	7 109 053
Olhão	1 080 268	0	5 489 990	6 570 258	7 108 648
Portimão	1 080 268	0	5 869 289	6 949 557	3 646 398
São Brás de Alportel	1 080 268	0	2 476 518	3 556 786	4 117 424
Silves	1 080 268	664 619	6 563 295	8 308 182	9 136 872
Tavira	1 080 268	477 608	5 568 865	7 126 741	7 480 272
Vila do Bispo	1 080 268	101 431	2 585 490	3 767 189	3 468 512
Vila Real de Santo António	1 080 268	0	2 937 011	4 017 279	3 272 098

Distrito: Guarda

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Aguiar da Beira	1 080 268	752 793	3 096 172	4 929 233	5 706 204
Almeida	1 080 268	866 771	5 059 628	7 006 667	8 111 093
Celorico da Beira	1 080 268	900 652	3 329 751	5 310 671	6 147 766
Figueira de Castelo Rodrigo	1 080 268	643 545	4 696 400	6 420 213	7 377 268
Fornos de Algodres	1 080 268	651 885	2 187 543	3 919 696	4 537 538
Gouveia	1 080 268	1 377 928	4 054 652	6 512 848	7 539 436
Guarda	1 080 268	2 227 344	9 563 069	12 870 681	14 899 422
Manteigas	1 080 268	421 043	2 069 397	3 570 708	4 070 497
Mêda	1 080 268	711 065	3 137 823	4 929 156	5 706 115
Pinhel	1 080 268	1 213 789	4 821 479	7 115 536	8 237 123
Sabugal	1 080 268	1 829 642	6 985 415	9 895 325	11 455 076
Seia	1 080 268	2 716 145	5 785 938	9 582 351	11 092 769
Trancoso	1 080 268	963 559	4 367 542	6 411 369	7 421 961
Vila Nova de Foz Côa	1 080 268	859 531	3 705 867	5 645 666	6 535 563

Distrito: Leiria

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Alcobaça	1 080 268	2 670 959	7 376 361	11 127 588	12 559 534
Alvaiázere	1 080 268	959 829	2 282 877	4 322 974	5 004 383
Ansião	1 080 268	1 550 331	2 131 722	4 762 321	5 640 860
Batalha	1 080 268	734 746	2 009 478	3 824 492	4 427 328
Bombarral	1 080 268	1 114 948	1 250 889	3 446 105	4 081 833
Caldas da Rainha	1 080 268	1 339 473	4 621 931	7 041 672	7 553 796
Castanheira de Pera	1 080 268	225 485	1 587 481	2 893 234	3 349 281
Figueiró dos Vinhos	1 080 268	790 247	2 395 969	4 266 484	4 938 988
Leiria	1 080 268	287 073	15 178 873	16 546 214	19 341 907
Marinha Grande	1 080 268	564 227	4 023 852	5 668 347	6 626 087
Nazaré	1 080 268	277 980	2 145 745	3 503 993	2 945 692
Óbidos	1 080 268	210 880	2 208 974	3 500 122	2 587 383
Pedrogão Grande	1 080 268	461 864	2 064 789	3 606 921	4 175 462
Peniche	1 080 268	387 028	3 103 826	4 571 122	5 205 671
Pombal	1 080 268	5 133 807	6 138 045	12 352 120	14 630 806
Porto de Mós	1 080 268	1 595 213	3 697 754	6 373 235	7 548 951

Distrito: Lisboa

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Alenquer	1 080 268	1 117 184	4 055 839	6 253 291	7 309 865
Amadora	1 080 268	2 151 935	15 862 216	19 094 419	22 320 664
Arruda dos Vinhos	1 080 268	210 547	2 154 871	3 445 686	3 889 092
Azambuja	1 080 268	149 244	3 542 344	4 771 856	5 652 155
Cadaval	1 080 268	1 033 384	2 394 261	4 507 913	5 218 473
Cascais	1 080 268	0	18 159 372	19 239 640	21 158 674
Lisboa	1 080 268	0	61 656 324	62 736 592	68 994 175
Loures	1 080 268	0	18 336 178	19 416 446	22 697 102
Lourinhã	1 080 268	660 874	2 782 058	4 523 200	5 104 993
Mafra	1 080 268	0	6 134 418	7 214 686	7 934 307
Odivelas	1 080 268	2 944 716	10 418 213	14 443 197	16 883 559
Oeiras	1 080 268	0	17 409 449	18 489 717	18 512 418
Sintra	1 080 268	4 801 369	27 193 573	33 075 210	38 663 688
Sobral de Monte Agraço	1 080 268	598 530	1 339 039	3 017 837	3 493 523
Torres Vedras	1 080 268	2 252 987	7 566 507	10 899 762	12 238 455
Vila Franca de Xira	1 080 268	0	11 772 519	12 852 787	15 024 429

Distrito: Portalegre

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Alter do Chão	1 080 268	398 969	2 469 350	3 948 587	4 570 983
Arronches	1 080 268	343 096	2 333 837	3 757 201	4 349 430
Avis	1 080 268	326 427	3 762 369	5 169 064	5 983 838
Campo Maior	1 080 268	869 400	2 243 487	4 193 155	4 804 327
Castelo de Vide	1 080 268	395 561	2 288 253	3 764 082	4 319 165
Crato	1 080 268	387 085	3 210 061	4 677 414	5 414 691
Elvas	1 080 268	1 674 809	5 242 362	7 997 439	9 258 036
Fronteira	1 080 268	286 801	1 920 911	3 287 980	3 404 828
Gavião	1 080 268	535 648	2 236 854	3 852 770	4 410 405
Marvão	1 080 268	402 793	1 834 981	3 318 042	3 841 048
Monforte	1 080 268	382 736	2 477 514	3 940 518	4 561 642
Nisa	1 080 268	800 879	4 565 261	6 446 408	7 462 522
Ponte de Sôr	1 080 268	1 303 989	5 461 807	7 846 064	9 082 799
Portalegre	1 080 268	1 268 926	5 032 611	7 381 805	8 545 362
Sousel	1 080 268	500 494	2 167 266	3 748 028	4 319 190

Distrito: Porto

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Amarante	1 080 268	6 219 674	6 080 066	13 380 008	15 481 287
Baião	1 080 268	2 772 546	3 279 988	7 132 802	8 448 641
Felgueiras	1 080 268	3 332 296	5 822 624	10 235 188	12 123 347
Gondomar	1 080 268	9 568 066	6 305 394	16 953 728	20 081 306
Lousada	1 080 268	3 025 954	4 720 143	8 826 365	10 454 628
Maia	1 080 268	0	10 455 075	11 535 343	13 484 387
Marco de Canaveses	1 080 268	5 672 607	5 490 341	12 243 216	14 501 813
Matosinhos	1 080 268	0	14 537 042	15 617 310	18 256 054
Paços de Ferreira	1 080 268	3 752 468	3 243 050	8 075 786	9 565 585
Paredes	1 080 268	2 781 432	9 826 505	13 688 205	16 213 367
Penafiel	1 080 268	5 657 148	7 499 917	14 237 333	16 863 797
Porto	1 080 268	0	25 313 589	26 393 857	29 026 479
Póvoa de Varzim	1 080 268	435 821	6 667 920	8 184 009	9 566 802
Santo Tirso	1 080 268	4 828 378	6 750 407	12 659 053	14 994 360
Trofa	1 080 268	2 023 374	3 280 843	6 384 485	7 137 547
Valongo	1 080 268	3 084 894	4 949 110	9 114 272	10 795 649
Vila do Conde	1 080 268	0	7 964 583	9 044 851	10 573 094
Vila Nova de Gaia	1 080 268	0	24 841 839	25 922 107	30 301 977

Distrito: Santarém

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Abrantes	1 080 268	2 906 511	7 153 153	11 139 932	12 787 537
Alcanena	1 080 268	673 333	2 887 316	4 640 917	5 320 009
Almeirim	1 080 268	1 579 772	2 533 515	5 193 555	6 023 819
Alpiarça	1 080 268	803 206	1 175 589	3 059 063	3 541 248
Benavente	1 080 268	0	4 073 392	5 153 660	4 874 383
Cartaxo	1 080 268	0	3 767 344	4 847 612	4 976 093
Chamusca	1 080 268	1 232 492	4 390 417	6 703 177	7 759 766
Constância	1 080 268	71 488	1 964 162	3 115 918	3 587 955
Coruche	1 080 268	1 868 792	6 963 791	9 912 851	11 475 365
Entroncamento	1 080 268	273 023	1 782 816	3 136 107	3 665 992
Ferreira do Zêzere	1 080 268	972 368	2 528 289	4 580 925	5 302 994
Golegã	1 080 268	501 950	1 350 560	2 932 778	3 368 135
Mação	1 080 268	738 789	4 216 900	6 035 957	6 987 375
Ourém	1 080 268	3 097 846	6 397 112	10 575 226	12 526 115
Rio Maior	1 080 268	1 388 744	3 390 634	5 859 646	6 783 272
Salvaterra de Magos	1 080 268	1 091 205	2 975 259	5 146 732	6 096 188
Santarém	1 080 268	1 968 224	9 277 629	12 326 121	14 359 646
Sardoal	1 080 268	431 279	1 858 040	3 369 587	3 900 717
Tomar	1 080 268	2 141 192	5 481 844	8 703 304	10 308 865
Torres Novas	1 080 268	1 318 140	5 821 667	8 220 075	9 306 598
Vila Nova da Barquinha	1 080 268	585 205	1 396 911	3 062 384	3 525 215

Distrito: Setúbal

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Alcácer do Sal	1 080 268	429 869	7 610 652	9 120 789	10 558 452
Alcochete	1 080 268	0	1 778 131	2 858 399	3 151 385
Almada	1 080 268	0	14 856 409	15 936 677	18 629 382
Barreiro	1 080 268	2 379 327	5 826 440	9 286 035	10 855 029
Grândola	1 080 268	276 001	5 219 681	6 575 950	7 349 002
Moita	1 080 268	4 262 408	4 571 815	9 914 491	11 743 489
Montijo	1 080 268	752 032	4 325 680	6 157 980	6 627 773
Palmela	1 080 268	1 084 487	6 377 546	8 542 301	8 649 757
Santiago do Cacém	1 080 268	2 147 254	7 863 316	11 090 838	12 839 031
Seixal	1 080 268	3 059 245	9 529 097	13 668 610	15 978 096
Sesimbra	1 080 268	0	3 855 415	4 935 683	5 654 342
Setúbal	1 080 268	0	10 401 865	11 482 133	13 292 005
Sines	1 080 268	0	2 700 585	3 780 853	4 313 055

Distrito: Viana do Castelo

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Arcos de Valdevez	1 080 268	2 625 122	6 605 012	10 310 402	11 812 725
Caminha	1 080 268	0	5 098 227	6 178 495	6 481 976
Melgaço	1 080 268	1 141 388	3 846 071	6 067 727	6 893 291
Monção	1 080 268	1 965 219	4 464 852	7 510 339	8 694 156
Paredes de Coura	1 080 268	1 056 467	4 029 429	6 166 164	7 092 775
Ponte da Barca	1 080 268	1 285 611	3 277 586	5 643 465	6 465 920
Ponte de Lima	1 080 268	4 114 081	6 714 794	11 909 143	13 239 780
Valença	1 080 268	662 771	3 633 545	5 376 584	6 224 068
Viana do Castelo	1 080 268	3 875 524	9 177 977	14 133 769	16 741 129
Vila Nova de Cerveira	1 080 268	420 431	4 294 378	5 795 077	6 622 558

Distrito: Vila Real

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Alijó	1 080 268	1 441 947	3 962 267	6 484 482	7 506 598
Boticas	1 080 268	787 829	3 544 273	5 412 370	6 265 495
Chaves	1 080 268	4 702 348	7 071 090	12 853 706	14 879 772
Mesão Frio	1 080 268	520 362	1 379 156	2 979 786	3 449 475
Mondim de Basto	1 080 268	1 070 532	3 175 834	5 326 634	6 166 245
Montalegre	1 080 268	1 362 986	7 216 707	9 659 961	11 185 612
Murça	1 080 268	749 602	2 513 050	4 342 920	50 274 472
Peso da Régua	1 080 268	1 963 197	2 721 787	5 765 252	6 813 221
Ribeira de Pena	1 080 268	969 174	2 768 213	4 817 655	5 577 038
Sabrosa	1 080 268	667 986	2 922 762	4 671 016	5 407 285
Santa Marta de Penaguião	1 080 268	1 090 358	1 858 331	4 028 957	4 664 021
Valpaços	1 080 268	2 254 974	5 811 224	9 146 466	10 588 177
Vila Pouca de Aguiar	1 080 268	1 900 981	4 402 264	7 383 513	8 547 339
Vila Real	1 080 268	2 959 963	6 720 661	10 760 892	12 220 287

Distrito: Viseu

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Armamar	1 080 268	790 812	2 530 965	4 402 045	5 095 917
Carregal do Sal	1 080 268	1 196 399	1 529 452	3 806 119	4 406 058
Castro Daire	1 080 268	2 063 117	4 413 700	7 557 085	8 748 270
Cinfães	1 080 268	2 802 855	3 556 009	7 439 132	8 741 848
Lamego	1 080 268	2 115 300	4 546 820	7 742 388	8 962 781
Mangualde	1 080 268	1 728 892	3 943 561	6 752 721	7 735 579
Moimenta da Beira	1 080 268	1 246 170	3 161 990	5 488 428	6 353 541
Mortágua	1 080 268	975 220	3 092 261	5 147 749	5 876 030
Nelas	1 080 268	1 101 843	2 515 021	4 697 132	5 331 041
Oliveira de Frades	1 080 268	1 076 328	2 156 877	4 313 473	4 993 384
Penalva do Castelo	1 080 268	1 147 845	2 711 691	4 939 804	5 674 240
Penedono	1 080 268	470 513	2 320 684	3 871 465	4 455 432
Resende	1 080 268	1 269 951	3 345 016	5 695 235	6 526 522
Santa Comba Dão	1 080 268	983 079	1 982 706	4 046 053	4 683 813
São João da Pesqueira	1 080 268	892 584	3 824 666	5 797 518	6 691 200
São Pedro do Sul	1 080 268	2 401 540	4 082 756	7 564 564	8 756 929
Sátão	1 080 268	1 708 969	2 567 492	5 356 729	6 201 083
Sernancelhe	1 080 268	840 742	2 925 418	4 846 428	5 610 345
Tabuaço	1 080 268	626 177	3 079 038	4 785 483	5 539 795
Tarouca	1 080 268	960 637	2 494 171	4 535 076	5 249 918
Tondela	1 080 268	3 042 720	5 479 232	9 602 220	11 115 770
Vila Nova de Paiva	1 080 268	767 181	1 919 066	3 766 515	4 360 212
Viseu	1 080 268	1 811 656	12 473 836	15 365 760	17 962 001
Vouzela	1 080 268	1 521 885	2 377 147	4 979 300	5 764 162

Região Autónoma dos Açores

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Angra do Heroísmo	1 080 268	3 285 123	5 218 648	9 584 039	11 094 723
Calheta (Açores)	1 080 268	532 181	1 662 643	3 275 092	3 791 328
Corvo	1 080 268	58 635	302 489	1 441 392	1 668 592
Horta	1 080 268	1 167 167	3 134 988	5 382 423	6 230 827
Lagoa (Açores)	1 080 268	1 183 974	2 215 362	4 479 604	5 185 701
Lajes das Flores	1 080 268	209 447	1 272 635	2 562 350	2 966 241
Lajes do Pico	1 080 268	596 287	2 069 668	3 746 223	4 336 722
Madalena	1 080 268	667 816	2 243 048	3 991 132	4 620 234
Nordeste	1 080 268	727 834	2 354 670	4 162 772	4 818 930
Ponta Delgada	1 080 268	1 782 214	11 052 847	13 915 329	16 108 733
Povoação	1 080 268	853 347	2 135 205	4 068 820	4 710 168
Praia da Vitória	1 080 268	2 518 052	2 922 137	6 520 457	7 548 244
Ribeira Grande	1 080 268	3 431 262	4 195 087	8 706 617	10 312 790
Santa Cruz da Graciosa	1 080 268	642 263	1 005 160	2 727 691	3 157 644
Santa Cruz das Flores	1 080 268	293 709	891 612	2 265 589	2 622 702
São Roque do Pico	1 080 268	396 736	1 513 465	2 990 469	3 461 842
Velas	1 080 268	574 467	2 132 750	3 787 485	4 384 487
Vila do Porto	1 080 268	706 487	1 893 445	3 680 200	4 260 292
Vila Franca do Campo	1 080 268	1 249 634	1 837 335	4 167 237	4 902 411

Região Autónoma da Madeira

Fundos	**Valores em Euros**				
Município	**FBM**	**FCM**	**FGM**	**Total1**	**Total2**
Calheta (Madeira)	1 080 268	1 259 362	3 738 305	6 077 935	7 035 970
Câmara de Lobos	1 080 268	4 201 439	1 790 304	7 072 011	8 376 636
Funchal	1 080 268	0	13 531 494	14 611 762	17 080 605
Machico	1 080 268	2 470 336	2 104 702	5 655 306	6 698 581
Ponta do Sol	1 080 268	885 495	1 492 904	3 458 667	4 096 713
Porto Moniz	1 080 268	370 200	2 083 395	3 533 863	4 090 888
Porto Santo	1 080 268	0	1 716 943	2 797 211	2 278 346
Ribeira Brava	1 080 268	1 278 162	2 035 713	4 394 143	5 204 762
Santa Cruz	1 080 268	610 636	4 264 772	5 955 676	6 961 963
Santana	1 080 268	1 116 202	3 037 321	5 233 791	6 058 768
São Vicente	1 080 268	722 058	2 275 731	4 078 057	4 720 861

Apêndice F – Inquérito

Políticas de Segurança dos Sistemas de Informação nas Câmaras Municipais em Portugal

Breve Nota Introdutória/Metodológica

A existência de Tecnologias e Sistemas de Informação cada vez mais sofisticados e modernos que facilitem a recolha, armazenamento, processamento e disseminação de informação é crucial para o bom desempenho de uma organização.

No que concerne à Administração Pública Local, os munícipes esperam das autarquias o desenvolvimento e modernização dos seus sistemas de informação, com vista à disponibilização de serviços que melhorem o seu bem estar e qualidade de vida.

A presença na Internet da totalidade das Câmaras Municipais é uma realidade desde 2004, segundo dados de um inquérito à Utilização das Tecnologias da Informação e da Comunicação nas Câmaras Municipais, promovido pelo Observatório da Sociedade da Informação e do Conhecimento e Agência para a Sociedade do Conhecimento. E quando se fala em Sistemas e Tecnologias de Informação, fala-se necessariamente de protecção de dados. Para a satisfação deste propósito, defende-se que as tecnologias e sistemas utilizados têm de transmitir confiança aos munícipes, pelo que se torna necessário considerar aspectos relacionados com a segurança da informação e dos sistemas e tecnologias que manipulam essa informação. Esta constatação levanta duas questões cuja resposta ainda não é certa:

I. Até que ponto as Câmaras Municipais se preocupam com a segurança dos seus sistemas de informação e se dispõem de sistemas de informação seguros?

II. As Câmaras Municipais têm implementadas políticas de segurança dos sistemas de informação?

É neste contexto que se enquadra o presente inquérito que pretende aferir, de uma forma clara, a realidade das Câmaras Municipais em matéria de segurança dos seus sistemas de informação e quantificar as que realmente têm políticas de segurança (incluindo-se neste conceito as políticas de privacidade) dos sistemas de informação.

Por política de segurança dos sistemas de informação entende-se documentos que orientam ou regulam as acções das pessoas ou sistemas no domínio da segurança dos sistemas de informação.

O método a aplicar é o seguinte:

Universo de referência: Câmaras Municipais (308 Câmaras)
Âmbito geográfico: Continente e Regiões Autónomas
Realização do estudo: Isabel M. Lopes
Âmbito do estudo: Doutoramento em Sistemas de Informação
Realização do trabalho de campo: Novembro de 2007
Técnica de recolha de informação: Inquérito (Via Correio Electrónico ou Via Contacto Telefónico)

Agradecendo desde já a vossa atenção solicitamos a resposta ao presente inquérito até ao dia 06-11-2007, o qual poderá ser enviado para o seguinte endereço de correio electrónico: isalopes@ipb.pt. Na eventualidade de qualquer dúvida, não hesite em contactar-me, por correio electrónico ou via telefónica (273303153).

Confidencialidade: É garantido o anonimato dos respondentes a este inquérito, bem como a confidencialidade dos dados recolhidos, servindo os mesmos apenas no âmbito deste projecto de investigação, nunca sendo mencionada nenhuma Câmara Municipal de forma isolada, uma vez que os dados serão tratados de forma agregada.

Instruções de Preenchimento: Nas perguntas fechadas, coloque um X no quadrado correspondente, ou, no caso de S/N, coloque um X sobre a resposta correcta. Nas perguntas abertas, escreva a sua resposta no espaço destinado.

Caracterização da Câmara Municipal e do Inquirido

Identificação: Câmara Municipal de
Nome do inquirido:
Cargo:
Anos de serviço nesse cargo:
Telefone:
Correio electrónico:
Data:

Questões Gerais

A Câmara possui uma política de segurança dos sistemas de informação?___S/N
(se a resposta por positiva, preencha o quadro 1 e 2, senão preencha o quadro 3).

Quadro 1

É um documento escrito?	S		
	N	Detalhe, por favor:	
O que aborda?	Tecnologia		
	Comportamentos		
	Outros		
Qual é o numero de páginas do documento?			
Quem tem conhecimento dessa política?	Executivo		
	Chefias		
	Funcionários		
	Munícipes		
Onde se encontra a política?	Em documento disponível internamente		
	Em documento interno reservado		
	Em documento disponível para o público		
	Outro		
Estão definidos os papéis e as responsabilidades?		S	N
Estão definidas as sanções para o não cumprimento da política?		S	N
Os utilizadores assinaram um termo de aceitação?		S	N

Quadro 2

Há quantos anos foi elaborada a Política de Segurança da Informação?				
Quem desencadeou o processo de formulação da política?				
Porque foi desenvolvido o processo de formulação?	Imperativo legal			
	Ordem do Executivo			
	Iniciativa dos Técnicos de Informática			
	Outro			
Quem a elaborou?	Pessoal Interno		Quem?	
	Pessoal Externo		Quem?	
	Pessoal Interno e Externo		Quem?	
Foi superiormente aprovada?	S	Qual o cargo?		
	N			
Sobre quem recaiu a responsabilidade da sua implementação?				
A Política está em vigor?			S	N
A sua implementação foi bem aceite pelos utilizadores?			S	N
Há alguém responsável pela observância ou cumprimento da política?			S	N

A Política é revista com que periodicidade?		
Existe uma única política global ou existem várias políticas parciais?		
A quem se destina ou aplica a política?	Pessoas	
	Tecnologias	
	Outro	

Quadro 3

Estão a pensar formular uma Política de Segurança da Informação?	S	Encontra-se em processo de elaboração?			S
					N
	N	A segurança da informação não é preocupação?	S	Porquê?	
			N	Porquê?	
Têm outros mecanismos de protecção da informação e dos sistemas informáticos?	S	Quais?			
	N				

Apêndice G – *CodeBook* para Análise das Entrevistas

Neste apêndice é apresentado o *CodeBook* que serviu de base para codificar as entrevistas e sua posterior análise.

Descrição dos Códigos

Código:	NOMECM
Descrição Breve:	Nome da Câmara Municipal
Descrição Completa:	Nome que descreve a Câmara Municipal
Quando usar:	Aplicar este código ao nome da Câmara Municipal a que a entrevista diz respeito. Utilizar para Câmaras pertencentes ao C1, C2, C3 e C4.
Quando não usar:	

Código:	BENEF
Descrição Breve:	Benefícios das políticas
Descrição Completa:	Benefícios (utilidade) das políticas
Quando usar:	Utilizar este código com um dos subcódigos associados (ex. BENEF.EBENEF)
Quando não usar:	

Código:	EBENEF
Descrição Breve:	Benefícios esperados com a política
Descrição Completa:	Benefícios (utilidade) esperados com a adopção da política
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código BENEF (BENEF.EBENEF). Utilizar para Câmaras pertencentes ao C3 (Q3).
Quando não usar:	

Código:	ELBENEF
Descrição Breve:	Benefícios esperados com a política pelos outros utilizadores
Descrição Completa:	Que opinião têm os outros elementos da Câmara em relação à utilidade da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código BENEF (BENEF.ELBENEF). Utilizar para Câmaras pertencentes ao C1 (Q8), C2 (Q3) e C3 (Q3).
Quando não usar:	

Código:	CBENEF
Descrição Breve:	Benefícios concretizados com a política
Descrição Completa:	Os benefícios (utilidade) esperados concretizam-se.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código BENEF (BENEF.CBENEF). Utilizar para Câmaras pertencentes ao C1 (Q9).
Quando não usar:	

Código:	DBENEF
Descrição Breve:	Diferença entre os benefícios esperados e os benefícios concretizados após a adopção/aplicação da política
Descrição Completa:	Explicações para eventuais diferenças entre os benefícios esperados e os concretizados antes e depois da aplicação da política de SSI.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código BENEF (BENEF.DBENEF). Utilizar para Câmaras pertencentes ao C1 (Q9).
Quando não usar:	

Código:	NBENEF
Descrição Breve:	Razões apontadas para não considerarem a política útil
Descrição Completa:	Razões apontadas para a não utilidade da política de SSI.
Quando usar:	Quando questionados se consideram a política útil e a resposta foi negativa. Utilizar para Câmaras pertencentes ao C4 (Q2).
Quando não usar:	

Código:	MPROT
Descrição Breve:	Mecanismos de protecção apontados para substituir as políticas
Descrição Completa:	Mecanismos de protecção apontados para substituir as políticas, nomeadamente mecanismos tecnológicos como anti-vírus, *firewall*, etc.
Quando usar:	Quando questionados sobre que mecanismos acham que podem substituir a política de SSI. Utilizar apenas em Câmaras que não têm política. Utilizar para Câmaras pertencentes ao C4 (Q3 e Q4).
Quando não usar:	

Código:	APOL
Descrição Breve:	Aprovação da política
Descrição Completa:	Aprovação da política de SSI
Quando usar:	NÃO USE ESTE CÓDIGO! Em vez disso, escolha um dos subcódigos associados.
Quando não usar:	

Código:	APSUP
Descrição Breve:	Aprovação superior da política
Descrição Completa:	Indicação de que a política vai ser superiormente aprovada.
Quando usar:	Quando respondem à questão formulada sobre se a política vai ser aprovada superiormente. Utilizar para Câmaras pertencentes ao C2 (Q14).
Quando não usar:	

Código:	APORG
Descrição Breve:	Onde vai ser aprovada a política
Descrição Completa:	Órgão ou entidade camarária que irá aprovar a política de SSI
Quando usar:	No caso em que a política será superiormente aprovada e se tenha a indicação do órgão ou entidade camarária em que tal sucederá. Utilizar para Câmaras pertencentes ao C2 (Q14).
Quando não usar:	

Código:	APPQ
Descrição Breve:	Porquê da aprovação superior da política
Descrição Completa:	O porquê da política ser superiormente aprovada
Quando usar:	Quando os entrevistados apresentam justificações para o facto da política ir ser superiormente aprovada no órgão ou entidade em causa. Este código surge na sequência de APORG. Utilizar para Câmaras pertencentes ao C2 (Q14).
Quando não usar:	

Código:	PROC
Descrição Breve:	Processo
Descrição Completa:	Forma processual como a formulação, implementação e revisão da política de SSI decorreram
Quando usar:	NÃO USE ESTE CÓDIGO! Em vez disso, escolha um dos subcódigos associados.
Quando não usar:	

Código:	FORM
Descrição Breve:	Formulação
Descrição Completa:	Aspectos relacionados com o processo de formulação da política de SSI
Quando usar:	Utilizar este código com um dos subcódigos associados (ex. PROC.FORM.CFORM).
Quando não usar:	

Código:	CFORM
Descrição Breve:	Como foi, como está a ser ou como vai ser a Formulação
Descrição Completa:	Como foi ou está a ser formulada a política de SSI.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código FORM (FORM.CFORM). Utilizar para Câmaras pertencentes ao C1 (Q1) e C2 (Q1).
Quando não usar:	

Código:	QFORM
Descrição Breve:	Quem elaborou ou está a elaborar a Política
Descrição Completa:	Quem elaborou ou está a elaborar a política de SSI.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código FORM (FORM.QFORM). Utilizar para Câmaras pertencentes ao C1 (Q2) e C2 (Q6).
Quando não usar:	

Código:	MFORM
Descrição Breve:	Métodos de Formulação
Descrição Completa:	Que métodos foram utilizados para a formulação da política de SSI.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código FORM (FORM.MFORM). Utilizar para Câmaras pertencentes ao C2 (Q8)
Quando não usar:	

Código:	PFORM
Descrição Breve:	Problemas na formulação
Descrição Completa:	Problemas experimentados na formulação da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código FORM (FORM.FFORM). Utilizar para Câmaras pertencentes ao C1 (Q7).
Quando não usar:	

Código:	SFORM
Descrição Breve:	Soluções para problemas na formulação
Descrição Completa:	Explicitações de soluções aplicadas para resolver problemas experimentados na formulação da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código FORM (FORM.SFORM). Utilizar para Câmaras pertencentes ao C1 (Q7) e C3 (Q4).
Quando não usar:	

Código:	IMPL
Descrição Breve:	Implementação
Descrição Completa:	Aspectos relacionados com a implementação da política de SSI
Quando usar:	Utilizar este código com um dos subcódigos associados (ex. PROC.IMPL.CIMPL)
Quando não usar:	

Código:	CIMP
Descrição Breve:	Como foi ou vai ser a Implementação
Descrição Completa:	Como foi ou vai ser implementada a política de SSI
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.CIMP). Utilizar para Câmaras pertencentes ao C1 (Q5) e C2 (Q2).
Quando não usar:	

Código:	PIMPL
Descrição Breve:	Problemas na implementação
Descrição Completa:	Problemas na implementação da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.PIMPL). Utilizar para Câmaras pertencentes ao C1 (Q7).
Quando não usar:	

Código:	SIMPL
Descrição Breve:	Soluções para problemas na implementação
Descrição Completa:	Explicitações para soluções aplicadas para resolver problemas experimentados na implementação da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.PIMPL). Utilizar para Câmaras pertencentes ao C1 (Q7).
Quando não usar:	

Código:	RIMPL
Descrição Breve:	Responsável pela implementação
Descrição Completa:	Responsável pela implementação da política da SSI.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.RIMPL). Utilizar para Câmaras pertencentes ao C2 (Q9).
Quando não usar:	

Código:	ROIMPL
Descrição Breve:	Responsável pela observância
Descrição Completa:	Responsável pela observância ou cumprimento da política da SSI.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.ROIMPL). Utilizar para Câmaras pertencentes ao C1 (Q15).
Quando não usar:	

Código:	CPOL
Descrição Breve:	Cumprimento da política
Descrição Completa:	Os utilizadores cumprem o descrito e recomendado na política no dia-a-dia.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.CPOL). Utilizar para Câmaras pertencentes ao C1 (Q14).
Quando não usar:	

Código:	GSPOL
Descrição Breve:	Grau de satisfação
Descrição Completa:	Grau de satisfação com a implementação da política da SSI
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.GSPOL). Utilizar para Câmaras pertencentes ao C1 (Q16).
Quando não usar:	

Código:	GSUPOL
Descrição Breve:	Grau de satisfação dos utilizadores
Descrição Completa:	Grau de satisfação dos utilizadores com a implementação da política da SSI
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.GSUPOL). Utilizar para Câmaras pertencentes ao C1 (Q16).
Quando não usar:	

Código:	LPOL
Descrição Breve:	Local
Descrição Completa:	Local onde vai ficar a política
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código IMPL (IMPL.LPOL). Utilizar para Câmaras pertencentes ao C2 (Q10).
Quando não usar:	

Código:	R E V
Descrição Breve:	Revisão
Descrição Completa:	Aspectos relacionados com a revisão da política de SSI
Quando usar:	Utilizar este código com um dos subcódigos associados (ex. PROC.REV.PREV).
Quando não usar:	

Código:	CREV
Descrição Breve:	Como foi ou vai ser feita a Revisão
Descrição Completa:	Como foi ou vai ser feita a revisão da política de SSI
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.CREV). Utilizar para Câmaras pertencentes ao C1 (Q6).
Quando não usar:	

Código:	QREV
Descrição Breve:	Quem fez ou vai fazer a revisão da Política
Descrição Completa:	Quem fez a revisão ou quem vai fazer a revisão da política de SSI.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.QREV).
Quando não usar:	

Código:	AREV
Descrição Breve:	Aprovação da revisão
Descrição Completa:	Indicação de se a revisão foi aprovada
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.AREV).
Quando não usar:	

Código:	QAREV
Descrição Breve:	Quem aprovou a revisão
Descrição Completa:	Indicação de quem aprovou a da revisão da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.QAREV).
Quando não usar:	Só utilizar quando a revisão da política foi aprovada.

Código:	TREV
Descrição Breve:	Tempos (periodicidade) das revisões
Descrição Completa:	Quando a política é revista e com que periodicidade.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.TREV).
Quando não usar:	

Código:	PNREV
Descrição Breve:	Porquê da não revisão da política
Descrição Completa:	Razões apontadas para não ser necessário rever a política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.PNREV). Utilizar para Câmaras pertencentes ao C1 (Q6).
Quando não usar:	

Código:	PREV
Descrição Breve:	Problemas na revisão
Descrição Completa:	Problemas na revisão da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.PREV). Utilizar para Câmaras pertencentes ao C1 (Q7).
Quando não usar:	

Código:	SPREV
Descrição Breve:	Soluções para problemas na revisão
Descrição Completa:	Explicitações para soluções aplicadas para resolver problemas experimentados na revisão da política.
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código REV (REV.PREV). Utilizar para Câmaras pertencentes ao C1 (Q7).
Quando não usar:	

Código:	XPROC
Descrição Breve:	Outro
Descrição Completa:	Outra componente de informação relacionada com o processo.
Quando usar:	Aplicar este código quando nenhum outro código referente a processo (PROC) se aplica.
Quando não usar:	

Código:	CONTX
Descrição Breve:	Contexto
Descrição Completa:	Factores internos ou externos que influenciam a adopção ou aplicação de uma política.
Quando usar:	NÃO USE ESTE CÓDIGO! Em vez disso, escolha um dos subcódigod associados.
Quando não usar:	

Código:	EXT
Descrição Breve:	Factores externos
Descrição Completa:	Factores económicos, políticos, legais, etc., que influenciam a adopção de políticas.
Quando usar:	Utilizar este código apenas para referências a factores externos à organização, ou seja, factores que se localizem no ambiente da organização. Utilizar este código com os subcódigos associados (ex. CONTX.EXT.ENTRV).
Quando não usar:	

Código:	INT
Descrição Breve:	Factores internos
Descrição Completa:	Factores estruturais, sociais, culturais, gestivos, etc., que influenciam a adopção ou aplicação de uma política.
Quando usar:	Utilizar este código apenas para referências a factores internos à organização, ou seja, para factores que se localizem dentro da fronteira da organização. Utilizar este código com os subcódigos associados (ex. CONTX.INT.ENTRV).
Quando não usar:	

Código:	ENTRV
Descrição Breve:	Entraves, obstáculos ou problemas
Descrição Completa:	Entraves, obstáculos ou problemas na adopção ou aplicação das políticas.
Quando usar:	Utilizar só quando nos referimos a aplicação das políticas e não quando se trata de problemas de formulação (PFORM), implementação (PIMPL) ou revisão (PREV). Utilizar no C1 (Q10 e Q11).
Quando não usar:	Não utilizar este código isoladamente, mas como sufixo do código INT ou EXT (ex.: CONTX.INT.ENTRV).

Código:	SENTRV
Descrição Breve:	Soluções para entraves, obstáculos ou problemas
Descrição Completa:	Explicitações para soluções aplicadas para resolver os entraves, obstáculos ou problemas na adopção ou aplicação das políticas.
Quando usar:	Utilizar para Câmaras pertencentes ao C1 (Q12).
Quando não usar:	Não utilizar este código isoladamente, mas como sufixo do código INT ou EXT (ex.: CONTX.INT.SENTRV).

Código:	FCRIT
Descrição Breve:	Factores críticos
Descrição Completa:	Factores que foram críticos para que tivesse sido possível iniciar-se o processo de formulação e posterior implementação da política.
Quando usar:	Utilizar para Câmaras pertencentes ao C1 (Q4) e C2 (Q5).
Quando não usar:	Não utilizar este código isoladamente, mas como sufixo do código INT ou EXT (ex.: CONTX.INT.FCRIT).

Código:	FPOL
Descrição Breve:	Falta Política
Descrição Completa:	Quem detectou a falta de uma política.
Quando usar:	Utilizar apenas para as câmaras que têm uma política, que se encontram em processo de formulação ou quando exista a intenção de adoptar uma política de SSI. Utilizar para Câmaras pertencentes ao C1 (Q3), C2 (Q4) e C3(Q2).
Quando não usar:	Não utilizar este código isoladamente, mas como sufixo do código INT ou EXT (ex.: CONTX.INT.FPOL).

Código:	FNADOP
Descrição Breve:	Factores explicativos do porquê de não ter uma política
Descrição Completa:	Factores que explicam porque é que a Câmara não tem uma política.
Quando usar:	Utilizar apenas para as Câmaras que não têm uma política de SSI. Utilizar para Câmaras pertencentes ao C3 (Q1).
Quando não usar:	Não utilizar este código isoladamente, mas como sufixo do código INT ou EXT (ex.: INT.FNADOP).

Código:	RNFPOL
Descrição Breve:	Factores explicativos do porquê de ainda não se ter iniciado o processo de formulação
Descrição Completa:	Factores que explicam porque é que a Câmara ainda não iniciou o processo de formulação da política de SSI.
Quando usar:	Utilizar apenas para as Câmaras que não têm uma política de SSI. Utilizar para Câmaras pertencentes ao C3 (Q4).
Quando não usar:	Não utilizar este código isoladamente, mas como sufixo do código INT ou EXT (ex.: CONTX.INT.RNFPOL).

Código:	RNAPOL
Descrição Breve:	Factores explicativos para não ter intenção de adoptar uma política
Descrição Completa:	Razões para não haver intenção de adoptar uma política de SSI.
Quando usar:	Utilizar apenas para as Câmaras que não têm uma política de SSI. Utilizar para Câmaras pertencentes ao C4 (Q1).
Quando não usar:	Não utilizar este código isoladamente, mas como sufixo do código INT ou EXT (ex.: CONTX.INT.RNAPOL).

Código:	FFPOLS
Descrição Breve:	Factores fundamentais para que uma política tenha sucesso
Descrição Completa:	Factores fundamentais para que uma política de SSI tenha sucesso no âmbito de uma Câmara
Quando usar:	Usar para Câmaras pertencentes ao C1 (Q17), C2 (Q15) e C3 (Q5).
Quando não usar:	

Código:	XCONTX
Descrição Breve:	Outro
Descrição Completa:	Outra informação relacionada com o contexto.
Quando usar:	Aplicar este código quando nenhum outro código existente se aplica.
Quando não usar:	

Código:	CONTEU
Descrição Breve:	Conteúdo
Descrição Completa:	O que constitui uma política de SSI
Quando usar:	NÃO USE ESTE CÓDIGO! Em vez disso, escolha um dos subcódigos associados.
Quando não usar:	

Código:	CARACT
Descrição Breve:	Características
Descrição Completa:	Características de uma política de SSI
Quando usar:	Utilizar este código com um dos subcódigos associados (ex. CONTEU.CARACT.NUMPOL).
Quando não usar:	

Código:	NUMPOL
Descrição Breve:	Número de políticas
Descrição Completa:	Existe uma única política global ou existem várias parciais
Quando usar:	Não utilizar este código isoladamente, mas como sufixo do código CARACT (ex.: CARACT.NPOL). Utilizar para Câmaras pertencentes ao C2 (Q7).
Quando não usar:	

Código:	XCARAC
Descrição Breve:	Outro
Descrição Completa:	Outra informação relacionada com o conteúdo
Quando usar:	Aplicar este código quando nenhum outro código existente se aplica.
Quando não usar:	

Código:	COMP
Descrição Breve:	Componentes
Descrição Completa:	Componentes de uma política de SSI
Quando usar:	Aglutinar este código a um dos códigos constantes do *Codebook* "Políticas" (ex. CONTEU.COMP.COMTAR). Utilizar para Câmaras pertencentes ao C2 (Q11, Q12 e Q13).
Quando não usar:	

Código:	XCONTEU
Descrição Breve:	Outro
Descrição Completa:	Outra informação relacionada com o conteúdo da política.
Quando usar:	Aplicar este código quando nenhum outro código existente se aplica.
Quando não usar:	

Código:	INTC
Descrição Breve:	Intenções
Descrição Completa:	Indicação de intenção de ter realizado ou de vir a realizar determinada acção.
Quando usar:	
Quando não usar:	

Código:	INTCIND
Descrição Breve:	Intenção Individual
Descrição Completa:	Indicação de intenção individual de ter realizado ou de vir a realizar determinada acção.
Quando usar:	Usar este código para indicações de intenções de se ter realizado ou de se vir a realizar determinada acção por uma determinada pessoa. Utilizar para Câmaras pertencentes ao C1 (Q2, Q3, Q15), C2 (Q4, Q6, Q9, Q11, Q14) e C3 (Q2).
Quando não usar:	

Código:	INTCCOL
Descrição Breve:	Intenção Colectiva
Descrição Completa:	Indicação de intenção colectiva de se ter realizado ou de se vir a realizar determinada acção
Quando usar:	Usar este código para indicações de intenções de se ter realizado ou de se vir a realizar determinada acção por um grupo de pessoas ou por uma entidade à qual não se associe uma pessoa perfeitamente determinada. Utilizar para Câmaras pertencentes ao C1 (Q2, Q3, Q15), C2 (Q4, Q6, Q9, Q11, Q14) e C3 (Q2).
Quando não usar:	

Apêndice H – Conteúdo das Políticas de SSI

Neste apêndice é apresentada a análise individual das Políticas de SSI, em termos das suas características e componentes.

1- Características das Políticas de SSI

Caso 1

No caso 1 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Regulamento Interno de Acesso à Internet e Contas de Correio Electrónico".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de cinco páginas e estrutura-se em cinco partes: "Introdução", "Responsabilidade", "Regras de Utilização do Serviço de Internet" e "Regras de Utilização do Correio Electrónico" e o Glossário.

Quem escreveu e aprovou o documento

A responsabilidade da definição deste documento é da Divisão de Informática, enquanto a aprovação é feita pelo Presidente da Câmara Municipal, conforme definido no ponto dois do documento.

Observações e omissões no texto

O documento em análise identificado como Caso 1 é escrito numa linguagem clara e fluida, são referidos alguns termos técnicos que são definidos (na própria palavra ou no glossário no final do documento), contudo verifica-se a existência de outros que mereciam ser definidos também, tais como, *Worms* e *Trojan*. O documento está devidamente estruturado, contudo omite partes comuns a políticas de SSI, conforme discutido no capítulo da revisão da literatura, nomeadamente a indicação da sua durabilidade, ou seja o prazo previsto entre as revisões do documento.

Caso 2

No caso 2 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Documento de Aceitação de Caixas de Correio Electrónico – Normas de Utilização do Correio Electrónico".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de três páginas e estrutura-se em três partes: "Introdução", "Legislação" e "Informação que chega via correio electrónico".

Quem escreveu e aprovou o documento

O documento não faz referência em parte alguma a quem o elaborou. O mesmo acontece em relação à sua aprovação.

Observações e omissões no texto

O documento identificado como Caso 2 abrange uma área muito específica que é o correio electrónico. No que diz respeito às suas características, pode ser considerado de fácil leitura e compreensão, contudo poderia em alguns pontos ser mais abrangente e focar aspectos que não foram aqui contemplados, tais como a Internet, os objectivos da política, os deveres e obrigações dos utilizadores. Da leitura do texto nota-se a omissão do preenchimento dos campos relativos à próxima revisão.

Caso 3

No caso 3 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Regulamento Interno de Utilização das Tecnologias de Informação e Comunicação".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de dezanove páginas e estrutura-se da seguinte forma: Página de rosto, Introdução, Índice, doze Capítulos com vinte e cinco Artigos e um anexo:

Capítulo I – Disposições Gerais: Artigo 1.º "Âmbito da Aplicação", Artigo 2.º "Objecto".

Capítulo II – Princípios de Actuação do Gabinete de Tecnologias de Informação e Comunicação: Artigo 3.º "Princípios do planeamento", Artigo 4.º "Princípio da coordenação", Artigo 5.º "Princípio da modernização administrativa", Artigo 6.º "Princípio da administração aberta", Artigo 7.º "Princípio da informação".

Capítulo III – Atribuição do Gabinete de Tecnologias de Informação e Comunicação: Artigo 8.º "Atribuições do gabinete de TIC".

Capítulo IV – Horário de Funcionamento: Artigo 9.º "Horário do gabinete de TIC",

Capítulo V – Formação em Ferramentas das Novas Tecnologias: Artigo 10.º "Formação".

Capítulo VI – Identificação, Aquisição, Transferência e Abate do Equipamento Informático: Artigo 11.º "Identificação dos equipamentos informáticos", Artigo 12.º

"Aquisição de equipamento informático", Artigo 13.º "Transferência do equipamento informático", Artigo 14.º "Abate do equipamento informático".

Capítulo VII – Regras e Responsabilidades do Utilizador: Artigo 15.º "Identificação do utilizador", Artigo 16.º "Organização da informação", Artigo 17.º "Assistência", Artigo 18.º "Utilização de equipamento informático".

Capítulo VIII – Regras para Impressão: Artigo 19.º "Impressão".

Capítulo IX – Regras de Utilização da Intranet/Portal: Artigo 20.º "Edição de texto", Artigo 21.º "Edição de imagens", Artigo 22.º "Área de trabalho".

Capítulo X – Regras de Utilização da Internet: Artigo 23.º "Utilização da Internet".

Capítulo XI – Regras de Utilização do Correio Electrónico: Artigo 24.º "Utilização do correio electrónico".

Capítulo XII – Excepções às Regras Apresentadas: Artigo 25.º "Excepções".

Quem escreveu e aprovou o documento

O regulamento em análise indica na página de rosto que foi elaborado pelo Gabinete de Tecnologias de Informação e Comunicação (GTIC), relativamente à sua aprovação a mesma página tem um carimbo da deliberação, que informa que foi deliberado em reunião ordinária, bem como a data dessa aprovação.

Observações e omissões no texto

A política em análise apresenta-se numa linguagem de fácil entendimento e com a sua estrutura bem definida, contudo são referidos alguns termos técnicos que mereciam ser definidos, tais como: *junk mail*, *chain letters* e *pyramid schemes*. Relativamente ao historial de revisões não é referido em parte alguma do documento. Outra omissão é o prazo previsto entre as revisões do documento.

Caso 4

No caso 4 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe D, logo, é uma Autarquia pequena.

O documento intitula-se "Normas de Utilização".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de uma página e estrutura-se em dois parágrafos e sete pontos.

Quem escreveu e aprovou o documento

O documento não faz referência em parte alguma a quem o elaborou. O mesmo acontece em relação à sua aprovação.

Observações e omissões no texto

O documento é demasiado sucinto e restrito nos aspectos abordados. Omite partes comuns a políticas de SS, o nível de abstracção é elevado e não é mencionada a sua durabilidade.

Caso 5

No caso 5 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe D, logo, é uma Autarquia pequena.

O documento intitula-se "Política de Uso de Computador, Programas de Software e Internet".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de catorze páginas e estrutura-se da seguinte forma: Página de Rosto, Índice e cinco pontos: "Introdução", "Software Protegido pelo Direito de Autor", "Segurança", "Correio Electrónico" e "Internet – Uso Aceitável".

Quem escreveu e aprovou o documento

Não é referido quem elaborou a política, contudo poderá ser entendido que foi o Gabinete de Informática Planeamento e Informação (GIPI) uma vez que é o nome que está patente em todas as folhas do documento no seu cabeçalho. O primeiro ponto do documento que corresponde à Introdução, refere no seu primeiro parágrafo que estas regras foram aprovadas pela Câmara Municipal na sua reunião ordinária. A data da aprovação nessa reunião é também indicada.

Observações e omissões no texto

A política em análise apresenta-se bem redigida, bem estruturada e numa linguagem fácil e compreensível. Relativamente ao historial de revisões, subsiste uma dúvida, na página de rosto a seguir ao nome do documento pode ler-se o seguinte: "Classificação: Normas internas – Manual de Procedimentos" "Rev. 1.1", ou seja, se é mencionada a revisão 1.1 é porque é uma revisão do documento e não um novo, contudo, isso não é claro no texto. Outra omissão é o prazo previsto entre as revisões do documento. Alguns termos utilizados no documento carecem de definição, tais como, *helpdesk*, *laptops*, *spamming*.

Caso 6

No caso 6 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Manual de Normas e Procedimentos de Segurança na Rede Informática da Câmara Municipal de …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de nove páginas e estrutura-se em doze partes: "Finalidade dos Recursos Informáticos", "Utilizadores da Rede da Câmara", "Software protegido", "Regras para utilização da Rede Interna da Câmara", "Regras para utilização do Correio Electrónico (e-mail)", "Regras para utilização da Internet" e "Atribuição exclusiva do Gabinete de Informática e Sistemas de Informação", "Atribuições dos utilizadores", "Atribuições das chefias", "Salvaguarda de ficheiros", "Penalidades" e "Responsabilidades".

Quem escreveu e aprovou o documento

Não é referido em parte nenhuma do documento quem o formulou nem por quem foi aprovado. A única referência relativamente a estes aspectos é a menção no rodapé de todas as páginas de uma data que se pressupõe ser a data de aprovação do documento.

Observações e omissões no texto

O documento em análise identificado como Caso 6 é escrito numa linguagem clara e fluida, contudo são referidos alguns termos técnicos que mereciam ser definidos, tais como, FTP, *Secure Copy*, DNS, WINS, *Gateway*, *Proxy* e tecnologias P2P. O documento está devidamente estruturado, contudo omite partes comuns a políticas de SSI, conforme discutido no capítulo da revisão da literatura, nomeadamente indicação da sua durabilidade, ou seja o prazo previsto entre as revisões do documento.

Caso 7

No caso 7 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe A, logo, é uma Autarquia muito grande.

O documento intitula-se "Regulamento Interno de Gestão e Utilização dos Meios Informáticos".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de seis páginas e estrutura-se da seguinte forma: Página de Rosto, Introdução e doze Artigos: "Competências", "Funções", "Aquisição dos Meios Informáticos", "Recepção dos Meios Informáticos", "Instalação e Utilização dos Meios Informáticos", "Requisição e Instalação de Consumíveis", "Pré-impressos e Formulários", "Funcionamento do Serviço de Informática", "Formação", "Actualizações", "Histórico do Parque Informático" e "Generalidades".

Quem escreveu e aprovou o documento

Não é referido quem elaborou a política em parte alguma do documento, o mesmo não se verifica em relação à sua aprovação, pois a página de rosto tem em rodapé o número e a data da deliberação de Câmara e a sua aprovação, com o seguinte texto: "Deliberação nº 1073/2002 (16/09/2002) – Aprovar o Regulamento Interno de Gestão e utilização dos Meios Informáticos que dada a sua extensão fica apenso à presente acta fazendo parte integrante da mesma. – Deliberação tomada por unanimidade e em minuta".

Observações e omissões no texto

A política em análise apresenta-se numa linguagem de fácil leitura e compreensão. Relativamente ao historial de revisões não é referido em parte alguma do documento. Outra omissão é o prazo previsto entre as revisões do documento.

Caso 8

No caso 8 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe D, logo, é uma Autarquia pequena.

O documento intitula-se "Normas de Utilização do Sistema de Informação do Município de …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de catorze páginas e estrutura-se da seguinte forma: Página de rosto (nota de serviço interno), nove Capítulos e Termo de Compromisso. Os nove Capítulos têm trinta e sete Artigos a eles associados:

Capítulo I – Introdução: Artigo 1.º "Fundamentos Principais".

Capítulo II – Definições: Artigo 2.º "Recursos Informáticos do M", Artigo 3.º "Autorização de Uso", Artigo 4.º "Utilizadores Autorizados".

Capítulo III – Responsabilidades Individuais: Artigo 5.º "Acesso a informação", Artigo 6.º "Propriedade Intelectual", Artigo 7.º "Utilização Ofensiva", Artigo 8.º "Situação de Ofensa", Artigo 9.º "Responsabilidade no Uso dos Recursos", Artigo 10.º "A integridade e Confiabilidade das Informações", Artigo 11.º "O Uso do Sistema".

Capítulo IV – Acesso às Instalações e Informações: Artigo 12.º "Proibição de Acesso Partilhado", Artigo 13.º "Utilizadores Não Autorizados", Artigo 14.º "Obrigatoriedade de Uso de *Password*s Seguras", Artigo 15.º "Uso Privilegiado pelos Administradores de Sistema", Artigo 16.º "Cancelamento de Acesso", Artigo 17.º "Acesso de Computadores à Rede", Artigo 18.º "Autorização de Uso de Mecanismos de Auditoria e Segurança".

Capítulo V – Acessos, Operações e Acções não Permitidas aos Utilizadores: Artigo 19.º "Descodificação e Acesso ao Controle de Informações", Artigo 20.º

"Actividades não Permitidas", Artigo 21.º "Monitorização Não Autorizada", Artigo 22.º "Uso de Informação e Materiais Protegidos por *Copyright*", Artigo 23.º "Propagandas e Campanhas Políticas", Artigo 24.º "Uso dos Recursos Informáticos em Actividades Particulares", Artigo 25.º "Uso Excessivo".

Capítulo VI – Manutenção, Controlo e Auditoria: Artigo 26.º "Controle de Acesso a Informações", Artigo 27.º "Acesso do Administrador ao Sistema", Artigo 28.º "Verificação de Uso, Inspecção de Arquivos e Auditoria", Artigo 29.º "Suspensão de Privilégios Individuais", Artigo 30.º "Possibilidade de Novo Acesso".

Capítulo VII – Responsabilidades do Administrador: Artigo 31.º "Medidas de Segurança", Artigo 32.º "Defesa de Direitos de Autor", Artigo 33.º "Deveres do Administrador de Sistemas".

Capítulo VIII – Procedimentos e Sanções: Artigo 34.º "Conhecimento e Concordância com as Normas de Utilização dos Sistemas de Informação do Município", Artigo 35.º "Responsabilidade pela Segurança e Incidentes", Artigo 36.º "Incidentes e suas Consequências", Artigo 37.º "Outros âmbitos sancionatórios".

Capítulo IX – Casos Omissos.

Quem escreveu e aprovou o documento

O documento não identifica em parte alguma do texto quem formulou as normas. Relativamente à sua aprovação, está claramente indicado na página de rosto, que corresponde a uma nota de serviço interno, que foram aprovadas em reunião ordinária do Órgão Executivo do Município e a correspondente data de aprovação. Essa referência está também em todos os rodapés do documento, que menciona o nome das normas, onde e em que data foram aprovadas.

Observações e omissões no texto

A política em análise apresenta-se bem redigido e estruturado, contudo omite partes comuns a políticas de SSI, nomeadamente indicação da sua durabilidade, ou seja, o prazo previsto entre as revisões do documento. O historial de revisões também não é referido.

Caso 9

No caso 9 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Normas Internas de Utilização dos Recursos Informáticos da Câmara Municipal do …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de oito páginas e estrutura-se em oito Capítulos e trinta e quatro Artigos:

Capítulo I – Introdução: Artigo 1.º "Objectivos", Artigo 2.º "Definições".

Capítulo II – Acesso aos Recursos Informáticos: Artigo 3.º "Utilização", Artigo 4.º "Utilizadores", Artigo 5.º "Administração do Sistema".

Capítulo III – Responsabilidades do Utilizador: Artigo 6.º "Compromisso de confidencialidade", Artigo 7.º "Acesso à informação", Artigo 8.º "Segurança no acesso", Artigo 9.º "Equipamento distribuído e privilégios associados", Artigo 10.º "Utilização ofensiva", Artigo 11.º "Utilização excessiva", Artigo 12.º "Integridade da Informação", Artigo 13.º "Responsabilidade pela informação", Artigo 14.º "Utilização de bases de dados".

Capítulo IV – Segurança e Permissões: Artigo 15.º "Acesso ao sistema e recursos informáticos", Artigo 16.º "Acesso às instalações", Artigo 17.º "Obrigatoriedade do uso de palavras passe seguras", Artigo 18.º "Ligação de equipamentos", Artigo 19.º "Acessos, operações e acções não permitidas aos utilizadores", Artigo 20.º "Propagandas e campanhas", Artigo 21.º "Actividades particulares", Artigo 22.º "Utilização abusiva", Artigo 23.º "Armazenamento de informação".

Capítulo V – Controlo e Auditoria: Artigo 24.º "Acesso do administrador", Artigo 25.º "Auditoria", Artigo 26.º "Suspensão de privilégios individuais".

Capítulo VI – Responsabilidades do Administrador: Artigo 27.º "Deveres do administrador", Artigo 28.º "Segurança dos dados", Artigo 29.º "Defesa de direitos de autor e de licenças", Artigo 30.º "Apoio ao utilizador".

Capítulo VII – Procedimentos e Sanções: Artigo 31.º "Conhecimento e concordância com as normas", Artigo 32.º "Responsabilidade pela segurança e incidentes", Artigo 33.º "Sanções".

Capítulo VIII – Casos omissos a estas normas: Artigo 34.º "Omissões".

Quem escreveu e aprovou o documento

A política de SSI aqui em análise não indica em parte alguma do texto quem o escreveu nem por quem foi aprovado.

Observações e omissões no texto

O regulamento em análise identificado como Caso 9 apresenta-se bem estruturado, contudo omite partes comuns a políticas de SSI, nomeadamente a indicação da sua durabilidade, ou seja, o prazo previsto entre as revisões do documento. O historial de revisões é igualmente omisso.

Caso 10

No caso 10 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

No caso 10 a política é composta por dois documentos, aqui designados por A e B. O documento A intitula-se "Normas Internas: Informática – Procedimentos de Aquisição, Instalação e Utilização". O Documento B tem como título "Norma Interna: Segurança Informática e dos Sistemas de Informação".

Dimensão e estrutura dos documentos

O documento A ("Procedimentos de Aquisição, Instalação e Utilização") tem a dimensão de duas páginas e estrutura-se em cinco partes: "Aquisição de equipamentos, aplicações, consumíveis", "Instalação de equipamento, aplicações", "Acessos electrónicos ao exterior", "Acesso electrónico a partir do exterior" e "Actividades de manutenção e a utilização de meios informáticos".

O documento B ("Segurança Informática e dos Sistemas de Informação") tem a dimensão de duas páginas e estrutura-se em duas partes: "Princípios fundamentais" e "Procedimentos e dispositivos operacionais".

Quem escreveu e aprovou os documentos

Em ambos os documentos não há indicação de quem os formulou. Relativamente à sua aprovação no cabeçalho dos documentos encontra-se uma tabela com vários campos, e um deles indica quem os homologou. No documento A o despacho de homologação é do Presidente da Autarquia. O documento B foi homologado pelo Chefe de Divisão de Organização e Gestão Informática.

Observações e omissões no texto

Os documentos em análise foram escritos numa linguagem clara e fluida. O documento A tem uma natureza fundamentalmente prescritiva, enquanto o documento B é basicamente descritivo, contudo são referidos alguns termos técnicos que mereciam ser definidos, ou pelo menos descritos por extenso, tais como, SMTP, FTP e Telnet. Os documentos apresentam uma estrutura simples e omitem partes comuns a políticas de SSI, conforme discutido no capítulo da revisão da literatura, nomeadamente indicação da sua durabilidade e a definição de termos técnicos. No documento B pode também apontar-se que o nível de abstracção é elevado, não abordando os assuntos de forma concreta e objectiva.

Caso 11

No caso 11 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, de uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se “Regulamento e Política de Uso de Computador, Software e Internet”.

Dimensão e estrutura do documento

O documento impresso tem a dimensão de oito páginas e estrutura-se em oito partes: página de título, página de índice, “Introdução”, “Software protegido por direitos de autor”, “Segurança”, “Correio Electrónico”, “Uso da Internet” e “Disposições finais”.

Quem escreveu e aprovou o documento

O documento não identifica claramente quem o formulou, no entanto, está sobejamente identificado quem o aprovou. No ponto referente à “Introdução” está definido de quem é a competência ao abrigo da lei que regula a aprovação deste tipo de documentos, competência delegada ao Presidente da edilidade, nessa conformidade o documento é assinado na última página pelo Presidente da Autarquia a que o documento diz respeito.

Observações e omissões no texto

O documento identificado como Caso 11 e no que respeita às suas características, pode ser considerado de fácil leitura e compreensão, focando pontos essenciais em matéria de SSI, notando-se a omissão do preenchimento dos campos relativos à próxima revisão e falta de definição de alguns termos, tais como *Freeware* e *Shareware*.

Caso 12

No caso 12 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 2, ou seja, uma Câmara que não têm implementada uma política de SSI, mas estão em processo de formulação ou adopção. Quanto à sua dimensão, esta Câmara é classificada na Classe A, logo, é uma Autarquia muito grande.

O documento intitula-se “Gestão da Segurança na óptica do utilizador”.

Dimensão e estrutura do documento

O documento impresso tem a dimensão de onze páginas e estrutura-se em oito partes: cabeçalho, “Introdução”, “Audiência”, “Segurança da Informação no Trabalho”, “Política Geral de Software”, “Computadores pessoais e portáteis”, “Políticas de Senhas” e “Correio Electrónico”.

Quem escreveu e aprovou o documento

A política de segurança em análise ainda não foi aprovada, uma vez que é uma Câmara que está no *Cluster* 2, ou seja, ainda não tem a política implementada, neste caso o processo de formulação já está concluído, falta a sua aprovação e implementação. Relativamente a quem a formulou não está referenciado em parte

alguma do documento, mas esta Câmara está no processo de certificação dos serviços e é nesse âmbito que a política foi formulada.

Observações e omissões no texto

O documento em análise, para além da identificação clara do seu propósito, de estar escrita numa linguagem clara e sucinta, e de definir termos técnicos, omite partes comuns a políticas de SSI, conforme discutido no capítulo da revisão da literatura, nomeadamente a durabilidade do mesmo.

Caso 13

No caso 13 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 2, ou seja, uma Câmara que não tem política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe A, logo, é uma Autarquia muito grande.

O documento intitula-se "Normas de Segurança dos Sistemas de Informação da Câmara Municipal de …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de oito páginas e estrutura-se em seis partes: "Segurança", "Utilização de Software", "Utilização de Hardware", "Utilização de Email", "Utilização de Internet" e "Utilização dos serviços de comunicação móveis".

Quem escreveu e aprovou o documento

O documento não identifica quem o elaborou. Como se trata de um Município que se enquadra no *Cluster 2*, a sua aprovação ainda não foi feita, contudo o documento encontra-se concluído.

Observações e omissões no texto

A política de SSI em análise está escrita numa linguagem clara e sucinta, apresentando-se devidamente estruturada. O documento omite partes comuns a políticas de SSI, nomeadamente, a definição de termos técnicos, a durabilidade do documento e, consequentemente, a referência à periodicidade das revisões do mesmo.

Caso 14

No caso 14 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 2, ou seja, uma Câmara que não tem política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe A, logo, é uma Autarquia muito grande.

O documento intitula-se "Regulamento de Utilização de Equipamento Informático".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de nove páginas e estrutura-se em onze partes: página da deliberação, página de título, "Objectivos", "Universo de Aplicação", "Elegibilidade", "Natureza da Atribuição", "Características dos Equipamentos Informáticos", "Condições de Utilização", "Custos Inerentes à Atribuição de Equipamentos Informáticos", "Aceitação formal" e "Anexo A – Regulação dos Conteúdos Aceitáveis".

Quem escreveu e aprovou o documento

O documento não identifica claramente quem formulou a política de SSI, contudo subentende-se que foi a Direcção Municipal de Tecnologias de Informação, Modernização Administrativa e Manutenção, pois é referenciada no rodapé do documento. Relativamente à aprovação da política, o texto da deliberação está escrito na primeira página do documento para ser assinado pelo Presidente de Câmara, mas o mesmo ainda não teve despacho uma vez que se trata de um Município que se enquadra no *Cluster* 2, ou seja, ainda não implementou a política.

Observações e omissões no texto

O documento omite partes comuns a políticas de SSI, conforme discutido no capítulo da revisão da literatura, uma vez que é um documento muito específico focando-se apenas nos equipamentos informáticos.

É de referir a incongruência de termos para designar a política de SSI, aparece simultaneamente como regulamento, regras e normas. Uma vez que o seu encaminhamento, nomeadamente em termos de aprovação, é diferente, deveria o documento ter uma única denominação.

O nível de abstracção desta política é baixo, explicando-se com bastante detalhe os pontos focados. A sua linguagem é bastante clara, tornando o documento de fácil leitura. O documento faz a omissão do prazo para as revisões, dizendo só que estas normas podem ser alteradas a qualquer altura.

Caso 15

No caso 15 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Normas de Segurança e Funcionamento dos Sistemas de Informação do Município de …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de vinte e seis páginas e estrutura-se da seguinte forma: Informação Interna, Página de Rosto, Índice, e nove Capítulos. Os nove Capítulos têm cinquenta e quatro pontos:

Capítulo 1 – Introdução.

Capítulo 2 – Responsabilidades do Gabinete de Gestão de Sistemas de Informação e do Pessoal de Informática.

Capítulo 3 – Instalações Físicas do Gabinete de Gestão de Sistemas de Informação: 3.1. Definição das áreas de segurança, 3.2. Responsáveis pelas áreas de segurança, 3.3. Acesso a instalações e equipamentos, 3.4. Segurança da energia, 3.5. Climatização, 3.6. Risco de incêndio, 3.7. Radiação electromagnética, 3.8. Infra-estruturas físicas, 3.9. Guarda de suportes de informação e software.

Capítulo 4 – Hardware (Suportes Físicos): 4.1. Registo do equipamento informático, 4.2. Protecção de equipamentos de comunicações, 4.3. Plano de passagem dos cabos e nós de ligação da rede, 4.4. Manutenção de equipamentos, 4.5. Computadores portáteis, 4.6. Ligação dos sistemas à energia, 4.7. Exposição dos suportes de informação aos raios solares, 4.8. Selecção de equipamento, software e consumíveis, 4.9. Equipamentos privados.

Capítulo 5 – Software de Sistema: 5.1. Instalação de software de sistema, 5.2. Utilização do software de sistema, 5.3. Acesso aos servidores da rede, 5.4. Política de *password*, 5.5. Invalidação de acesso à rede ou sistema após tentativas inválidas, 5.6. Software da base adquirido, 5.7. Instalação de software não autorizado.

Capítulo 6 – Software aplicacional: 6.1. Protecção de acessos ao software de aplicações, 6.2. Configuração dos sistemas pessoais, 6.3. Definição de privilégios de acesso às aplicações, 6.4. Criação e alteração de bases de dados, 6.5. Desenvolvimento de software aplicacional, 6.6. Vírus informáticos.

Capítulo 7 – Dados: 7.1. Recolha e alteração de dados, 7.2. Espaço nos servidores do *Data Center*, 7.3. Informação contida nos discos dos computadores pessoais, 7.4. Dados confidenciais, 7.5. Transferências de dados, 7.6. Processamento de dados nos servidores, 7.7. Transferência de dados entre organizações diferentes, 7.8. Salvaguarda e recuperação dos dados nos servidores, 7.9. Salvaguarda dos dados nos computadores pessoais, 7.10. Definição de privilégios de acesso aos dados dos servidores.

Capítulo 8 – Política de acessos: 8.1. Acessos e ligações, 8.2. Servidores de comunicações contratados.

Capítulo 9 – Utilização dos sistemas: 9.1. Responsabilidade pelos sistemas informáticos, 9.2. Dever de sigilo do pessoal de informática, 9.3. Protecção jurídica, 9.4. Incidentes e avarias, 9.5. Identificação de utilizador, 9.6. Palavras passe dos utilizadores, 9.7. Condicionamento dos acessos à rede fora das horas de trabalho, 9.8. Arranque dos computadores, 9.9. Saída das aplicações, 9.10. Encerramento e bloqueio das estações de trabalho, 9.11. *Stand-by* dos computadores portáteis.

Quem escreveu e aprovou o documento

O documento não identifica em parte alguma do texto quem formulou as normas, contudo, na informação interna aparece o envio por parte do técnico de informática de uma proposta de alteração das normas para aprovação, pelo que se pressupõe que foi ele que as elaborou. Relativamente à sua aprovação, na informação interna está

um despacho com o texto de que "Está aprovado" e a assinatura e data de aprovação. Não é legível a assinatura que deu o parecer positivo à alteração das normas.

Observações e omissões no texto

A política apresenta-se bem redigida e estruturada, contudo o seu tamanho em número de páginas excede em muito o recomendado na literatura sobre a temática. Tratando-se de uma revisão ao documento, não é mencionado o prazo previsto entre as revisões do documento, apesar de aparecer uma indicação a este respeito na Introdução que refere que "Tratando-se de uma área em constante evolução, estas normas deverão ser revistas sempre que se torne necessário".

Caso 16

No caso 16 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento não apresenta qualquer título.

Dimensão e estrutura do documento

O documento impresso tem a dimensão de uma página e estrutura-se em quatro partes. O documento tem um texto corrido sem títulos ou pontos, mas distinguem-se quatro partes diferentes.

Quem escreveu e aprovou o documento

O documento não faz referência em parte alguma a quem o elaborou. O mesmo acontece em relação à sua aprovação.

Observações e omissões no texto

O documento é demasiado sucinto e restrito nos aspectos abordados. Omite partes comuns a políticas de SSI, nomeadamente em relação a alguns termos técnicos que emprega e que deveriam estar definidos, o nível de abstracção é elevado e não é mencionada a sua durabilidade.

Caso 17

No caso 17 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe B, logo, é uma Autarquia grande.

O documento intitula-se "Regulamento Interno Sobre a Utilização dos Meios Informáticos de Comunicação e de Transmissão de Dados pelos Trabalhadores e Colaboradores do Município da …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de dez páginas e estrutura-se da seguinte forma: Preâmbulo e seis Artigos: "Âmbito", "Deveres dos Utilizadores", "Direitos dos Utilizadores", "Administradores do Sistema Informático e das Bases de Dados", "Coordenador do Gabinete de Informática e Telecomunicações" e "Entrada em Vigor".

Quem escreveu e aprovou o documento

Não é referido quem elaborou a política em parte alguma do documento, o mesmo se verifica para quem aprovou o regulamento, contudo no último artigo é mencionado quando entra em vigor, designadamente no primeiro dia útil seguinte ao da liberação de aprovação pela Câmara Municipal, pelo que o documento deverá ter sido aprovado nesse órgão.

Observações e omissões no texto

A política em análise apresenta-se numa linguagem de fácil leitura e compreensão. Relativamente ao historial de revisões não é referido em parte alguma do documento. Outra omissão é o prazo previsto entre as revisões do documento.

Caso 18

No caso 18 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe B, logo, é uma Autarquia grande.

O documento intitula-se "Norma de Controlo Interno das Aplicações e do Ambiente Informático".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de vinte páginas e estrutura-se da seguinte forma: página de título, página de índice, "Introdução" e seis Capítulos contendo cada um vários Artigos:

Capítulo I – Disposições Gerais: Artigo 1.º "Âmbito de Aplicação", Artigo 2.º "Objectivos", Artigo 3.º "Competências", Artigo 4.º "Regras básicas", Artigo 5.º "Administração de recursos".

Capítulo II – Segurança Física: Artigo 6.º "Instalações", Artigo 7.º "Manutenção do equipamento", Artigo 8.º "Contrato de manutenção", Artigo 9.º "Inventário".

Capítulo III – Aquisição "Hardware": Artigo 10.º "Aquisição".

Capítulo IV – Aquisição, Desenvolvimento e Manutenção de "Software": Artigo 11.º "Aquisição software", Artigo 12.º "Desenvolvimento de software", Artigo 13.º "Documentação de suporte", Artigo 14.º "Manutenção do software", Artigo 15.º "Segurança do software", Artigo 16.º "Reposição de cópias de segurança", Artigo 17.º "Processamentos pesados".

Capítulo V – Controlo de Acessos: Artigo 18.º "Palavra chave", Artigo 19.º "Detecção de anomalias", Artigo 20.º "Acesso à informação".

Capítulo VI – Disposições Finais: Artigo 21.º "Delegação de funções", Artigo 22.º "Alterações", Artigo 23.º "Entrada em vigor".

Quem escreveu e aprovou o documento

O documento não faz referência em parte alguma a quem o elaborou. Quanto à sua aprovação é referenciado por meio de um carimbo na página de título por quem foi aprovado que no presente caso foi em Reunião de Câmara e a data da reunião em que foi aprovado.

Observações e omissões no texto

O documento identificado como Caso 18, no que diz respeito às suas características, pode ser considerado de fácil leitura e compreensão, referindo sempre o Programa e normas a que dá cumprimento. Da leitura do texto nota-se a omissão do preenchimento dos campos relativos à próxima revisão, no texto só é referido que o documento poderá ser alterado por deliberação do Órgão Executivo sempre que as razões de eficácia, segurança ou outras o justifiquem.

Caso 19

No caso 19 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Regulamento Municipal de Informática sobre Regras de Uso dos Computadores, Programas de Software e Internet/Mail".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de quatro páginas e estrutura-se numa Introdução, dois Capítulos e sete Artigos:

Introdução – "Exposição de Motivos"

Capítulo I – Disposições Gerais: Artigo 1.º "Software protegido pelos direitos de autor", Artigo 2.º "Segurança", Artigo 3.º "Correio Electrónico", Artigo 4.º "Internet".

Capítulo II – Disposições Finais: Artigo 5.º "Dúvidas e omissões", Artigo 6.º "Responsabilidade", Artigo 7.º "Entrada em Vigor".

Quem escreveu e aprovou o documento

O documento não faz referência em parte alguma a quem o elaborou. Quanto à sua aprovação é referenciado no final do documento que foi aprovado pelo executivo em reunião de Câmara e a data da reunião ordinária em que a deliberação foi tomada.

Observações e omissões no texto

O documento identificado como Caso 19 no que diz respeito às suas características, pode ser considerado de fácil leitura e compreensão. Da leitura do texto nota-se a omissão do preenchimento dos campos relativos à próxima revisão.

Caso 20

No caso 20 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Normas de Utilização de Sistemas de Informação Municipais".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de quatro páginas e estrutura-se em seis partes: página de título com a deliberação, "Utilização do equipamento informático", "Utilização da Rede", "Utilização do Correio Electrónico", "Utilização da Internet" e "Solicitações dos utilizadores aos Serviços de Informática".

Quem escreveu e aprovou o documento

O documento em análise apresenta na página de rosto a deliberação, esta é assinada pela chefe de divisão municipal e para além da data da reunião da Câmara Municipal em que as normas foram aprovadas a deliberação tem o seguinte teor: "Normas de utilização de Sistemas de Informação – A Câmara Municipal deliberou, por unanimidade, aprovar as normas de utilização devendo ser efectuada a sua divulgação a todos os serviços e conhecimento aos funcionários utilizadores".

Relativamente aos responsáveis pela formulação e implementação da política de segurança, a sua identificação não é feita em parte alguma do documento.

Observações e omissões no texto

O documento identificado como Caso 20, no que diz respeito às suas características, pode ser considerado de fácil leitura e compreensão, contudo poderia em alguns pontos ser mais abrangente em relação aos pontos abordados. Da leitura do texto nota-se a omissão do preenchimento dos campos relativos à próxima revisão e falta de definição de alguns termos.

Caso 21

No caso 21 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, de uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe B, logo, é uma Autarquia grande.

O documento intitula-se “Manual de Normas e Procedimentos de Segurança na Rede Informática da Câmara Municipal de …”.

Dimensão e estrutura do documento

O documento impresso tem a dimensão de quatro páginas e estrutura-se em oito partes: cabeçalho do documento, “Finalidade dos Recursos Informáticos”, “Utilizadores da Internet”, “Direito à Propriedade”, “Regras para Utilização da Rede Interna da Câmara”, “Regras para Utilização do Correio Electrónico”, “Regras para Utilização da Internet” e “Penalidades”.

Quem escreveu e aprovou o documento

O documento foi escrito pelo gabinete de informática e modernização administrativa. O documento mereceu posteriormente o despacho de aprovação pelo Presidente da Câmara a que o documento diz respeito. No despacho pode ler-se o seguinte texto “Visto. Determino o estrito cumprimento deste manual de normas devido ao sistemático abuso da rede informática da Câmara Municipal de … ou por razões de distracção ou de desatenção de que é este sistema unicamente destinado ao serviço público”. Posteriormente é despachado para todos os departamentos para cumprimento com a indicação da data do despacho.

Observações e omissões no texto

O documento identificado como Caso 21 e no que respeita às suas características, pode ser considerado de fácil leitura e compreensão, apesar do não preenchimento dos campos relativos à próxima revisão e falta de definição de alguns termos, tais como: *JunkMail*; IP; DNS; WINS; *Gateway* e *Proxy*.

Caso 22

No caso 22 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe D, logo, é uma Autarquia pequena.

O documento intitula-se “Normas de Utilização de Serviços (Internet/E-mail) – Carta do Utilizador”.

Dimensão e estrutura do documento

O documento impresso tem a dimensão de cinco páginas e estrutura-se em catorze pontos: “Objecto”, “Adesão aos Serviços – Procedimentos”, “Identificação do Utilizador Registado”, “Qualidade do Utilizador”, “Regras Técnicas”, “Serviços”, “Conteúdos”, “Direitos de Propriedade Intelectual”, “Bases de Dados Constituídas Pelos Utilizadores”, “Utilização dos Serviços”, “Publicidade”, “E-Marketing e E-Commerce”, “Dados Pessoais” e “Termos de Aceitação”.

Quem escreveu e aprovou o documento

Não é referido quem elaborou a política, nem quem a aprovou, contudo na última página do documento está uma data, que se presume que seja da sua elaboração, bem como os nomes e assinaturas dos seguintes elementos: o vice-Presidente e dois elementos que assinaram pelo Sector de Informática.

Observações e omissões no texto

A política em análise apresenta-se bem redigida, bem estruturada e numa linguagem fácil e compreensível. Relativamente ao historial de revisões não é referido em parte alguma do documento, outra omissão é o prazo previsto entre as revisões do documento.

Caso 23

No caso 23 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Regulamento de Acesso e de Utilização dos Recursos Informáticos da Câmara Municipal de …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de dez páginas e estrutura-se da seguinte forma: introdução e seis artigos, designadamente "Âmbito e Aplicação", "Acesso aos Recursos e Serviços de Informática", "Propriedade, Privacidade e Confidencialidade", "Serviços e Recursos", "Ética e Regras de Utilização" e "Normas".

Quem escreveu e aprovou o documento

Não é referido quem elaborou a política em parte alguma do documento, o mesmo se verifica para quem aprovou o regulamento e em que data.

Observações e omissões no texto

A política em análise apresenta-se numa linguagem fácil, contudo a sua estrutura não está muito bem definida o que torna a leitura do documento um pouco confuso. Relativamente ao historial de revisões não é referido em parte alguma do documento. Outra omissão é o prazo previsto entre as revisões do documento, mencionando simplesmente no último parágrafo, como uma nota final o seguinte: "… está sujeito a actualizações que se consideram necessárias em conformidade com o desenvolvimento da informática da autarquia".

Caso 24

No caso 24 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 1, ou seja, uma Câmara com política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe C, logo, é uma Autarquia média.

O documento intitula-se "Manual de Normas e Procedimentos de Segurança na Rede Informática da Câmara Municipal de …".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de treze páginas e estrutura-se em seis Capítulos e vinte e cinco Artigos:

Capítulo I – Disposições Gerais: Artigo 1.º "Integração orgânica e designação", Artigo 2.º "Objecto e legislação habilitante".

Capítulo II – Estrutura e Competências: Artigo 3.º "Estrutura", Artigo 4.º "Competências", Artigo 5.º "Funções do responsável pelo Núcleo de Apoio de Informática".

Capítulo III – Identificação e solicitações ao Núcleo de Apoio de Informática: Artigo 6.º "Identificação dos utentes", Artigo 7.º "Solicitações dos utentes ao Núcleo de Apoio de Informática", Artigo 8.º "Pedidos de novos equipamentos".

Capítulo IV – Direitos, deveres e proibições: Artigo 9.º "Direitos dos utentes", Artigo 10.º "Deveres dos utentes", Artigo 11.º "Proibições relacionadas com os acessos de cada utente", Artigo 12.º "Proibições relativas aos utentes".

> Secção I – Do correio electrónico: Artigo 13.º "Condicionantes à utilização do correio electrónico", Artigo 14.º "Acesso ao serviço de correio electrónico".
> Secção II – Da utilização das aplicações Internet: Artigo 15.º "Acesso à Internet", Artigo 16.º "Condicionantes do acesso à Internet".
> Secção III – Da utilização das aplicações administrativas e outros em rede: Artigo 17.º "Acesso às aplicações administrativas e outras em rede", Artigo 18.º "Condicionantes da utilização das aplicações administrativas e outras em rede".

Capítulo V – Auditoria e regime disciplinar: Artigo 19.º "Auditoria", Artigo 20.º "Regime disciplinar".

Capítulo VI – Disposições finais: Artigo 21.º "Avaliação de desempenho do Núcleo de Apoio de Informática", Artigo 22.º "Das tarifas", Artigo 23.º "Revisão do presente regulamento", Artigo 24.º "Dúvidas e omissões", Artigo 25.º "Entrada em vigor".

Quem escreveu e aprovou o documento

O regulamento de informática aqui em análise não indica em parte alguma do texto quem o escreveu. Relativamente à sua aprovação e uma vez que está publicado em Diário da República, é indicada a data em que foi aprovado em Reunião de Câmara e

a data em que foi a votação na Assembleia Municipal. Este documento mereceu a aprovação de dois órgãos do Município e foi posteriormente tornado público através da sua publicação em Diário da República e como se trata de um regulamento, ficou em fase de apreciação pública durante trinta dias.

Observações e omissões no texto

O regulamento em análise identificado como Caso 24 está escrito com muito rigor, muito bem redigido e sempre justificado ao obrigo da lei que regula os serviços de informática e afins. O documento apresenta-se bem estruturado, contudo omite partes comuns a políticas de SSI, conforme discutido no capítulo da revisão da literatura, nomeadamente indicação da sua durabilidade, ou seja, o prazo previsto entre as revisões do documento (no texto só é referido que será revisto por iniciativa ou proposta dos órgãos municipais competentes).

Caso 25

No caso 25 é analisado um documento de uma Câmara Municipal incluída no *Cluster* 2, ou seja, uma Câmara que não tem política de segurança. Quanto à sua dimensão, esta Câmara é classificada na Classe B, logo, é uma Autarquia grande.

O documento intitula-se "Regras para Utilização dos Meios Informáticos".

Dimensão e estrutura do documento

O documento impresso tem a dimensão de três páginas e estrutura-se em seis partes: página de despacho, "Normas Gerais", "Utilizadores", "PC's", "Rede" e "Correio Electrónico".

Quem escreveu e aprovou o documento

O documento foi elaborado pela Divisão de Informática e Tecnologia e a proposta foi enviada ao Director de Administração Geral para despacho e encaminhamento para posterior aprovação. Relativamente à aprovação, uma vez que se trata de uma Autarquia incluída no Cluster 2, a política ainda não foi aprovada.

Observações e omissões no texto

O documento identificado como Caso 25, e no que respeita às suas características, pode ser considerado de fácil leitura e compreensão, apresentando-se de uma forma sucinta. Pode apontar-se como omissão o não preenchimento dos campos relativos à próxima revisão.

2- Componentes das Políticas de SSI

Caso 1

Conteúdo do documento

A primeira parte, intitulada "Introdução", destaca a Internet e o correio electrónico como ferramentas para uma eficaz execução das funções desenvolvidas pelo Município, quando utilizadas de forma apropriada. Por isso, justifica-se a necessidade de regras para que esses serviços sejam eficazes. O último parágrafo deste ponto define que o regulamento deve ser divulgado por todos os trabalhadores e colaboradores dos órgãos, serviços e organismos do Município, que tenham acesso à Internet e ao serviço de correio electrónico institucional.

A parte referente as "Responsabilidades" está dividida em três parágrafos. O primeiro define que é da responsabilidade da Divisão de Informática a definição destas regras. O segundo parágrafo diz que é da responsabilidade do presidente da Câmara Municipal a sua aprovação. O último parágrafo define que é da responsabilidade de todos os trabalhadores e colaboradores dos órgãos, serviços e organismos do Município, que tenham acesso ao serviço de Internet e correio electrónico institucional, o seu integral cumprimento.

A parte designada por "Regras de utilização do serviço de Internet" é composta por dois pontos. O primeiro, que se denomina de "Regras de utilização da Internet", define um conjunto de regras de utilização da Internet, entre elas:

- Os serviços reservam-se o direito de inspeccionar todos os ficheiros armazenados em áreas privadas da sua rede, com vista a garantir o cumprimento das normas de funcionamento;
- Não pode ser exibido, arquivado, guardado, distribuído, editado ou gravado material sexualmente explícito recorrendo à rede ou aos recursos informáticos do Município;
- A utilização de quaisquer recursos dos serviços para actividades ilegais é motivo para processo disciplinar e consequente investigação por parte das autoridades competentes;
- Nenhum funcionário pode utilizar deliberadamente as instalações e o equipamento do Município para efectuar *download* de software ilegal ou de dados ilegais;
- Nenhum funcionário pode utilizar a tecnologia de acesso à Internet do Município para propagar deliberadamente vírus, *worms*, *trojans* ou código informático malicioso.

O segundo ponto referente às regras de utilização da Internet, refere-se a "recomendações e boas práticas" e compreende um conjunto de itens, nomeadamente:

- Mensalmente, os funcionários deverão proceder à limpeza dos ficheiros temporários e *cookies* resultantes das pesquisas feitas na Internet, de forma a optimizar o desempenho do computador;
- Recomenda-se especial cuidado com a utilização de suportes amovíveis de informação, como disquetes, CDs, DVDs ou *Pen-drives;*

- Para salvaguarda da informação é aconselhável a criação de cópias de segurança, tendo em conta eventuais anomalias nos sistemas informáticos;
- Não é aconselhável desligar os equipamentos de forma abrupta, sem proceder ao correcto encerramento do sistema operativo.

A quarta parte, intitulada "Regras de utilização das contas de correio electrónico institucionais", é composta por dois pontos. O primeiro ponto, que se denomina por "Regras de utilização do Correio Electrónico", aborda aspectos como a utilização desse recurso, a qual fica sujeita às normas de utilização implementadas, nomeadamente, filtros e retenção de mensagens, podendo a qualquer momento ser impedida a sua utilização, após constatação de que essa utilização viola as normas de segurança, consome demasiados recursos ou prejudica significativamente o tempo de resposta do sistema.

O segundo ponto, denominado por "Recomendações", define um conjunto de recomendações para salvaguardar a informação emanada e recebida nos serviços e para reduzir os riscos de congestão de rede, bem como, recomendações de forma a evitar a propagação de vírus, *worms*, *trojans* ou código informático malicioso pela rede aquando da leitura do correio electrónico.

Por último o glossário define termos técnicos constantes no documento, tais como, *spam*, encriptação, *attachment*, *malware*, *cracking*.

Componentes em falta

A política de segurança que se analisa no Caso 1, no que concerne às suas componentes, apresenta uma estrutura bastante completa, mas só em relação a dois recursos (Internet e Correio Electrónico). A indicação de quem contactar em caso de dúvidas não é feita, nem é referido o responsável pela manutenção do documento.

É possível uma identificação clara dos destinatários do documento, porém, podem-se apontar outras omissões no conteúdo do documento, designadamente a do Propósito e Objectivos. Em relação aos objectivos do regulamento só são abordados muito sumariamente na "Introdução", não estando os mesmos claramente definidos. Quanto ao propósito, não se elabora sobre este ponto em qualquer parte da política.

Caso 2

Conteúdo do documento

A parte intitulada "Introdução" contém o título e subtítulo do documento, nomeadamente "Documentos de Aceitação das Caixas de Correio Electrónico" e "Normas de Utilização do Correio Electrónico". No parágrafo referente à introdução é justificado que com o advento das TI e da utilização massiva do correio electrónico na Câmara Municipal é criado um conjunto de normas com base na legislação existente que salvaguarde os pressupostos inerentes a estas tecnologias, sendo assim o acesso mais fácil e rápido à informação.

A parte intitulada "Legislação" faz referência ao Decreto-Lei n.º 135/99, focando-se na descrição dos Artigos 26.º e 39.º desse Decreto.

Relativamente ao Artigo 26.º os pontos apresentados são o 2º e o 4º, que abordam aspectos como:

- A correspondência transmitida por via electrónica tem o mesmo valor da trocada em suporte de papel devendo ser-lhe conferida, pela Administração e pelos particulares, idêntico tratamento.
- Compete ao dirigente máximo do serviço designar os funcionários responsáveis pela informação oficial do serviço ou organismo, prestada através da transmissão electrónica de dados.

Relativamente ao Artigo 39.º os pontos referenciados são o 1º e 2º, que abordam os seguintes aspectos:

- Toda a correspondência, designadamente sugestões, críticas ou pedidos de informação cujos autores se identifiquem, dirigida a qualquer serviço, será objecto de análise e decisão, devendo ser objecto de resposta com a maior brevidade possível, que não excederá, em regra, 15 dias.
- Nos casos em que se conclua pela necessidade de se alongar o prazo referido no número anterior, deve o serviço dar informação intercalar da fase de tratamento do assunto em análise.

A parte designada por "Informação" tem um parágrafo introdutório, onde está definido que o correio electrónico é um instrumento de trabalho, devendo ser utilizado apenas para troca de informação de carácter profissional. É definido posteriormente a quem será atribuída uma caixa de correio electrónico.

Nos parágrafos seguintes são definidos os acessos às caixas de correio electrónico. É descrita a forma como encaminhar um e-mail recebido, que tem de ser reencaminhado para o serviço de expediente para que se dê o respectivo registo de entrada e saída. É definido também que têm de existir duas pessoas responsáveis que garantam o tratamento ininterrupto da informação, encaminhamento interno e/ou externo, resposta, colocação de informação de carácter oficial no local pré-definido e assegurar uma resposta aos munícipes.

O último parágrafo define que para salvaguarda de bom funcionamento dos sistemas, todos os possuidores de caixas de correio devem participar em amostragens, no caso de ser necessário um escrutínio para avaliação técnica de questões relativas a possíveis fontes de vírus e outras problemáticas de segurança em conformidade com o Decreto-Lei n.º 67/98.

Seguidamente é apresentado um esquema de encaminhamento de correio e uma tabela com a indicação do endereço de correio electrónico do responsável pela caixa de correio e a sua assinatura.

Componentes em falta

Considerando que é um documento que inclui as directivas da Autarquia em matéria de SSI, mais concretamente em relação ao correio electrónico, nota-se a omissão da identificação do responsável pela manutenção do documento, não há qualquer referência a sanções que a Autarquia possa impor a quem não cumprir aquilo que o documento estabelece, embora o facto do responsável pela caixa de correio assinar o

documento atestando a sua aceitação e conhecimento do mesmo pode subentender a possibilidade de uma qualquer sanção em caso de incumprimento. Falta também a identificação da entidade que aprovou o documento, bem como a data de aprovação.

Caso 3

Conteúdo do documento

O documento inicia-se com uma página de rosto que contém o logótipo e designação da Câmara Municipal, o título do regulamento, o carimbo com a deliberação e no rodapé por quem foi elaborado e em que data.

Na "Introdução" está definido o objectivo e o propósito do regulamento, segue-se a listagem da legislação a que este regulamento dá cumprimento, a indicação de quem contactar em caso de dificuldades na interpretação que (GTIC) e a forma como vai ser distribuído. O regulamento será entregue a todos os funcionários e agentes que executem trabalho nas instalações do Município, sendo assinado um formulário próprio que será incluído no processo do funcionário. Qualquer alteração por aditamento ou revisão a este regulamento, que não justifique a sua remodelação total, será publicado na intranet do Município. Seguem-se duas páginas com o Índice.

O Capítulo I, denominado por "Disposições Gerais", aborda o âmbito do regulamento, definido como, "estabelece os princípios gerais que norteiam a utilização do equipamento informático, tecnologias de Informação e comunicação do Município". O segundo artigo deste capítulo denominado por "Objecto", define que "o presente regulamento estabelece e define as regras e as condições a que devem obedecer todos os elementos que utilizam os recursos computacionais e da rede de dados e comunicações do Município".

O Capítulo II, designado por "Princípios de Actuação do Gabinete de Tecnologias de Informação e Comunicação", aborda um conjunto de princípios de actuação pelos quais o GTIC se deve pautar: planeamento, coordenação, modernização administrativa, administração aberta e informação.

O Capítulo III é denominado por "Atribuições do Gabinete de Tecnologias de Informação e Comunicação". Entre as atribuições do GTIC está a de assegurar a administração, a manutenção e a adequada exploração dos sistemas de informação, garantindo os mecanismos de protecção, segurança e controlo de acesso definidos, de forma a garantir a privacidade e a integridade, quer dos vários componentes que formam os sistemas informáticos e de comunicações, quer da informação constante dos ficheiros informáticos centralizados ou que circulem na rede.

O Capítulo IV, designado por "Horário de Funcionamento", define o horário de funcionamento do GTIC.

O Capítulo V, designado por "Formação em Ferramentas das Novas Tecnologias", define que os utilizadores do equipamento informático têm o direito de receber formação adequada no domínio da exploração do mesmo, tendo em conta as respectivas funções e o posto de trabalho.

O Capítulo VI, intitulado "Identificação, Aquisição, Transferência e Abate do Equipamento Informático", aborda aspectos como identificação dos equipamentos através do número de série dos mesmos a aquisição pressupor sempre o estudo e análise do GTIC e a transferência e abate de equipamento informático de passar pelo GTIC.

No Capítulo VII, intitulado "Regras e Responsabilidades do Utilizador", são destacáveis os seguintes aspectos: a identificação do utilizador através do *login* e *password*, que responsabiliza o utilizador pela sua correcta utilização. Outro aspecto é a organização da informação, por exemplo, em pastas, dever ser efectuada de forma intuitiva, de modo a ser entendida por qualquer elemento, sendo-lhe atribuído nomes que indicam o assunto e conteúdo da mesma. Por último, é listado um conjunto de procedimentos a seguir em caso de detecção de anomalias.

O Capítulo VIII, designado por "Regras para Impressão", define que o equipamento de impressão do Município deve ser utilizado única e exclusivamente para serviço do mesmo devendo ser utilizado correctamente e com moderação.

O Capítulo IX é denominado por "Regras de Utilização da Intranet/Portal". O portal do Município foi arquitectado pensando no utilizador, tendo como principal prioridade, a acessível, rápida e eficaz actualização dos conteúdos. Toda a informação é colocada pelos utilizadores de cada unidade orgânica, para esse efeito, é indicado como editar texto, imagens e a área de trabalho. A aprovação de conteúdo e do *layout* será da responsabilidade dos aprovadores.

O Capítulo X, intitulado "Regras de Utilização da Internet", é composto por um artigo que define um conjunto de pontos relacionados com a utilização da Internet, realçando-se os seguintes:

- É expressamente proibido utilizar ferramentas externas de conversação (chat, Messenger, etc.) na infra-estrutura disponibilizada pelo Município.
- É expressamente proibido ocupar largura de banda de acesso à internet para ligar a rádios ou conteúdos multimédia.
- A utilização de páginas de *webmail* que possam causar infecção na rede de dados e comunicações será responsabilidade do utilizador.
- É expressamente proibido disponibilizar, enviar, transferir e transmitir qualquer conteúdo que seja ilegal.
- É expressamente proibido disponibilizar, transmitir e enviar qualquer informação do Município que não tenha sido previamente autorizada. O incumprimento desta regra é considerado fuga de informação punido por Lei.
- O Município reserva-se o direito de inspeccionar todos os ficheiros armazenados em áreas privadas da sua rede, com vista a garantir o cumprimento de Leis ou as regras deste regulamento.

O Capítulo XI, designado por "Regras de Utilização do Correio Electrónico", define um conjunto de aspectos relacionados com a utilização do correio electrónico, nomeadamente:

- A caixa de correio deve ser utilizada só para trabalhos do Município, não devendo ser utilizada para troca de correspondência pessoal.

- O utilizador identificado como o autor do registo de um endereço de correio electrónico é o único responsável pelos conteúdos alojados na caixa de correio.
- O Município reserva-se o direito de auditar o cabeçalho das mensagens enviadas e recebidas, assegurando o cumprimento da Lei da Protecção de Dados Pessoais e assegurar o cumprimento deste regulamento.

O Capítulo XII, intitulado "Excepções às Regras Apresentadas", define que qualquer excepção necessária ao apresentado neste regulamento, deverá ser colocada por escrito, dirigido ao responsável do GTIC, justificando a sua necessidade.

Por fim, tem-se o Anexo, que é uma Declaração com o seguinte teor: " (Nome) funcionário/agente do Município das …, declara que lhe foi entregue o Regulamento Interno de Utilização das Tecnologias de Informação e Comunicação, o qual se compromete a tomar conhecimento e cumprir", seguindo-se a indicação da data e a assinatura do funcionário ou agente.

Componentes em falta

O regulamento analisado no que concerne às suas componentes, apresenta uma estrutura bastante completa. A identificação de quem contactar em caso de dúvidas e de alguma anomalia é feita, contudo não é referido o responsável pela manutenção do documento. Não é possível uma identificação clara dos destinatários do documento, contudo pode subentender-se que sejam os mesmos a quem é feira a sua divulgação, que é identificado com sendo todos os funcionários e agentes que executem trabalho nas instalações do Município.

Caso 4

Conteúdo do documento

O primeiro parágrafo define para que fim o "Espaço internet" foi criado pelo Município, pretendendo que este espaço seja um espaço de bem-estar físico e virtual, ao mesmo tempo mostrar ao público que a Internet é uma ferramenta de trabalho indispensável e também um instrumento de lazer.

O segundo parágrafo estabelece as regras a serem respeitadas no referido espaço de acesso à Internet, onde se podem destacar as seguintes:

- Definição do tempo que cada utilizador poderá aceder à Internet.
- Proibição do uso de *pen drive* sem a autorização do monitor.
- Não ser permitido instalar ou desinstalar programas e/ou ficheiros.
- Não ser permitida a consulta de páginas com conteúdo menos próprio ou ilícito de qualquer tipo.

Componentes em falta

O documento analisado, no que concerne às suas componentes, apresenta uma estrutura bastante simples e muito restrito, referindo-se apenas ao "Espaço Internet". A indicação de quem contactar em caso de dúvidas não é feita. Outra omissão é não estar feita a identificação dos destinatários do documento.

Outra omissão no documento analisado é a falta de identificação do objectivo e propósito das normas. Na política de SSI em análise não há qualquer referência a sanções que a Câmara Municipal possa impor a quem não cumprir aquilo que o documento estabelece. O documento é meramente informativo, não responsabilizando explicitamente os utilizadores sobre nada em concreto.

O documento é omisso também na identificação de quem o aprovou e em que data, bem como em muitos aspectos que normalmente são abordados quando se trata da SSI, muito pelo facto de se tratar de um documento com uma dimensão bastante reduzida e de abrangência muito específica.

Adverte-se aqui para o facto que dada a natureza deste documento ser direccionada apenas para o "Espaço Internet" e face à sua reduzida dimensão e abrangência, não corresponde ao que se tem exposto sobre as componentes e características que se esperam encontrar numa política de SSI. Contudo, uma vez que para a Câmara Municipal a que este documento pertence é tida como política de SSI, foi assim considerada e analisada como as demais.

Caso 5

Conteúdo do documento

A folha de rosto tem no canto superior esquerdo o nome do Município e no canto superior direito "Câmara Municipal GIPI", no centro o título da Política seguindo-se a Classificação do documento e que é a Rev. 1.1, sucedendo-se o mês e ano de aprovação, no rodapé tem uma frase com o seguinte: Entregue a (espaço em brando) em (formato data).

Segue-se a página de Índice com a descrição dos cinco pontos que compõem o documento.

O ponto 1, denominado "Introdução", dá ênfase a um conjunto de aspectos onde se destacam os seguintes:

- Em que data foi a política aprovada.
- Que a política foi aprovada em reunião ordinária da Câmara Municipal.
- Os destinatários da política, que são todos os colaboradores do Município ou terceiros devidamente autorizados a acederem a qualquer sistema informático ou computador isolado, pertença ou meramente operado pelo Município.
- O propósito da política, que é proteger os activos de informação detidos e utilizados pelo município de todas as ameaças, internas ou externas, deliberadas ou acidentais, e satisfazer todas as exigências regulamentadas e/ou legisladas.
- Define as sanções para os utilizadores que praticarem actos previstos na Lei de Criminalidade Informática e demais legislação em vigor que poderão para além de uma acção criminal, incorrer em acção disciplinar.
- Por último, define que a política será publicada nos procedimentos internos do Município incluindo a sua inclusão na Internet, qualquer aditamento ou revisão será comunicado a todos os colaboradores através de correio electrónico ou qualquer outra forma escrita.

O ponto 2, designado “Software protegido pelo direito de autor”, menciona a lei do direito de autor que regulamenta o uso de propriedade intelectual. De entre os aspectos versados realçam-se os seguintes:

- É ilegal copiar qualquer peça de software a menos que expressamente permitido pelo legal detentor dos direitos de autor.
- Nenhum colaborador da Câmara deverá fazer ou executar de qualquer forma cópias de qualquer software.
- Qualquer colaborador que reproduza software ilegalmente ficará sujeito às penalidades criminais e cíveis que daí possam advir.
- Todo o software só pode ser adquirido com parecer favorável do Gabinete de Informática.
- Não é permitido aos utilizadores trazer software do exterior e instalá-lo em qualquer computador da Câmara.
- A instalação de aplicações de terceiros, jogos ou *screen savers* não é permitida em qualquer computador da Câmara.

O ponto 3, intitulado “Segurança”, aborda um conjunto de aspectos importantes, entre eles:

- A todos os utilizadores são consignados um *username* e uma *password* que são únicas e que não podem ser partilhadas com qualquer outro colaborador.
- As *passwords* não devem ser escritas, têm de respeitar um determinado número de caracteres e ser alteradas em intervalos regulares.
- Nunca deixar um computador ligado à rede desacompanhado e com a *password* introduzida.
- É considerado crime tentar ter acesso deliberado a um sistema para o qual não se tenha autorização.
- O Gabinete de Informática verifica regularmente todos os sistemas e eventuais tentativas de acesso não autorizado aos mesmos.
- Os dados importantes para o funcionamento dos serviços devem ser salvaguardados numa unidade de rede.
- A responsabilidade de todos os dados que se encontram nos serviços de rede é dos Serviços de Informática que assegurará que os *backups* são executados regularmente e armazenados em local seguro.
- Nenhum dispositivo periférico de qualquer tipo (máquinas fotográficas digitais, PDA’s, etc.) pode ser instalado ou configurado em qualquer computador da Câmara.

O ponto 4, intitulado “Correio electrónico – Uso Aceitável”, observa que a Câmara providencia o uso de um sistema de correio electrónico para ajudar os colaboradores no desempenho do seu trabalho e que o seu uso deverá ser limitado às actividades oficiais. Outros aspectos relacionados com o uso do correio electrónico são definidos, nomeadamente:

- Listagem de mensagens proibidas.
- Nenhuma mensagem deveria ser enviada ou recebida cujo conteúdo tenha a ver com actividades ilegais.
- O sistema não pode ser utilizado para ganhos financeiros pessoais.
- Correio electrónico da Câmara Municipal assim como outros documentos internos, não devem ser enviados para destinos fora da Câmara.

- O utilizador que se ligou a um computador será considerado como o autor de qualquer mensagem enviada desse computador.
- Os endereços de correio electrónico não devem ser públicos se tal não for necessário.
- O correio electrónico não deve ser usado para enviar grandes arquivos apensos, a menos que seja muito urgente.
- Não se devem abrir anexos de correio electrónico executáveis.

O ponto 5, designado de "Internet - Uso Aceitável" é composto por um conjunto de pontos, podendo ser realçados os seguintes:

- A Câmara Municipal providenciará acesso à Internet aos colaboradores no sentido de os ajudar no seu desempenho profissional, subentendendo-se que o seu uso deverá ser limitado aos processos oficiais da Câmara.
- Nenhuma mensagem que possa comprometer ou criar atritos na Câmara Municipal por se ofensiva ou abusiva, deverá ser colocada na Internet.
- Não deverá envolver-se em qualquer actividade ilegal através da utilização da Internet.
- O utilizador que está ligado na rede será considerado como a pessoa que está a explorar a Internet, devendo terminar ou suspender a sessão sempre que se ausente do seu local de trabalho.

Componentes em falta

Como componente em falta neste documento tem-se a não identificação do responsável pela manutenção do documento.

Caso 6

Conteúdo do documento

O cabeçalho do documento contém o logótipo da Câmara, a designação completa da Câmara, a designação do gabinete de informática e sistemas de informação e o título. Como está mencionado no início do documento a designação do Gabinete do Informática poder-se-á entender que foi este Gabinete que o elaborou.

A parte intitulada "Finalidade dos Recursos Informáticos" indica que os recursos de tecnologias de informação disponibilizados pela autarquia são destinados exclusivamente às actividades da instituição.

A parte designada por "Utilizadores da Rede da Câmara Municipal" identifica quem são os utilizadores da rede informática da Câmara, que neste caso, são os funcionários, estagiários (com a devida autorização da chefia) e prestadores de serviços para fins relacionados com a actividade da Câmara Municipal desde que devidamente autorizados.

A parte referente ao "Software protegido" é composta por onze parágrafos, onde se refere que os programas homologados e instalados nos computadores e nos servidores de rede são propriedade exclusiva da Câmara Municipal, sendo vedada a sua cópia parcial ou integral, excepto para fins específicos de cópias de segurança.

Neste ponto é também indicada a proibição de cópias não autorizadas de software, ficando o utilizador que copie ilegalmente software sujeito às penalidades criminais e civis que daí possam advir. É indicada também a proibição dos utilizadores trazerem software não licenciado do exterior e instalá-lo em qualquer computador da Autarquia.

Por fim, neste ponto é remetido para o Gabinete de Informática e Sistemas de Informação a responsabilidade pelo registo e actualização de todo o software.

A parte intitulada por "Regras para utilização da Rede Interna da Câmara Municipal" é composta por doze pontos, incluindo orientações que os utilizadores devem seguir no âmbito da utilização da rede interna da Autarquia. São definidos os comportamentos a observar ou a evitar na utilização na rede interna, nomeadamente:

- Que todos os recursos informáticos da rede de computadores deverão ser utilizados exclusivamente para fins profissionais, que envolvam actividades relacionadas com os serviços da Câmara;
- Que todos os utilizadores da rede interna receberão *login* e *password* de acesso exclusivos para a sua utilização e é obrigatório que todos os utilizadores tenham *passwords* individuais;
- Nunca deixar o computador ligado à rede desacompanhado com a sessão aberta e consequentemente com a *password* introduzida;
- Que todos os ficheiros que não tenham fins profissionais devem ser apagados dos equipamentos para evitar problemas futuros com auditorias.

Restrições na utilização da rede interna são também listadas, nomeadamente a proibição de instalação ou configuração de qualquer dispositivo periférico num computador da Autarquia, excepto pelo gabinete de informática e sistemas de informação, bem como a proibição de ligar computadores pessoais ou de terceiros à rede da Câmara Municipal sem o prévio conhecimento do Gabinete de Informática.

A parte intitulada por "Regras para utilização do Correio Electrónico (e-mail)", composta por nove parágrafos, embora difira da anterior, a natureza dos seus conteúdos não é muito diversa, uma vez que ambas estipulam comportamentos a observar ou a evitar na utilização dos recursos informáticos, nomeadamente:

- Que as mensagens tanto internas como externas devem ser exclusivamente de carácter profissional;
- As mensagens de correio electrónico que totalizem mais de 40 MB apenas devem ser enviadas após as 17:00h, excepto os e-mails internos e os que por conveniência e urgência de serviço devam ser enviados imediatamente;
- Reservar-se a Câmara o direito de auditar a utilização das contas de correio electrónico da Câmara fornecidas aos utilizadores, sem se caracterizar tal acção como invasão de privacidade.

Restrições na utilização do correio electrónico são listadas, nomeadamente no que diz respeito às contas, estando indicada a proibição de manter configuradas contas de correio electrónico de servidores externos. As configurações e o tamanho limite para o envio de correio electrónico são também mencionados, estando definido como tamanho máximo para envio de correio electrónico o limite máximo de 10 MB.

A parte designada por “Regras para a utilização da Internet” é composta por quinze parágrafos, embora a sua abrangência seja diferente das duas partes anteriormente focadas, a sua natureza não difere muito dessas. Restrições e comportamentos a adoptar por parte dos utilizadores são aqui descritos, nomeadamente o controlo a todos os acessos à Internet, com a realização de auditorias nas páginas consultadas, podendo vir a ser desenvolvidos relatórios com nomes, páginas consultadas e tempo de consulta. Proibições de utilização de programas de troca de mensagens instantâneas são aqui apresentadas, a alteração das configurações da rede e de acesso à Internet é também proibida, bem como a proibição de ouvir rádio e ver televisão através da rede da Câmara.

A parte intitulada de “Atribuição exclusiva do Gabinete de Informática e Sistemas de Informação” é composta por cinco parágrafos, definindo quais as responsabilidades, atribuídas a esse gabinete, designadamente:

- Definir e divulgar as medidas de segurança da informação;
- Instalar ou remover componentes, fazer manutenção e controlar hardware e software;
- Homologar hardware e software;
- Autorizar tecnicamente a aquisição de hardware e software;
- Realizar auditorias de hardware e software, com a finalidade de garantir a protecção dos recursos informáticos e o seu uso exclusivo nas actividades da Câmara Municipal.

A parte designada de “Atribuições dos utilizadores” é apresentada em sete parágrafos e enumera as responsabilidades e obrigações de cada utilizador, nomeadamente a responsabilidade pela guarda e protecção dos recursos informáticos colocados à sua disposição, bem como responder pelo uso exclusivo e intransferível das suas *passwords*. É referida como obrigação a aquisição de conhecimento técnico necessário para a correcta utilização dos recursos.

A parte intitulada “Atribuições das chefias” é apresentada em cinco parágrafos e apresenta as chefias como a interface entre os restantes utilizadores e o gabinete de informática. Às chefias é-lhes atribuído o dever de zelar pelo cumprimento destas normas e procedimentos e notificar imediatamente o gabinete de informática e sistemas de informação sobre quaisquer vulnerabilidades e ameaças de quebra de segurança, bem como educar os funcionários sobre os princípios e procedimentos de segurança da informação, e advertir formalmente o utilizador e aplicar as sanções adequadas quando este violar os princípios ou procedimentos de segurança.

A décima parte intitulada “Salvaguarda de ficheiros” é composta por três parágrafos, apresentando responsabilidades tanto do gabinete de informática como dos utilizadores, tais como:

- A responsabilidade de todos os dados que se encontram nos servidores de rede é da responsabilidade do Gabinete de Informática e Sistemas de Informação que assegurará que os *Backups* regulares são executados e armazenados em local seguro;
- Os utilizadores devem manter, obrigatoriamente, os dados críticos da autarquia nos servidores de rede;
- É da responsabilidade exclusiva do utilizador a cópia e a guarda dos dados existentes no posto do local de trabalho.

Na parte designada de “Penalidades” está indicado que todos os utilizadores são responsáveis pelo uso correcto das ferramentas electrónicas de propriedade da Câmara e que todas as práticas que representam ameaça à segurança da informação serão tratadas com a aplicação de sanções disciplinares.

Por último, a parte designada de “Responsabilidades” descreve a obrigatoriedade de todos (utilizadores, chefias e gabinete de informática e sistemas de informação) cooperarem para que o sistema de segurança atinja a desejada eficácia. É também dito que todos os utilizadores da rede informática da Câmara passem a receber uma cópia deste manual.

Componentes em falta

A política de segurança que se analisa no Caso 6, no que concerne às suas componentes, apresenta uma estrutura bastante completa. A indicação de quem contactar em caso de dúvidas é feita, é também indicado quem contactar para o envio de sugestões de actualização, pedidos de excepção ou comunicação de incidentes detectados, contudo não é referido o responsável pela manutenção do documento.

É possível uma identificação clara dos destinatários do documento, porém, podem-se apontar outras omissões no conteúdo do documento, designadamente a do Propósito e Objectivos. Em relação ao objectivo avançado pelo documento para a política observa-se a falta de justificação para além da razão administrativa para o seu estabelecimento. Quanto ao propósito não se elabora sobre este ponto em qualquer parte da política.

Outra omissão que se verifica neste documento é a falta de identificação da entidade que aprovou a política de SSI.

Caso 7

Conteúdo do documento

Os vários artigos que compõem o documento são precedidos por uma breve “Introdução” que destaca a importância das novas tecnologias no processo de modernização administrativa e a necessidade de regulamentar alguns aspectos relacionados com a aquisição e utilização das TI, nas suas diversas componentes (hardware, software, comunicações, Internet, etc.).

O Artigo I, denominado por “Competências”, define que é à Divisão de Informática (DI) que compete gerir os recursos informáticos existentes ou a implementar nos demais serviços da Câmara.

O Artigo II, designado por “Funções”, define que a DI terá as seguintes funções:

- Administração dos sistemas informáticos centrais, bases de dados e comunicações.

- Zelar pela segurança dos sistemas centrais, das aplicações e dos dados, bem como o desenvolvimento e implementação das normas e de todas as medidas de segurança.
- Elaborar e/ou acompanhar os estudos e projectos relacionados com os sistemas de informação.
- Instalar e/ou acompanhar a instalação de novas aplicações e formação dos utilizadores, bem como assegurar o bom funcionamento e manutenção dos produtos e ainda garantir a existência dos manuais actualizados.
- Manter o bom funcionamento de todos os sistemas informáticos (servidores e microcomputadores) e respectivos periféricos, bem como diagnosticar as causas de interrupção dos sistemas e promover a sua recuperação.
- Estabelecer o fluxo de atendimento dos serviços solicitados, bem como o controlo e andamento dos serviços em execução e apoiar todos os serviços na implementação e utilização dos meios informáticos.

O Artigo III, intitulado "Aquisição dos meios informáticos", define que é a DI que acompanha e deve auscultar os serviços sobre as aquisições de software e hardware, bem como o acompanhamento de todas as aquisições de meios informáticos.

O Artigo IV, designado por "Recepção dos meios informáticos", define que essa recepção, é feita pela DI que confirma as especificações técnicas, bem como regista e mantém actualizada a informação sobre o parque informático existente na Câmara.

O Artigo V, intitulado "Instalação e utilização dos meios informáticos", define que essa responsabilidade é da DI. A responsabilidade da DI vai desde o deslocamento de equipamento entre serviços, à instalação de software.

O Artigo VI, intitulado "Requisição e instalação de consumíveis", define que a requisição interna dos diversos consumíveis informáticos é da responsabilidade dos respectivos utilizadores e deverá ser feita ao armazém de acordo com as regras de funcionamento deste. A DI emitirá parecer sobre a aquisição deste tipo de materiais, bem como nas quantidades necessárias, tendo em consideração os equipamentos existentes na Câmara.

O Artigo VII, designado por "Pré-impressos e formulários", define que a criação de novos pré-impressos ou formulários, a actualização dos já existentes ou a recuperação de *stock* no armazém serão obrigatoriamente acompanhados pela DI, de acordo com a racionalização dos circuitos de informação e das normas aplicativas do software instalado.

O Artigo VIII, intitulado "Funcionamento do Serviço de Informática", aborda vários aspectos como o horário, a forma como são feitas as cópias de segurança e recuperação de informação em servidores, as cópias de segurança e recuperação de informação nos postos de trabalho, a forma de participação e resolução de anomalias, os responsáveis pelo zelo dos equipamentos e a forma como é feita a cedência de acessos e permissões.

O Artigo IX, designado por "Formação", define que nas fases de implementação das soluções informáticas e sempre que for necessário, será ministrada a formação

adequada, sendo esta previamente elaborada e estruturada pelo órgão responsável da formação profissional, com o apoio da DI.

O Artigo X, designado por "Actualizações", define que as actualizações são feitas dependendo da disponibilidade financeira para cada ano e de acordo com o Plano de Actividades estabelecido, procedendo-se às actualizações indispensáveis e devidamente fundamentadas, a nível dos equipamentos, software e formação dos utilizadores.

O Artigo XI, intitulado "Histórico do Parque Informático", define que a Divisão de Aprovisionamento colaborará com a DI, no sentido de manter o inventário de todo o equipamento actualizado.

O Artigo XII, designado por "Generalidades", aborda que a DI deverá, no âmbito das suas funções, zelar pelo cumprimento das Normas e que a Câmara Municipal, através do seu Presidente ou Vereador responsável pela área de Informática, prestará quaisquer esclarecimentos adicionais sobre esta matéria e também sobre os casos omissos, implementando, sempre que se justifique, as alterações necessárias e adequadas em conformidade com a evolução e expansão da informatização na autarquia.

Componentes em falta

O regulamento analisado, no que concerne às suas componentes, apresenta uma estrutura direccionada para o parque informático, restringindo assim a sua estrutura. A responsabilidade pela manutenção do documento não é clara. Não é feita a identificação dos destinatários do documento, bem como os objectivos e propósito do regulamento. Outra missão é a não referência a sanções a aplicar a quem não cumprir com o regulamentado.

Caso 8

Conteúdo do documento

A página de rosto indica que se trata de uma nota de serviço interno do Vereador do Pelouro para os utilizadores de Informação do Município. Para além da identificação do assunto, contém dois parágrafos com a identificação da sua aprovação, descrição dos objectivos das presentes normas e a forma como vão ser divulgadas. Essa nota é assinada pelo Vereador do Pelouro.

O capítulo I, denominado por "Introdução", é composto por um artigo. A Introdução tem um preâmbulo, que nos dois primeiros parágrafos justifica o porquê das presentes normas, por fim refere o propósito e objectivo das mesmas. O primeiro artigo define que o uso dos recursos informáticos deve estar relacionado com o estudo de questões respeitantes ao Município.

O capítulo II, designado por "Definições", é composto por três artigos, em que se aborda:

- Recursos informáticos do Município – são identificados todos os recursos informáticos do Município desde impressoras a fotocopiadores.

- Autorização de uso – a autorização do uso dos recursos informáticos é feita para utilização nas instalações pertencentes ao Município.
- Utilizadores autorizados – são considerados todos os funcionários técnicos e administrativos e colaboradores do Município.

O capítulo III, intitulado "Responsabilidades do Utilizador", é composto por sete artigos, que abordam:

- Acesso a informações – Nenhum utilizador pode ter acesso, copiar, alterar ou eliminar ficheiros de terceiros sem autorização explícita.
- Propriedade intelectual – Todos os utilizadores têm o dever de respeitar a propriedade intelectual e os direitos de autor.
- Utilização ofensiva – Nenhum utilizador pode, sob quaisquer circunstâncias, usar os recursos informáticos do Município para difamar ou caluniar.
- Situação de ofensa – Entende-se por ofensa o uso intencional dos recursos para perturbar, amedrontar ou ameaçar que possam indisponibilizar recursos informáticos de forma intencional ou causar danos ou prejudicar as pesquisas e invadir a privacidade do Município.
- Responsabilidade no uso dos recursos – Os utilizadores devem estar cientes das regras e normas de uso dos recursos de informática evitando cortar o acesso a outras pessoas e sobrecarregar os recursos informáticos.
- Integridade e confiabilidade das informações – O utilizador deve entender a natureza mutável de informações armazenadas electronicamente, além de verificar a integridade das informações a que acede ou usa.
- Uso do sistema – O utilizador é responsável pela segurança e integridade da informação do Município armazenada no disco do computador sob sua responsabilidade.

O capítulo IV, intitulado "Acesso às Instalações e Informações", é composto por sete artigos que abordam aspectos como:

- Proibição de acesso partilhado – Certos códigos e autorizações são do uso individual e intransmissível e não podem ser partilhados com terceiros.
- Utilizadores não autorizados – Não é permitido executar ou configurar software ou hardware com a intenção de facilitar o acesso a utilizadores não autorizados.
- Obrigatoriedade de uso de *password*s seguras – O utilizador é responsável pela manutenção de *passwords* seguras, devendo seguir as normas e procedimentos definidos nestas normas.
- Uso privilegiado pelos administradores de Sistema – Informações obtidas por meio de direitos especiais e privilégios devem ser tratadas como privadas e totalmente confidenciais pelos administradores, que responderão por qualquer uso indevido.
- Cancelamento de acesso – ao deixar de ser funcionário ou colaborador o acesso ao sistema será bloqueado.
- Acesso de computadores à rede – Nenhum equipamento poderá ser ligado à rede informática sem a notificação e autorização do Sector de Informática.
- Autorização de uso de mecanismos de auditoria e segurança – O administrador de sistema possui autorização para utilizar o sistema de segurança ou qualquer mecanismo que julgue adequado para a auditoria e controle dos computadores e da rede.

O capítulo V, designado por "Acessos, Operações e Acções Não Permitidas aos Utilizadores", é composto por sete artigos, focando aspectos como:

- Descodificação e acesso ao controle de informações – é proibido usar qualquer software ou outro dispositivo para interceptar ou descodificar *passwords* ou obter informações armazenadas nos computadores de outros utilizadores.
- Actividades não permitidas – É expressamente proibida toda e qualquer tentativa deliberada de retirar o acesso à rede ou a qualquer computador do Município ou de prejudicar o seu rendimento.
- Monitorização não autorizada – Os recursos de informática não podem ser utilizados para o controlo e reserva não autorizados de mensagens electrónicas ou qualquer transmissão de dados.
- Uso de informação e materiais protegidos por *copyright* – Só com autorização ou licença poderá um utilizador servir-se de material protegido por *copyright*.
- Propagandas e campanhas políticas – É proibido o uso dos recursos informáticos da Município para campanhas políticas ou propaganda de qualquer espécie.
- Uso dos recursos informáticos em actividades particulares – É proibido o uso de recursos informáticos em actividades particulares.
- Uso excessivo – O uso dos recursos informáticos, tais como mensagens electrónicas, acesso à Internet, armazenamento de dados em computadores ou a impressão de ficheiros, não devem ser excessivos nem interferir na utilização e acesso de outros utilizadores a esse recurso.

O capítulo VI – Manutenção, Controlo e Auditoria – é composto por cinco artigos, que abordam as seguintes temáticas:

- Controle de acesso a informações – Os utilizadores devem controlar permanentemente o acesso às suas informações e às suas formas de armazenamento, no entanto, antes da cessação do vínculo de trabalho devem entregar ao seu superior hierárquico o acesso aos dados e documentos armazenados pertencentes ao Município.
- Acesso do administrador ao sistema – O administrador tem acesso aos ficheiros, contudo todos os privilégios individuais e direitos dos utilizadores deverão ser preservados.
- Verificação de uso, inspecção de arquivos e auditoria – O administrador de sistemas deve rever e observar periodicamente as informações, certificando-se de que não houve a violação de leis ou a utilização para fins não autorizados.
- Suspensão de privilégios individuais – Pode-se suspender todos os privilégios a um utilizador, por razões ligadas à segurança física e ao bem-estar do utilizador ou por inobservância das regras constantes neste documento.
- Possibilidade de novo acesso – O acesso pode ser restabelecido quando a segurança e o bem-estar ou os interesses estiverem assegurados.

O capítulo VII, intitulado "Responsabilidades do administrador", é composto por três artigos que abordam:

- Medidas de segurança – O administrador de sistemas é responsável pela implementação de medidas de segurança necessárias para garantir a integridade da informação, independentemente da maneira pela qual esteja armazenada e comunicar superiormente o desrespeito por qualquer norma.
- Defesa de direitos de autor – Para garantir os direitos de autor, só o Sector de Informática está habilitado a instalar software e hardware nos computadores.
- Deveres do administrador de sistemas – Cabe ao administrador de sistemas a responsabilidade de assegurar o cumprimento deste regulamento, manter e actualizar dados de todos os utilizadores autorizados, manter no Município um registo de ocorrências de violação dos regulamentos, garantir a segurança dos meios e dos dados, preservar informações confidenciais como, por exemplo, ficheiros de utilizadores e códigos de acesso ao sistema.

O capítulo VIII, denominado por "Procedimentos e Sanções", é composto por quatro artigos que abordam as seguintes temáticas:

- Conhecimento e concordância com as normas de utilização dos sistemas de informação do Município – Os utilizadores têm de assinar um termo de compromisso, no qual manifestem conhecimento e concordância com as presentes normas, comprometendo-se a respeitar e fazer respeitar o presente documento.
- Responsabilidade pela segurança e incidentes – Todos os utilizadores e administradores do sistema têm o dever de comunicar superiormente qualquer tentativa de acesso não autorizado ou qualquer outro uso indevido de recursos informáticos.
- Incidentes e suas consequências – Os incidentes envolvendo utilizadores são comunicados ao Administrador de Sistemas que deles dará conhecimento ao Vereador do Pelouro.
- Outros âmbitos sancionatórios – As sanções impostas pelo Município não isentam o responsável de outras acções legais. O desconhecimento destas normas por parte do utilizador não o isenta das responsabilidades e das sanções aplicáveis, nem pode minimizar as medidas aplicáveis.

O capítulo IX – "Casos omissos" define que as omissões a estas normas serão decididas pelo Executivo Municipal.

Por último, o termo de compromisso identifica o utilizador através do preenchimento do campo com o seu nome e assinatura com indicação da data a seguinte declaração: Declara ter conhecimento das Normas de Utilização do Sistema de Informação do Município cujo conteúdo se compromete respeitar e fazer respeitar.

Componentes em falta

Falta referenciar com clareza quem contactar em situações anómalas e em que casos informar o departamento de informática.

Caso 9

Conteúdo do documento

O capítulo I, denominado "Introdução", é composto por dois artigos, o primeiro define que as presentes normas regulamentam o uso apropriado dos recursos informáticos, com vista à protecção e privacidade efectiva de utilizadores e dados. O segundo artigo define o que se entende por: "recursos informáticos", "sistema informático" e "privilégios de administração".

O capítulo II, designado por "Acesso aos recursos informáticos", é composto por três artigos. O primeiro artigo é designado de "utilização" e remete para o artigo 1.º a utilização dos recursos, bem como a indicação de que os utilizadores devem estar cientes das normas de utilização dos sistemas e recursos informáticos, evitando, desse modo, procedimentos que prejudiquem ou impeçam outras pessoas de terem acesso a esses recursos ou de usá-los de acordo com o que é determinado.

O segundo artigo deste capítulo, que corresponde ao 4.º neste documento, é designado por "Utilizadores" e define que são considerados potenciais utilizadores dos recursos informáticos todos os funcionários e trabalhadores, bem como os eleitos. É indicado também neste ponto o que é necessário solicitar para se poder ser utilizador. Essa categoria extingue-se quando o indivíduo deixar de ser funcionário, trabalhador ou eleito.

O terceiro artigo, designado por "Administração do sistema", define que o administrador de sistema é um utilizador com privilégios especiais e responsabilidades acrescidas face ao sistema e aos recursos, devendo ser o responsável da área/serviço onde está enquadrada a Informática. É também mencionado que deve ser indicado um segundo administrador que também deve ser membro da referida área.

O capítulo III, intitulado "Responsabilidades do utilizador", é composto por nove artigos. O primeiro, que é o artigo 6.º do documento, é intitulado "Compromisso de confidencialidade" e obriga o utilizador do sistema e recursos informáticos a não divulgar, sem autorização do Presidente da Câmara, qualquer informação constante no sistema informático. O segundo artigo deste capítulo, intitulado "Acesso à informação", determina que compete ao responsável de um serviço determinar qual a informação que deve estar disponível e a que utilizadores.

O terceiro artigo, intitulado "Segurança no acesso", responsabiliza o utilizador pela manutenção das *passwords*, bem como, pelas acções indevidas que venham a ser efectuadas a partir do seu acesso ao sistema. O quarto artigo designado "Equipamento distribuído e privilégios associados" responsabiliza o utilizador pelo equipamento que lhe foi atribuído e pela configuração do mesmo. O quinto artigo deste capítulo, intitulado de "Utilização ofensiva" proíbe que utilizadores, sob quaisquer circunstâncias, utilizem o sistema e recursos informáticos da Câmara para difamar, caluniar ou por qualquer modo ofender outros utilizadores ou qualquer entidade, singular ou colectiva, pública ou privada.

O sexto artigo, designado “Utilização excessiva”, proíbe os utilizadores de deliberadamente sobrecarregar os recursos informáticos e determina que os utilizadores devem armazenar a informação, sempre que possível, no servidor central.

O sétimo artigo “Integridade da informação” indica que para manter a integridade dos dados os utilizadores não devem confiar em mensagens de correio electrónico ou outras informações que contrariem as suas expectativas, sem antes verificar directamente junto do possível remetente da mensagem.

O oitavo artigo, intitulado “Responsabilidade pela informação”, responsabiliza os utilizadores pela informação por si produzida e gerida. Antes de perder a qualidade de utilizador, deve disponibilizar, a um superior, documentos por si armazenados.

O nono artigo, designado por “Utilização de bases de dados”, determina que o utilizador com acesso a bases de dados, centralizadas ou não, deve compreender que a informação que nelas consta interage, quase sempre, com vários processos, aplicações ou utilizadores, sendo ele responsável pela integridade da informação que utiliza, devendo compreender a natureza mutável da mesma.

O capítulo IV, intitulado “Segurança e permissões”, é composto por nove artigos e aborda aspectos como:

- Acesso ao sistema e recursos informáticos – é feito através da *password* e outros tipos de autorização, que são de uso pessoal e intransmissível, e não podem ser partilhadas com terceiros, só podendo aceder utilizadores autorizados.
- Acesso às instalações – Só é permitido o acesso de funcionários ligados à Informática aos pólos técnicos, podendo haver excepções quando devidamente justificadas e autorizadas.
- Obrigatoriedade do uso de *passwords* seguras – As *passwords* devem ser substituídas assim que são atribuídas e depois com uma certa regularidade. As *passwords* que sejam comuns não podem ser alteradas sem conhecimento de todos os interessados.
- Ligação de equipamento – Nenhum equipamento pode ser ligado ao sistema ou recursos informáticos da Câmara sem autorização do administrador do sistema ou, em último caso, do Presidente da Câmara.
- Acessos, operações e acções não permitidas aos utilizadores – Os utilizadores não podem usar qualquer software ou outro dispositivo para interceptar ou desconfigurar informações armazenadas ou que estejam a circular nos recursos informáticos. Não é permitida a instalação ou execução de qualquer software que não esteja autorizado para o recurso informático em causa, a não ser por meio de um pedido escrito ao administrador do sistema.
- Propagandas e campanhas – É proibido o uso do sistema ou recursos informáticos em propaganda partidária, bem como qualquer tipo de publicidade não autorizada pelo Presidente da Câmara.
- Actividades particulares – Os recursos informáticos não podem ser utilizados para trabalhos particulares dos utilizadores.
- Utilização abusiva – O uso individual dos recursos informáticos, tais como mensagens electrónicas, acesso à Internet, o armazenamento de dados em computadores e servidores ou a impressão de arquivos, não devem ser

excessivos nem interferir na utilização e acesso de outros utilizadores a estes recursos.

- Armazenamento de informação – Não é permitido o acesso a páginas de Internet, assim como armazenamento nos recursos informáticos de material com conteúdo reservado a adultos ou outro que possa, por qualquer forma, ferir a susceptibilidade de colegas ou ir contra a Lei.

O capítulo V, designado por "Controlo e auditoria", é composto por três artigos, intitulados "Acesso do Administrador", "Auditoria" e "Suspensão de privilégios individuais". No primeiro artigo é definido que o administrador do sistema pode ter acesso aos arquivos e bases de dados dos utilizadores e da Câmara Municipal, bem como ao tráfego que circula pela rede, de forma a garantir a segurança, manutenção e conservação dos mesmos, assim como realizar as auditorias necessárias. No entanto, todos os privilégios individuais e direitos de privacidade deverão ser preservados.

O segundo artigo define que o administrador possui autorização para utilizar os mecanismos que julgar mais adequados para a realização de auditorias e o controle do sistema e recursos informáticos, no âmbito da presente norma. Deve efectuar auditorias periódicas aos dados armazenados e informação que circula pela rede. Se houver evidência de actividade que possa comprometer a segurança do sistema ou dos recursos informáticos, o administrador pode monitorizar e verificar todas as actividades de um determinado utilizador, a bem do interesse da Câmara Municipal.

O terceiro, que é o artigo 25.ºdo documento em análise, define que um utilizador poderá ver suspensos alguns ou todos os privilégios em relação ao uso dos recursos informáticos da Câmara Municipal, por determinação do Presidente da Câmara ou administrador responsável pelo sistema, por motivo de segurança, bem-estar de outros utilizadores ou interesses da Câmara Municipal. A situação anterior poderá ser refeita quando as razões que originam a suspensão forem ultrapassadas.

O capítulo VI – Responsabilidades do administrador – é composto por quatro artigos. O primeiro artigo intitulado "Deveres do administrador", elenca um conjunto de responsabilidades atribuídas ao administrador:

- Assegurar o cumprimento destas normas;
- Manter fichas com dados de todos os equipamentos instalados e autorizados, incluindo o software instalado por equipamento e confirmação do utilizador;
- Manter registo do nome de utilizador e data de atribuição de privilégios, bem como da tomada de conhecimento por parte do mesmo da presente norma e de outras normas;
- Manter um registo das ocorrências de problemas de segurança, integridade ou violação das normas;
- Garantir a segurança dos sistemas informáticos;
- Efectuar cópias de segurança;
- Controlar o acesso físico aos equipamentos sob sua responsabilidade;
- Adaptar medidas apropriadas de segurança em relação a software e licenças adquiridas;
- Administrar todo o processo de gestão de utilizadores;

- Verificar os acessos ao sistema e registos de auditoria para controlar tentativas de violação e quebra de segurança.

Os três restantes artigos deste capítulo, abordam:

- Segurança dos dados – O administrador dos recursos informáticos é responsável pelas medidas de segurança necessárias para garantir a salvaguarda dos dados da Câmara Municipal.
- Defesa de direitos de autor e de licenças – O administrador deve monitorizar, remota ou localmente, os recursos informáticos, de forma a garantir que os direitos de autor e licenciamento são respeitados.
- Apoio ao utilizador – Compete ao serviço de Informática apoiar o utilizador nos equipamentos e software que necessite.

O capítulo VII, intitulado "Procedimentos e sanções", é composto por três artigos que abordam:

- Conhecimento e concordância com a norma – Os utilizadores do sistema ou recursos informáticos da Câmara Municipal devem tomar conhecimento da presente norma. Devem também assinar a ficha, relativamente ao equipamento que lhe está distribuído.
- Responsabilidade pela segurança e incidentes – Todos os utilizadores têm o dever de comunicar superiormente qualquer tentativa de acesso não autorizado ou uso indevido dos sistemas.
- Sanções – Qualquer violação à presente norma é susceptível de constituir ilícito disciplinar. O possível desconhecimento desta norma por parte do utilizador não o isenta das responsabilidades e das sanções aplicáveis, nem pode minimizar as medidas aplicáveis.

Por último, o capítulo VIII – "Casos omissos a estas normas" – é composto por um artigo, que define que os casos omissos deverão ser resolvidos tendo em atenção a Lei geral ou outras normas que venham a ser publicadas nesta área.

Componentes em falta

Para além da identificação do propósito e objectivo no artigo 1.º, não estão claramente identificadas as entidades que o aprovaram nem a data em que foi aprovado.

Caso 10

Conteúdo dos documentos

O documento A principia com um cabeçalho que inclui um título (Norma Interna e a identificação da Câmara Municipal) seguido de uma tabela com um conjunto de campos: Tipo; N.º; Título; Sumário; Homologante; Data; Revogação; Tipo, N.º e Data. Este documento, intitulado "Procedimentos de Aquisição, Instalação e Utilização", estabelece as regras que os utilizadores devem seguir para a aquisição, instalação e utilização dos recursos informáticos da Autarquia.

A primeira parte, designada por "Aquisição de equipamentos, aplicações, consumíveis", indica os procedimentos a seguir na Câmara Municipal para a

aquisição de equipamentos, aplicações informáticas e consumíveis, nomeadamente tinteiros, *toners*, papel, ratos, dispositivos de memória *flash*, disquetes e CDs/DVDs.

A parte intitulada "Instalação de equipamentos, aplicações" define que a instalação de equipamentos e aplicações deve apenas ser executada pela Divisão de Organização e Gestão Informática ou sob a sua supervisão, não sendo atribuídos aos utilizadores direitos de administração sobre o equipamento informático que lhe estiver distribuído, contudo é admissível a atribuição de direitos de administração, com fundamento na natureza das actividades exercidas e no reconhecimento de suficiente competência técnica do utilizador.

A parte referente aos "Acessos electrónicos ao exterior" começa por indicar que os acessos electrónicos ao exterior – Internet, e-mail e outros – são tecnicamente possíveis a partir de qualquer computador ligado à rede informática da Câmara Municipal, desde que o utilizador tenha acedido a esse computador com o seu *login*. São definidas as regras para atribuição de acessos, ou seja, para cada tipo de acesso electrónico ao exterior é necessária uma autorização específica, podendo um mesmo utilizador estar autorizado a usar apenas um ou diversos tipos de acesso electrónico ao exterior.

A parte intitulada por "Acessos electrónico a partir do exterior" partilha a estrutura descrita no parágrafo anterior, contudo neste caso o acesso electrónico é a partir do exterior para a área de trabalho do sistema informático da Câmara Municipal, que deve ser assegurado via VPN com a devida autorização superior.

A última parte referente a "Actividades de manutenção e a utilização de meios informáticos" refere os procedimentos a tomar para evitar perdas de informação e outros riscos, quando se estão a fazer certos procedimentos de manutenção, os quais só devem ser efectuados se não existirem utilizadores activos na rede informática, motivo pelo qual o documento estipula os horários de manutenção e impedimentos de utilização a observar.

Quanto ao documento B, o seu propósito é estabelecer os princípios, procedimentos e dispositivos genéricos em ordem a garantir a confidencialidade, integridade e disponibilidade dos dados e da informação suportada por meios electrónicos. O documento principia com o mesmo quadro que o documento A, com os campos já descritos anteriormente.

Na parte "Princípios fundamentais" aponta-se a obrigatoriedade de todos, no âmbito das suas funções, contribuírem para que os princípios gerais e os procedimentos de segurança sejam respeitados e os dispositivos de segurança se mantenham operacionais.

Quanto aos "Procedimentos e dispositivos operacionais", o documento fornece orientações relativas à segurança física e à segurança lógica. Dentro da segurança física são abrangidos:

- Unidades de alimentação ininterrupta – UPS (Uninterruptible Power Supply) automática, com alertas por correio electrónico;
- Unidades de substituição com imagens periódicas;

- Agentes de monitorização permanentes, com alertas por correio electrónico;
- Contratos de assistência com tempos de reposição dependentes da criticidade do equipamento.

Relativamente à segurança lógica são abrangidos:

- Sistemas de *Backups* dos equipamentos servidores com rotinas:
  - Diárias – Diferenciais
  - Semanais – Incrementais
  - Mensais – Totais
  - *Backups* Mensais guardados em cofre com protecção adequada a suportes magnéticos, em localização geográfica diferente.
- Sistema contra acessos indevidos:
  - Gestão centralizada de direitos de acesso a recursos;
  - Monitorização permanente de equipamentos não autorizados, com alertas por correio electrónico;
  - Equipamentos de intervenção pró-activa contra tentativas de intrusão.

Componentes em falta

Os documentos que se analisam no Caso 10, no que concerne às suas componentes, apresentam uma estrutura bastante simples. A indicação de quem contactar em caso de dúvidas não é feita, não é indicado quem contactar para o envio de sugestões de actualização, pedidos de excepção ou comunicação de incidentes detectados.

Outra omissão é não estar feita a identificação clara dos destinatários do documento, bem como o objectivo da política.

Nos documentos em análise não há qualquer referência a sanções que a Câmara Municipal possa impor a quem não cumprir aquilo que o documento estabelece.

Caso 11

Conteúdo do documento

A página de título inclui a identificação da Autarquia, o título e o número de páginas do documento.

A parte intitulada “Índice” apresenta a estrutura do conteúdo do documento.

A parte designada de “Introdução” indica a função do documento, que é estipular as regras a que os colaboradores do Município ou terceiros devidamente autorizados estão obrigados quando acederem a qualquer sistema informático ou computador isolado, pertença ou meramente operado pelo Município.

Identifica também o seu propósito, ou seja, visa proteger os activos de informação detidos e utilizados pelo Município de quaisquer intromissões, quer internas ou externas, deliberadas ou acidentais.

Por último, esta parte refere a lei que confere competências ao Presidente da Câmara de o aprovar e os meios a utilizar para a sua divulgação pelos utilizadores dos sistemas de informação da Autarquia, que vai ser através da Intranet do Município.

A parte referente ao "Software protegido por direitos de autor", que se divide em dez pontos, fundamentalmente descritivos, informa os utilizadores em relação a diversas vertentes sobre o software da Autarquia instalado nos diferentes postos de trabalho, nomeadamente em relação ao licenciamento do software. O Núcleo de Informática é focado em vários dos pontos, como sendo o responsável pelo registo e actualização de todo o software, instalando as actualizações consoante venham a ser disponibilizadas e mantendo o controlo de todas as versões disponíveis.

A parte designada de "Segurança" é composta por doze pontos, em cinco dos quais são estabelecidos os critérios para a criação, alteração, manutenção e transmissão de *passwords* de acesso ao sistema informático.

Os critérios para a criação de *passwords* estabelecem que estas deverão conter no mínimo seis caracteres e não devem ser fáceis de decifrar.

Os critérios para a alteração de *passwords* determinam a frequência com que as *passwords* deverão ser alteradas, onde não está definido o intervalo de tempo, mas a indicação de que essa mudança deverá ter intervalos regulares e a disponibilização do Núcleo de Informática para ajudar em caso de dúvidas.

Finalmente, os critérios para a manutenção e transmissão de *passwords* ditam que as *passwords* não devem ser escritas ou deixadas onde outros as possam encontrar e que os computadores nunca devem ficar ligados à rede com a sessão aberta quando o seu utilizador se ausenta.

Este ponto do documento aborda também os *Backups* e como os utilizadores devem guardar os dados para os mesmos poderem ser processados de forma a que seja possível fazer os *Backups* de segurança. Finalmente, é proibida a instalação ou configuração nos computadores do Município de dispositivos periféricos (máquinas fotográficas, PDA's, etc.).

A parte intitulada por "Correio Electrónico" é composta por doze pontos, os quais definem os objectivos e propósitos da utilização do correio electrónico pelos utilizadores do município que é o de ajudar os funcionários no desempenho das suas funções. Nesta parte são estipulados comportamentos a observar ou a evitar na utilização dos recursos informáticos, no que se refere ao correio electrónico, entre eles:

- O Município poder remover correio electrónico pessoal identificável para preservar a integridade do sistema de correio electrónico;
- Nenhum trabalhador poderá usar o sistema de correio electrónico de forma a que o mesmo possa ser interpretado como insulto ou ofensivo por qualquer outra pessoa, ou empresa, que sob qualquer forma possa prejudicar a imagem do Município;
- O utilizador que se ligou a um computador é considerado como autor de qualquer mensagem enviada desse computador. Os utilizadores devem lembrar-se de fechar a sessão quando ausentes do posto de trabalho.

As restrições na utilização do correio electrónico são listadas, nomeadamente no que diz respeito:

- Às contas de correio electrónico, nomeadamente em temos de envios de anexos fixando os 7MB como limite máximo para o tamanho dos ficheiros a enviar em mensagens de correio electrónico;
- É interdito o envio de cartas ou outro tipo de mensagens/documentos para cadeias de solidariedade;
- Não subscrever listas de correio electrónico que não sejam do interesse do Município.

A parte designada por "Uso da Internet" é composta por nove pontos, embora a sua abrangência seja diferente das duas partes anteriormente focadas, não difere muito dessas. Restrições e comportamentos a adoptar por parte dos utilizadores são aqui descritos. O tipo de acesso livre ou condicionado é referido no primeiro ponto listado, conforme a sua atribuição para o executivo, directores de departamento, chefes de divisão ou secção e restantes funcionários. Proibições de consultar determinados sites são aqui referidas, bem como o impedimento de a alteração das configurações da rede e de acesso à Internet e descarga de software.

A última parte – "Disposições Finais" – refere o intervalo de um ano para as regras serem objecto de análise e avaliação, visando a prestação de um melhor serviço e desempenho. Refere-se ainda neste ponto que as presentes regras podem ser revistas por sugestões dos utilizadores a quem se destinam.

Componentes em falta

O Documento que se analisa no Caso 11, no que diz respeito às suas componentes, apresenta uma estrutura devidamente delineada, incidindo o seu conteúdo directamente nos pontos fulcrais da SSI. A indicação de quem contactar em caso de dúvidas é feita ao longo do documento indicando também quem contactar para o envio de sugestões de actualização, pedidos de excepção ou comunicação de incidentes detectados, contudo não é indicado o responsável pela manutenção do documento.

No documento são superficialmente identificados os seus destinatários, bem como o seu propósito. Também é indicado que qualquer suspeita de violação do regulamento que possa afectar os sistemas do Município serão tratados nos termos da lei, sem indicação específica das sanções a aplicar. Pode-se ainda apontar outra omissão no conteúdo do documento, que é a não definição dos objectivos da política. No decorrer da leitura do documento, verifica-se uma incongruência no que diz respeito ao tipo de documento, umas vezes é denominado de "Regras" e outras vezes de "Regulamento", um aspecto importante uma vez que a luz da lei da Administração Pública a sua aprovação e âmbito são muito diferentes.

Caso 12

Conteúdo do documento

O cabeçalho do documento é uma tabela que contém o logótipo da Câmara e da Divisão de Modernização Administrativa e Tecnológica, e as suas respectivas designações, o título do documento é aqui apresentado como: Instrução de Trabalho – Gestão de Segurança na Óptica do Utilizador. No canto superior direito apresenta-se um quadro com os seguintes campos: o código do documento; a Edição/Revisão, neste caso tem A01 e a data, que não especifica se é de elaboração ou de formulação. Esta tabela tem também o campo objectivo e âmbito, quanto ao primeiro está definido que o objectivo é a definição da política de segurança na óptica do utilizador, o segundo campo, referente ao âmbito, está escrito que é a segurança da informação.

A parte intitulada "Introdução" começa por observar que a informação é reconhecida como um recurso estratégico e as ameaças aos sistemas de informação devem ter as respostas apropriadas. A informação deve estar disponível, ser autêntica, exacta e actualizada para se manter válida. A utilização intensiva e crítica dos sistemas de informação deve ser minimamente controlada, no sentido de assegurar a continuidade das actividades do Município.

A parte designada de "Audiência" indica o que visa a política, referindo que a política pode ser aplicável a todos os funcionários da Autarquia, de acordo com o compromisso da sua chefia. Refere ainda neste ponto que a política deve ser iniciada e mantida pelo responsável pela Segurança da Informação do Município.

A parte intitulada "Segurança da Informação no Trabalho" é composta por três pontos, que são o Propósito, Definição e Descrição. No primeiro ponto está definido o propósito, ou seja, o objectivo da Segurança da Informação, que é definido como o de garantir a integridade, a confidencialidade e a disponibilidade dos dados e o de ajudar a avaliar a finalidade dos mesmos. O segundo ponto consiste na definição de um conjunto de conceitos: Disponibilidade, Confidencialidade, Integridade, Repúdio e Finalidade. O último ponto, que é a descrição, aborda temas como os riscos potenciais, a confidencialidade dos dados, o armazenamento dos dados, a destruição de dados, as cópias de segurança de dados, os vírus, as boas práticas e as más práticas. Todos estes temas são abordados como recomendações aos utilizadores e não como proibições.

A parte designada por "Política Geral de Software" inicia-se com a definição do propósito da secção que visa a integridade dos sistemas de TIC e pôr em prática a política de licenciamento de software do Município. Segue-se um conjunto de definições, para termos como: Licenciamento de Software; *Freeware*; *Shareware*; Software de Domínio Público e *Plug-in*. O terceiro ponto desta parte define o que são vírus informáticos. O último ponto, denominado software, define e explana os seguintes aspectos: Riscos potenciais, Responsabilidades, Licença de Software, Aprovação de Software, Manutenção de Software, Utilização de Software, Cópia de Segurança do Software e Software Antivírus.

A parte intitulada por “Computadores pessoais e portáteis” é composta por três pontos, iniciando-se com a definição do propósito da secção, define de seguida os conceitos de “computadores” e “hardware”, descreve no terceiro ponto as responsabilidades, configuração, manutenção e gestão de hardware, a utilização do computador e o furto de portáteis.

Dentro do ponto “Responsabilidades” podem-se destacar os seguintes aspectos:

- Cada utilizador é responsável pelo hardware que lhe foi atribuído e deve tratá-lo com cuidado;
- Utilizar o equipamento, software e dados atribuídos pelo Município exclusivamente para os trabalhos do Município;
- Qualquer falha resultará, geralmente, na reinstalação da configuração standard.

Dentro do ponto “Configuração, Manutenção e Gestão de Hardware”, pode-se destacar os seguintes aspectos:

- As configurações de hardware de todos os computadores e periféricos são da responsabilidade da Divisão de Modernização Administrativa e Tecnológica. Isto inclui orçamento, padrões, compras, instalação, configuração, manutenção e suporte;
- Os utilizadores não devem alterar as configurações de hardware, acrescentar ou remover componentes do seu computador pessoal ou portátil sem a aprovação da Divisão de Modernização Administrativa e Tecnológica.

O ponto sobre a utilização do computador descreve que o equipamento atribuído pelo Município deve ser usado apenas para os trabalhos do Município.

O último aspecto dentro do ponto “Computadores pessoais e portáteis” é o “Furto de Portáteis” onde se define que o utilizador deve estar ciente do crescente risco de furtos de portáteis e que os portáteis são muito fáceis de roubar e fáceis de revender.

A parte designada por “Política de Senhas” é composta por três pontos. O primeiro ponto define o propósito desta secção, que é adoptar uma boa política de senha pessoal, a qual é a primeira barreira contra acessos não autorizados aos sistemas existentes. Nos pontos seguintes são explicados, na perspectiva do utilizador, responsabilidades, boas práticas e procedimentos na escolha de uma senha.

Como responsabilidades destacam-se que os utilizadores devem estar conscientes de que são responsáveis por todas as tentativas ou acções cometidas, não autorizadas, com o seu nome de utilizador e senha. É absolutamente imperativa a não divulgação de seu nome de utilizador e respectiva senha. Os utilizadores também devem estar conscientes do risco de personificação, nunca devendo fornecer o nome de utilizador e respectiva senha por telefone ou por correio electrónico.

Ainda no ponto referente à “Política de Senhas” elabora-se sobre a escolha da senha, referindo bons e maus exemplos na sua escolha e exemplos de procedimentos a adoptar.

A parte intitulada por “Correio Electrónico” é composta por três pontos. O primeiro define o propósito, que é efectuar o serviço de distribuição de mensagens

electrónicas baseado na rede Internet. Nos dois pontos seguintes são explicados, na perspectiva do utilizador, a configuração do correio electrónico, nomeadamente em termos de consulta e utilização do serviço de e-mail por *webmail*, as quotas para as caixas de correio, a protecção contra vírus, a implementação de uma sistema Anti-Spam, algumas precauções a ter com o e-mail e boas práticas, como por exemplo, compactar os ficheiros sempre que o volume o justifique; apagar de imediato ficheiros com a extensão .exe ou mensagens consideradas suspeitas e por último evitar clicar em *links* que vêm em e-mails, mesmo se o remetente for conhecido.

Componentes em falta

O documento que se analisa no Caso 12, no que concerne às suas componentes, apresenta-se devidamente estruturado. Está definido quem inicia e mantém a política de SSI e a existência de um responsável pela segurança da informação no Município. É feita a identificação dos destinatários do documento. A omissão que se verifica nesta política é a inexistência da definição de sanções que a Autarquia possa impor a quem não cumprir com o estipulado no documento.

Caso 13

Conteúdo do documento

A parte intitulada "Segurança" é composta por quatro pontos, abordando temáticas como a segurança lógica, os equipamentos informáticos e/ou periféricos, o acesso e utilização de serviços dos centros de dados (*Data Centers*) e o acesso às salas técnicas (bastidores e equipamento activo).

O primeiro ponto define um conjunto de proibições e recomendações, em relação às políticas de *passwords* e ao abandono do computador com a sessão aberta. Os utilizadores são também neste ponto responsabilizados por tentativas de acesso deliberado a um sistema para o qual não tenham autorização. O utilizador é responsável pela salvaguarda (*backup*) dos dados pessoais. As *passwords* não devem ser escritas, ou deixadas onde outros as possam encontrar e serem óbvias, devem também ser alteradas regularmente.

O segundo ponto tem um conjunto de recomendações, nomeadamente os cuidados a ter com os portáteis, que não devem ficar desacompanhados em qualquer local; bem como os procedimentos a ter nas seguintes situações: a movimentação, ou instalação, de equipamento informático ou periféricos dentro ou fora das instalações do Município carece de conhecimento prévio superior, quanto à remoção ou proposta de abate de equipamento será efectuada pelo departamento responsável após coordenação com os serviços competentes, assegurando que são actualizados os registos de hardware e software apropriados.

O terceiro ponto define quem tem autorização de aceder aos centros de dados da Autarquia (*Data Centers*), que são instalações que permitem alojar de forma adequada todos os sistemas de informação considerados críticos para a Autarquia. Neste sentido, estão apenas autorizados a aceder aos centros de dados da Câmara os técnicos do Departamento de Informática.

O quarto e último aspecto abordado dentro do ponto "Segurança" definido como "Acesso às salas técnicas (bastidores e equipamento activo)", sendo em tudo idêntico ao ponto anterior, mas neste caso dirigido a outro sector. Estão apenas autorizados a fazer alterações de *patching* e configurações de equipamentos activos, os técnicos do Departamento de Informática e outros técnicos devidamente autorizados.

A parte designada de "Utilização de Software" indica que a lei dos direitos de autor que regulamenta o uso de propriedade intelectual incluindo o software, é muito directa – excepto nos casos previstos na Lei, é ilegal copiar qualquer peça de software, a menos que expressamente permitido pelo legal detentor dos direitos de autor. Posto isto, é indicado que o seu não cumprimento poderá acarretar consequências legais. É proibida a reprodução de software. É também proibido proporcionar o acesso a qualquer software do Município a terceiros, assim como trazer software de fora das instalações municipais e instalá-lo em qualquer computador do Município.

A parte intitulada "Utilizadores de Hardware" define que o hardware é um activo da Câmara Municipal e não de determinado serviço ou departamento, que são os usufrutuários deste tipo de activos. É definido que a divisão de informática é o gestor interno destes activos. É proibido o transporte de hardware de fora das instalações municipais e instalá-lo em qualquer computador do Município, assim como não levar o hardware para fora das instalações ou instalá-lo nos computadores pessoais dos utilizadores e é também indicado que todos os computadores do Município serão auditados regularmente de modo a manter actualizado o registo de bens móveis do Município.

A parte intitulada por "Utilização de Email" estipula comportamentos a observar ou a evitar na utilização dos recursos informáticos. Restrições na utilização do correio electrónico são listadas, nomeadamente no diz respeito à proibição do envio ou recepção de material como cadeias de solidariedade; pirataria e terrorismo; mensagens cujo conteúdo esteja relacionado com actividades ilegais; pronúncias indistintas étnicas, religiosas, ou raciais; mensagens cujo conteúdo reflicta a intenção de obter proveitos financeiros pessoais e mensagens sexualmente explícitas ou caricaturas e mensagens. Em virtude do email não ser um meio de comunicação seguro e inviolável, torna-se fundamental declarar abertamente que tal meio de comunicação poderá não ser confidencial e que o Município não poderá ser responsabilizado por danos causados pela não inviolabilidade do email.

A parte designada por "Utilização de Internet" inicia-se com a especificação de que o Município providenciará acesso à Internet aos seus funcionários e colaboradores em função das tarefas a desempenhar no âmbito das suas actividades profissionais na Câmara Municipal, especificadas pelos respectivos dirigentes. Recomendações, proibições e responsabilidades para o seu uso são aqui definidas. Como exemplo de uma recomendação é a de que o utilizador encerre a sua sessão sempre que se ausentar do seu local de trabalho. Como exemplo de responsabilidade é o de que responsabiliza o utilizador de descarregar qualquer ficheiro da Internet ou capturar qualquer imagem que é exibida. Como exemplo de proibições apontam-se:

- O utilizador envolver-se em qualquer actividade ilegal enquanto usa a Internet;

- Participar em jogos *on-line* ou ter canais activos incluindo qualquer canal de conversação que transmite constantes actualizações frequentes no computador;
- Visitar *sites* na Web que exibam conteúdos de natureza pornográfica ou que contenham material que possa ser considerado ofensivo.

A parte intitulada por "Utilização dos serviços de comunicação móveis" é composta por cinco pontos, que abordam aspectos como roubo, extravio e má utilização; atribuição de *kits*, auriculares, *bluetooth* e outros acessórios adicionais; atribuições de telemóveis *triband*; atribuição por mudança de gama de telemóveis e telemóveis em garantia. Recomendações e orientações em relação a estes aspectos na utilização dos serviços de comunicação móveis são aqui definidas, designadamente de que no caso de roubo terá que ser enviada ao gabinete de informática cópia da participação do mesmo às autoridades e de que sempre que um equipamento estiver dentro do prazo de garantia não será atribuído um novo telemóvel. O equipamento será reparado sempre que possível, desde que não implique custos adicionais para a Câmara Municipal.

Componentes em falta

Face à análise efectuada ao documento é possível apontar uma série de aspectos que foram preteridos, nomeadamente a não definição de quem inicia e mantém a política de SSI e a definição do responsável pela segurança da informação no Município. Também não é feita claramente a identificação dos destinatários do documento.

Outras omissões que se verificam nesta política são a inexistência da definição de sanções que a Autarquia possa impor a quem não cumprir com o estipulado no documento e por último, mas não menos importante, a não definição na política de SSI do seu propósito e dos seus objectivos.

Caso 14

Conteúdo do documento

A folha de rosto do documento contém o logótipo da Câmara, a designação completa da Câmara, o título do documento e o texto para a deliberação de aprovação do Regulamento de utilização de equipamento informático. O conteúdo do texto de deliberação tem como subtítulo "Regras para equipamento informático" e o seguinte conteúdo "Na sequência da necessidade de criar uma Norma de Equipamentos Informáticos na Câmara Municipal de … é definido um conjunto de princípios e de regras para utilização de equipamento atribuído pela autarquia a colaboradores, conforma documento anexo". Findo o texto é indicada a data e o local para a assinatura do Presidente de Câmara.

A página de título apresenta o logótipo e designação da Câmara Municipal, o título do documento e a data.

A parte intitulada "Objectivos" indica que a presente política de equipamentos informáticos visa definir os termos e condições de atribuição de material informático

da autarquia aos seus colaboradores elegíveis no âmbito desta regulamentação e a sua utilização.

A parte designada de "Universo de Aplicação" define que os princípios e normas definidos neste documento respeitam à utilização de equipamento informático na Câmara Municipal.

A parte designada por "Elegibilidade" define como elegíveis para atribuição de computador da Autarquia, os colaboradores a quem esteja atribuída uma função à qual tenha sido reconhecida a necessidade do uso de ferramentas informáticas. A atribuição será feita depois da devida autorização da chefia e validada pela Direcção Municipal de Tecnologias de Informação, Modernização Administrativa e Manutenção.

A parte designada por "Natureza da Atribuição" é composta por três pontos, e foca aspectos como a definição de que a concessão de equipamento informático da autarquia deverá ser fundada no factor "função" e não no factor "pessoa" e a obrigatoriedade de entregar o equipamento sem reservas caso o colaborador cessar o motivo pelo qual o equipamento foi atribuído ao colaborador.

A parte intitulada por "Características dos Equipamentos Informáticos" define que o equipamento poderá ser novo ou existente. A parte de atribuição de portáteis é também abordada, bem como a atribuição de um monitor externo. É também indicada a obrigatoriedade de todos os equipamentos da Câmara Municipal serem identificados através de uma etiqueta de inventário.

A parte designada por "Condições de Utilização" é composta por cinco pontos, onde responsabilidades, restrições e comportamentos a adoptar por parte dos utilizadores são descritos. É atribuída à Direcção Municipal de Tecnologias de Informação, Modernização Administrativa e Manutenção a responsabilidade pela gestão do software instalado no equipamento; de poder levar a cabo auditorias aos equipamentos que entender necessárias para garantir que o software instalado está devidamente legalizado. Os colaboradores a quem foi atribuído um equipamento são responsáveis por garantir o seu bom tratamento e conservação; os colaboradores a quem foi atribuído um portátil, em particular, são responsáveis por:

- Assegurar a confidencialidade da informação presente no equipamento, o que inclui transportá-lo de uma forma segura;
- Recorrer aos serviços da Divisão de Informática para assegurar que sejam efectuados salvaguardas à informação do equipamento, quando solicitado;
- Verificar a actualidade do software de antivírus ligando-se, pelo menos, uma vez por semana à rede da Câmara, ou à Internet para esse efeito.

A parte intitulada de "Custos Inerentes à Atribuição de Equipamento Informático" designa como inerentes à atribuição de equipamento informático e, como tal, suportados pela Câmara, todos os custos imputáveis ao funcionamento e utilização normal do equipamento.

A parte designada de "Aceitação formal" define que a partir da data de aprovação deste documento só serão entregues equipamentos com aceitação formal destas condições de utilização.

Por último, o "Anexo A", intitulado "Regulação dos Conteúdos Aceitáveis", proíbe a circulação de certos conteúdos na rede da Câmara Municipal, nomeadamente ficheiros multimédia que não sejam necessários ao exercício da função profissional, programas ou ficheiros de instalação de software não aprovados e que não estejam devidamente licenciados e de conteúdos que invalidam os princípios de integridade, ética e responsabilidade social desta Câmara Municipal.

É definido também neste anexo a aplicabilidade do descrito no parágrafo anterior, que afecta a utilização de espaço em disco de todos os equipamentos informáticos da Câmara Municipal e dos seguintes serviços: área partilhada, sistema de e-mail, pastas públicas de e-mail, áreas pessoais na rede e salvaguarda dos portáteis.

Este anexo termina com a definição dos responsáveis pela implementação da norma. A confidencialidade da informação é também tida em conta, bem como, a definição em relação às possíveis alterações. A norma poderá ser alterada a qualquer altura e todas as subsequentes alterações serão devidamente comunicadas, no portal de normas da Direcção Municipal de Tecnologias de Informação, Modernização Administrativa e Manutenção.

Componentes em falta

O Documento que se analisa no Caso 14, no que diz respeito às suas componentes, apresenta uma estrutura simples, focando aspectos como de quem é a responsabilidade por implementar e manter a política de SSI, contudo não é feita claramente a identificação dos destinatários do documento.

Outras omissões que se verificam nesta política são a inexistência da definição de sanções que a Autarquia possa impor a quem não cumprir com o estipulado no documento.

Caso 15

Conteúdo do documento

A informação interna tem o número da informação, o ano e quem a emitiu (o Gabinete de Gestão de Sistemas de Informação). O Assunto merece destaque também nesta informação que é: Proposta de alteração a "Normas de Degurança e Funcionamento dos Sistemas de Informação do Município de …". Para além da identificação do assunto, contém um parágrafo com um texto que submete à apreciação superior a presente proposta. Esta informação é assinada pelo técnico de informática. No cabeçalho da informação tem dois espaços, um com o parecer que manuscritamente tem um despacho a ser enviado para o Gabinete de Gestão de Sistemas de Informação (GGSI) com conhecimento para o Gabinete da Qualidade, Avaliação e Modernização Administrativa (GAQ) de "Está aprovada" com a assinatura não legível e a data, e outro com o despacho assinado e datado e com indicação de que o documento foi entregue as GAQ.

A folha de rosto tem no centro o nome das Normas e no rodapé o nome do GGSI e o mês e o ano. Seguem-se duas páginas de Índice com a descrição de todos os capítulos e pontos do documento.

O Capítulo 1, denominado por "Introdução", realça a importância dos sistemas de informação e dos recursos que lhe estão associados. Essa importância tem cada vez mais um papel relevante no funcionamento das organizações, assim, é indispensável garantir um nível de responsabilização e controlo sobre os diferentes componentes de forma a prevenir e minimizar os potenciais riscos.

O Capítulo 2, designado por "Responsabilidades do Gabinete de Gestão de Sistemas de Informação e do Pessoal de Informática", destaca que a segurança informática deve resultar da verificação das regras de controlo interno e, especialmente, da responsabilização. Por isso, é indispensável clarificar as atribuições e responsabilidades que cabem ao GGSI e ao pessoal da carreira de Informática. As competências do GGSI estão definidas no Artigo 18º do Regulamento da Estrutura, Organização e Quadro de Pessoal da Câmara Municipal de …, e as áreas, conteúdos funcionais, funções e tarefas inerentes ao pessoal da carreira de informática estão definidas no Decreto-Lei n.º 97/2001, de 26 de Março e Portaria n.º 358/2002, de 3 de Abril.

O Capítulo 3, intitulado "Instalações Físicas do Gabinete de Gestão de Sistemas de Informação", é composto por nove pontos, que abordam aspectos, como o estabelecimento de áreas de segurança para efeitos de controlo e responsabilização, nomeadamente o *Data Center* e o GGSI e o seu responsável, que é o Coordenador Técnico do GGSI. A área ocupada pelo *Data Center* é considerada reservada e deverá manter-se sempre fechada, a área ocupada pelo GGSI é considerada igualmente reservada e deverá manter-se fechada fora das horas de serviço. Os equipamentos vitais para manter o sistema informático em funcionamento deverão estar ligados a unidades de alimentação ininterrupta do *Data Center*, que garantem o seu funcionamento, em caso de falha inesperada da energia. A área do *Data Center* deverá ter as condições de temperatura e humidade que não interfiram com o seu funcionamento normal. Estes locais têm de ter em conta o risco de incêndio e a não existência de radiações electromagnéticas, para tal tem de possuir sistemas de extinção adequados. As instalações do GGSI devem possuir um espaço protegido contra fogo e acessos não autorizados para guardar as cópias de segurança e dos dados, bem como informação considerada confidencial. Um exemplar das cópias de segurança deverá também ser guardado fora da organização.

O Capítulo 4, intitulado "Hardware (Suportes Físicos)", é composto por nove pontos. Por "suportes físicos" entende-se todos os equipamentos susceptíveis de recolher, armazenar, processar ou transportar dados. Os cuidados mais importantes a ter com os suportes físicos são os seguintes:

- O equipamento informático deverá ser convenientemente inventariado pelo GGSI. O GGSI manterá ainda uma base de dados actualizada de todo o equipamento informático e software instalado, endereços atribuídos, chaves do software instalado, datas de aquisição, fornecedores e localização.
- Os equipamentos de comunicação deverão ser verificados periodicamente para evitar ligações fora do controlo do GGSI.

- O plano de passagem dos cabos e nós de ligação da rede deve ser mantido actualizado.
- A manutenção dos equipamentos só pode ser feita por pessoal autorizado pelo GGSI. O GGSI efectuará, mensalmente, uma verificação periódica da configuração e funcionamento dos equipamentos, da qual elaborará o respectivo relatório.
- Os computadores portáteis deverão ser devidamente guardados e transportados. Os computadores não deverão ser desligados durante a execução de qualquer tarefa. Os equipamentos informáticos não devem estar expostos à acção directa dos raios solares de forma continuada.
- Não é permitida a ligação de equipamentos dos quais a Câmara não seja proprietária ao sistema informático do Município.

O Capítulo 5, designado por "Software de Sistema", é composto por sete artigos. Por "software de sistema" entende-se o sistema operativo, software de comunicações, de gestão de base de dados e outros necessários para suportar as aplicações instaladas. O software de sistema merece cuidados especiais porque é a base do sistema informático, tais como:

- Apenas o pessoal do GGSI está autorizado a instalar e configurar software.
- A utilização do software de sistema será constantemente monitorizada, com vista a determinar se os utilizadores estão de facto a utilizar só os processos para os quais dispões de acesso autorizado.
- O código de acesso de cada utilizador deverá revelar o mínimo de informação para não incentivar acessos não autorizados.
- O sistema poderá obrigar à alteração de palavra passe após determinado período.
- O sistema deverá invalidar o acesso à rede ou sistema após um certo número de tentativas inválidas.
- O software de base adquirido deve garantir as orientações estabelecidas pelo GGSI, para evitar custos desnecessários e evitar a sua utilização abusiva.
- Não é permitida a instalação de software sem prévia autorização do GGSI.

O Capítulo 6, denominado por "Software Aplicacional", é composto por seis pontos. Por "software aplicacional" entende-se todos os programas associados ao processamento de um determinado tipo de dados (contabilidade, tesouraria, pessoal, etc.), independentemente de ser adquirido ou desenvolvido na organização. De entre as disposições destacam-se:

- O tipo de acesso às aplicações deve ser atribuído tendo por base o tipo de função desempenhada pelo respectivo utilizador.
- Os utilizadores não devem alterar a configuração dos computadores e dos programas instalados, de forma a garantir a necessária compatibilidade entre os sistemas e a facilidade de actualização e utilização.
- O GGSI elabora e assegura a actualização da "Relação de acessos a aplicações", onde se encontram identificados os utilizadores e os respectivos níveis de acesso que lhes foram atribuídos por aplicação.
- A criação e alteração da estrutura de bases de dados deve ser efectuada exclusivamente por um técnico do GGSI.
- O desenvolvimento de software deverá ser precedido da definição dos objectivos e requisitos do projecto por parte do colaborador requerente da

aplicação, requer solicitação formal ao Vereador do Pelouro e carece da aprovação.
- A instalação e actualização das aplicações de antivírus são asseguradas pelo GGSI.

O Capítulo 7, intitulado "Dados", é composto por dez pontos. A integridade e actualização dos dados dependem, ainda que não exclusivamente, da forma como são manipulados e da segurança dos meios tecnológicos que os processam. De entre as disposições realçam-se as seguintes:

- A recolha e alteração de dados deverão ser sempre controladas pelos responsáveis das unidades orgânicas a quem compete o controlo da informação.
- Os servidores de ficheiros do Município contemplam as seguintes áreas: Acesso reservado, Autarquia e Partilha. A reposição dos dados e ficheiros, em caso de falha, é da responsabilidade do pessoal do GGSI, recorrendo aos últimos dados salvaguardados.
- A informação contida nos discos dos computadores pessoais é da responsabilidade dos utilizadores.
- Os dados confidenciais deverão ser sempre que possível objecto de cuidados especiais de segurança, designadamente cifra através de software adequado.
- As transferências de dados de uma máquina para outra ou de um suporte para outro devem ser sempre do conhecimento dos responsáveis pela informação transferida.
- A salvaguarda de dados deverá ser feita em condições de segurança e deve existir sempre um plano de recuperação definido, juntamente com a identificação de quem deve actuar e das tarefas respectivas em caso de emergência.
- O GGSI condicionará os acessos aos servidores de forma a ter em conta a propriedade e a responsabilidade de alteração dos dados, bem como a necessidade de os utilizar decorrente das funções exercidas na organização. Os privilégios de acesso às aplicações deverão ser revistos sempre que o funcionário mude de unidade orgânica ou deixe de ter vínculo contratual à organização.

O Capítulo 8, denominado por "Política se Acesso", é composto por dois pontos (Acessos e ligações e Serviços de comunicações contratados). Relativamente à politica de acessos de e para o exterior, deverão ser instituídos sistemas de controlo na rede que garantam segurança dos sistemas, dos dados e dos serviços disponíveis, contra acessos não autorizados.

O Capítulo 9 – "Utilização dos Sistemas" é composto por onze pontos. Este capítulo determina que deverão existir mecanismos de autenticação, autorização e contabilização de utilizadores que permitem impedir utilizações indevidas dos sistemas informáticos do Município. A utilização dos sistemas deve ser monitorizada periodicamente com vista à detecção e correcção de qualquer situação anómala. De entre os aspectos versados realçam-se os seguintes:

- Os computadores pessoais são da responsabilidade do pessoal a quem estão afectos ou que os utilizam regularmente. Quando se trate de equipamentos de uso colectivo ficam à guarda do coordenador da unidade orgânica onde estão colocados.

- O pessoal de informática está especialmente obrigado ao dever de sigilo e à não divulgação dos dados sensíveis a que tenha acesso no exercício das suas funções.
- Deverá ser assegurada a protecção jurídica dos programas de computador e dos dados pessoais nos termos da lei aplicável em vigor.
- Qualquer anomalia no funcionamento de equipamento informático, software ou rede deverá ser sempre comunicada ao GGSI.
- Todos os utilizadores terão um nome utilizador único e exclusivo, para assim garantir que a utilização e as alterações introduzidas possam ser associadas inequivocamente ao seu possuidor, para além disso, terão uma *password* pessoal e intransmissível por cada utilizador.
- Poderá ser condicionado o acesso ao sistema informático do Município fora das horas de trabalho sempre que seja necessário por motivos que o justifiquem.
- Os utilizadores deverão sempre desligar as estações de trabalho. Não devem abandonar o computador se este estiver ligado à rede sem terminar as sessões de trabalho ou sem ter procedido ao respectivo bloqueio.
- Os computadores portáteis deverão ter o modo *stand-by* activado, ou pelo menos o dispositivo de bloqueio do teclado e apagamento do ecrã, através da respectiva combinação de teclas, quando disponível.

Componentes em falta

Está claramente identificada a aprovação das normas, bem como a data em que foram aprovadas, contudo a assinatura não é legível, não se podendo indicar e precisar por quem foram aprovadas.

Não há qualquer referência a sanções que a organização possa impor a quem não cumprir aquilo que o documento estabelece.

Caso 16

Conteúdo do documento

A primeira parte do documento menciona que para contribuir para o regulamento do sistema informático da Câmara Municipal o funcionário é informado sobre alguns procedimentos. O funcionário devidamente identificado assina no final o documento comprovativo de como tomou conhecimento. A identificação do funcionário tem o seu nome. A identificação do equipamento com que o utilizador habitualmente trabalha é também feita com a indicação do seu nome, número de inventário e o serviço onde está localizado.

A segunda parte deste documento refere as obrigatoriedades que o funcionário que vai assinar o documento tem. As obrigatoriedades são: guardar todos os documentos de serviço na pasta que lhe está destinada no computador pessoal; diariamente executar a rotina de cópia dos ficheiros para o servidor para efeitos de *backup* e por último, semanalmente executar a aplicação *anti-spyware*.

Na terceira parte deste documento é mencionado para conhecimento, o software que fica instalado no computador do utilizador. O utilizador assina o termo de aceitação e de conhecimento do documento.

Na quarta e última parte deste documento está referenciado que o utilizador tomou conhecimento e a data em que assinou este termo de aceitação.

Componentes em falta

O documento que se analisa no Caso 16, no que concerne às suas componentes, apresenta uma estrutura bastante simples. A indicação de quem contactar em caso de dúvidas não é feita, não sendo indicado quem contactar para o envio de sugestões de actualização, pedidos de excepção ou comunicação de incidentes detectados.

Outra omissão é não estar feita a identificação dos destinatários do documento dentro de toda a autarquia, contudo é feita a identificação nominal, uma vez que o destinatário individualmente tem de assinar o documento.

Outra omissão no documento analisado, é a falta de identificação do objectivo e propósito da política.

Na política de SSI em análise não há qualquer referência a sanções que a Câmara Municipal possa impor a quem não cumprir aquilo que o documento estabelece. O documento é meramente informativo, não responsabilizando explicitamente os utilizadores sobre nada em concreto. Nota-se, no entanto, que o facto de o utilizador assinar o documento atestando a sua aceitação e conhecimento do mesmo, pode subentender a possibilidade de uma qualquer sanção em caso de incumprimento.

O documento é omisso também na identificação de quem o aprovou e em que data, bem como em muitos aspectos que normalmente são abordados quando estamos a tratar da SSI, muito pelo facto de se tratar de um documento com uma dimensão bastante reduzida e de abrangência limitada.

Caso 17

Conteúdo do documento

O documento inicia-se com um "Preâmbulo", onde se define o objectivo do regulamento, seguindo-se algumas proibições, como por exemplo: a proibição de aceder ou transmitir mensagens com relevância criminal ou de carácter injurioso, ofensivo ou discriminatório e proibição do abuso de utilização dessas comunicações para fins pessoais.

O Artigo I, denominado por "Âmbito", menciona a quem se aplica o presente regulamento, que são os funcionários do quadro, agentes, contratados ao abrigo de contrato individual de trabalho e aos colaboradores em regime de prestação de serviços. É indicado também neste artigo que o regulamento rege todas as comunicações ou transmissões de dados efectuados por telefone, correio electrónico ou outras formas de transmissão de dados por via telemática e o acesso à Internet.

O Artigo II, designado por “Deveres dos Utilizadores”, define quem são os utilizadores, que correspondem aos definidos no artigo anterior e um conjunto de deveres afectos aos utilizadores dos meios de comunicação ou de transmissão de dados, tais como:

- Zelar pela boa conservação dos equipamentos que lhe forem atribuídos.
- Assegurar a integridade e a actualização dos dados que tenha o dever de tratar profissionalmente.
- Manter sigilo profissional em relação a todos os dados pessoais de que tenha conhecimento.
- Não aceder ou transmitir mensagens com relevância criminal ou de carácter injurioso, ofensivo ou discriminatório.

O Artigo III, denominado por “Direitos dos Utilizadores”, define que os utilizadores dos meios de comunicação ou de transmissão de dados têm direito a:

- Aceder aos meios de comunicação e de transmissão de dados necessários ao exercício das suas funções profissionais.
- Possuir um código e uma senha pessoal e possuir uma caixa de correio electrónico.

O Artigo IV, designado por “Administradores do Sistema Informático e das Bases de Dados”, define estes papéis como os trabalhadores aos quais caiba, por força de funções expressamente atribuídas ou do respectivo contrato individual de trabalho ou de prestação de serviços, supervisionar e coordenar o funcionamento e a utilização do sistema informático e das bases de dados.

O Artigo V, designado por “Coordenador do Gabinete de Informática e Telecomunicações”, estabelece o que compete e este Coordenador, onde se destaca:

- Transmitir e fazer cumprir todas as directivas e instruções do órgão executivo do Município respeitantes ao sistema informático, às bases de dados e aos sistemas de telecomunicações.
- Promover todas as medidas organizativas e técnicas necessárias ao bom funcionamento do sistema informático, à integridade e segurança das bases de dados e a fidedignidade e correcta utilização dos dados pessoais, bem como ao planeamento, gestão e implementação necessários ao sistema informático.

O Artigo VI, intitulado “Entrada em Vigor”, define que o presente regulamento interno entra em vigor no primeiro dia útil seguinte ao da deliberação de aprovação pela Câmara Municipal.

Componentes em falta

O regulamento analisado, no que concerne às suas componentes, apresenta uma estrutura bastante simples. Não é referido o responsável pela manutenção do documento. Outras omissões no conteúdo do documento podem ser observadas, designadamente a do Propósito do documento e a falta de identificação da entidade que aprovou o regulamento, embora se possa subentender pelo exposto no Artigo VI que tenha sido em reunião ordinária da Câmara Municipal.

Caso 18

Conteúdo do documento

A parte intitulada "Introdução", constituída por três pontos, define que as presentes normas existem para dar cumprimento com o definido na alínea f) do n.º 3 da Introdução do Sistema de Controlo Interno e do ponto 2.9.2, alínea h) das considerações técnicas do POCAL (Plano Oficial de Contabilidade das Autarquias Locais), define ainda as consequências da falta de segurança dos dados e que as regras e procedimentos constantes no documento devem visar a segurança do sistema informático.

O capítulo I, intitulado "Disposições Gerais", é composto por cinco artigos. O primeiro artigo é designado por "Âmbito de Aplicação" e define que o presente documento é aplicável a todos os serviços da Autarquia.

O segundo artigo é denominado "Objectivos" e contém o enunciado de dois grandes objectivos:

- Garantir que o tratamento dos dados e programas permita a obtenção de informação permanentemente actualizada e em conformidade com os elementos que lhe deram origem.
- Responsabilizar, aos diferentes níveis, os intervenientes no sistema pela protecção de dados e programas, instalações, material informático, do pessoal, das comunicações e de outras actividades que ponham em causa a segurança das aplicações, a integridade da informação e a continuidade dos trabalhos.

O terceiro artigo é designado de "Competências", sendo composto por três pontos, que abordam aspectos como a quem compete aprovar e manter em funcionamento as presentes Normas, que é o órgão Executivo, define também de quem é a responsabilidade pela implementação, apoio, coordenação, fiscalização e controlo das normas e procedimentos estabelecidos nestas Normas, que é o departamento de informática, e a quem compete dar cumprimento às normas definidas no documento, que é às direcções de departamento de divisão e de secção, dentro das respectivas unidades orgânicas.

O quarto artigo é designado de "Regras básicas" e é composto por três pontos, onde se podem destacar duas abordagens, uma que define contra o que os dados e programas devem ser convenientemente protegidos, designadamente contra indiscrições, fugas, violações ou descuidos, e outra que define a quem se restringe o acesso a dados, programas e aplicações informáticas, nomeadamente os funcionários com efectiva necessidade de acesso para cumprimento e desempenho das suas funções.

Por último, o quinto artigo, que é designado de "Administração de recursos", é composto por três pontos, que focam aspectos como por exemplo:

- Compete ao Chefe/Responsável do Centro de Informática, Sistemas e Telecomunicações atribuir as tarefas e responsabilidades do pessoal do Centro.

- A atribuição de responsabilidades e de tarefas deverá ser determinada e gerida de forma a salvaguardar a continuidade dos serviços.
- A gestão dos recursos deverá garantir, permanentemente, o apoio às unidades orgânicas na utilização da informação, das ferramentas e das aplicações existentes, assim como, a disponibilidade, coerência e qualidade dos dados necessários ao sistema de informação.

O capítulo II, designado "Segurança Física", é composto por quatro artigos. O primeiro artigo é intitulado de "Instalações" e está subdividido em três grandes pontos: Edifícios, Energia Eléctrica e Climatização. O primeiro ponto aborda as características que a localização do Centro de Informática, ou qualquer equipamento de arquivo de informação central (Servidores) e o espaço, bem como, o espaço físico destinado à unidade central de periféricos, devem ter. O segundo ponto define como a rede de energia eléctrica deverá ser instalada. O terceiro ponto define as condições que o sistema de climatização deve respeitar.

O segundo artigo menciona os tipos de serviços que os contratos de manutenção devem contemplar de forma a garantir a funcionalidade do equipamento informático. São definidas também as responsabilidades do Centro de Informática em matéria de reparações.

O terceiro artigo do Capítulo dois aborda em termos gerais um conjunto de pontos que um contrato de manutenção deve contemplar.

O último artigo deste capítulo define as ligações que o Centro de Informática deve ter com a Secção de Património e vice-versa, de forma a manter actualizada a informação respeitante ao inventário do equipamento.

O capítulo III, intitulado "Aquisição de Hardware", é composto por um artigo que se designa de "Aquisição" que é dividido em quatro pontos. O primeiro ponto define os artigos do Sistema de Controlo Interno a ter em conta para a aquisição de equipamento informático. O segundo ponto define que na aquisição de hardware deverá garantir-se a adequação do equipamento às necessidades efectivas dos utilizadores. O terceiro ponto aborda a forma como os pedidos/requisições internas devem ser fundamentadas pelos respectivos requisitantes. O quarto e último ponto define um conjunto de responsabilidades afectas ao Centro de Informática para o processo de aquisição, nomeadamente de equipamento informático de maior complexidade.

O capítulo IV, intitulado "Aquisição, Desenvolvimento e Manutenção de Software", é composto por sete artigos. O primeiro designado "Aquisição de Software" é subdividido em dois pontos, focando o primeiro que na aquisição de software tem de se salvaguardar a adequação e manutenção do produto, o segundo ponto tem doze alíneas onde está definido o que o Centro de Informática deve fazer para garantir o estipulado no ponto anterior.

O segundo artigo, designado por "Desenvolvimento de software", descreve um conjunto de procedimentos mínimos que o Centro de Informática deve respeitar no desenvolvimento de projectos informáticos.

O terceiro artigo é denominado “Documentação de suporte” e define as medidas a implementar, indicando o mínimo de documentação que haverá obrigatoriamente existir em cada aplicação, bem como, a divulgação da documentação e a manutenção de toda a documentação actualizada.

No quarto artigo deste capítulo, que se designa por “Manutenção do software”, é descrito um conjunto de pontos que salvaguardam a integridade e continuidade dos trabalhos informáticos. Um conjunto de responsabilidades, alocadas ao Centro de Informática, são descritas com o intuito de garantir o bom funcionamento das aplicações.

O quinto artigo, designado por “Segurança do software”, define que de forma a garantir a continuidade dos trabalhos e a existência de um histórico de toda a informação relevante, designadamente ficheiros, base de dados, de programas e aplicações, deve existir um plano de segurança do sistema informático. Nesse sentido, um conjunto de medidas são descritas de forma a tornar esse plano eficaz, nomeadamente: os ficheiros a copiar, o momento em que deve ser efectuada a sua cópia, como proceder à recuperação da informação sempre que situações de erro ou avaria obriguem à sua reposição e definição da periodicidade das cópias de segurança.

O sexto artigo, designado por “Reposição de cópias de segurança”, define quando se deve recorrer às normas e procedimentos de recuperação. A reposição da informação é feita sempre que surjam incidentes, como por exemplo: avarias de equipamento, avarias de climatização ou de energia eléctrica, destruição de ficheiros e erros de programação.

O último artigo deste capítulo, designado por “Processamentos pesados”, define que compete ao Centro de Informática manter actualizada a listagem dos processamentos que mais recursos necessitam quando executados, tipificando-os de acordo com o grau de afectação no desempenho do sistema informático e referindo: quem os pode executar, em que condições devem ser iniciados, a periodicidade da sua execução e os procedimentos pré e pós-processamento.

O capítulo V, intitulado “Controlo de acessos”, é composto por três artigos. O primeiro é o artigo 18º, denominado “Palavra chave”, estabelece a associação de uma *password* a um utilizador, através da tipificação dos acessos com as devidas autorizações superiores, conselhos e recomendações para ser garantida a exclusividade da *password* e a forma para o utilizador poder alterar esse código de acesso.

O segundo artigo deste capítulo é definido como “Detecção de anomalias” e é composto por cinco pontos que abordam: como devem ser controladas as anomalias ou infracções às regras de uso e acesso ao sistema, através de avaliações à utilização do sistema informático e elaboração de relatórios descrevendo as situações anómalas detectadas.

O terceiro artigo, designado por “Acesso à informação”, define que o acesso à execução, consulta e/ou recolha de informação das bases de dados constante dos

equipamentos de arquivo de informação central (servidores) é exclusiva dos utilizadores autorizados para o efeito.

Por último, o capítulo VI – "Disposições Finais" – é composto por três artigos, o primeiro, designado por "Delegação de funções", define que o Centro de Informática poderá delegar responsabilidades sempre que considere que, tendo em conta a especificidade das tarefas, o serviço a co-responsabilizar reúne as condições técnicas necessárias e capacidades para desempenhar as tarefas de forma eficiente.

O segundo artigo, denominado "Alterações", define que estas normas podem ser alteradas por deliberação do Órgão Executivo, sempre que as razões de eficácia, segurança ou outras o justifiquem. Define também que é da responsabilidade do Centro de Informática recolher informações e contribuições, analisá-las e formular propostas de alteração e renovação das Normas de Controlo Interno das Aplicações, que visem o aumento de eficácia e segurança do sistema informático.

O terceiro e último artigo define que esta norma revoga todas as normas internas e ordens de serviço anteriores na parte em que contrariem as regras e procedimentos estabelecidos no presente documento. A indicação da data em que vai entrar em vigor é também aqui referenciada.

Componentes em falta

A política em análise no Caso 18 é mais específica no que diz respeito á parte tecnológica. Considerando que é um documento que inclui as directivas da Autarquia em matéria de Ambiente Informático, nota-se a omissão da identificação de sanções que o Município possa impor aos utilizadores. Falta também a identificação da entidade que aprovou o documento, bem como a data de aprovação.

Caso 19

Conteúdo do documento

A parte intitulada "Exposição de Motivos" define que as Regras de Uso dos Computadores foram formuladas para evitar práticas de reprodução e utilização ilegal de software, conforme previsto no Código dos Direitos de Autor, bem como na Lei n.º 109/91, de 28 de Agosto. É também referido que estas Regras são "obrigatórias para todos os funcionários ou terceiros devidamente autorizados a aceder a qualquer sistema informático ou manipulado pelo Município". O último parágrafo deste ponto define a finalidade destas Regras que é "proteger os utilizadores do Município de todas as ameaças, quer internas ou externas, deliberadas ou acidentais e satisfazer todas as exigências regulamentadas e/ou legisladas".

O capítulo I, intitulado "Disposições Gerais", é composto por quatro artigos. O primeiro artigo é designado por "Software protegido pelos direitos de autor", sendo composto por dezassete pontos, que focam aspectos como por exemplo:

- É ilegal copiar qualquer peça de software a menos que expressamente permitido pelo legal detentor dos direitos de autor.

- Nenhum funcionário da Câmara Municipal deverá fazer ou executar de qualquer forma cópias de qualquer software.
- O Presidente da Câmara Municipal não tolerará o uso de cópias não autorizadas de software. Qualquer funcionário que reproduza software ilegalmente ficará sujeito às penalidades criminais, civis e disciplinares que daí possam advir, as quais podem incluir multas ou prisão, além do respectivo procedimento disciplinar.
- É interdito a qualquer funcionário proporcionar o acesso a qualquer software pertença do Município a qualquer estranho.
- Todo o software deve ser proposto pelo Gabinete de Informática, que instalará os programas nos computadores designados ou nos servidores.
- O Gabinete de Informática ficará responsável pelo registo e actualização de todo o software conforme fornecido pelos respectivos fornecedores, instalando as actualizações consoante venham a ser disponibilizadas, mantendo o controlo de todas as versões disponíveis no Município.
- Não é permitido aos funcionários/utilizadores trazer software do exterior e instalá-lo em qualquer computador do Município.
- O software do Município não deve ser levado para o exterior e instalado nos computadores pessoais dos funcionários/utilizadores.
- Todos os computadores do Município serão auditados regularmente, pelo Gabinete de Informática. Havendo software ilegal no computador de um funcionário/utilizador será o mesmo removido no momento e elaborada uma participação ao Presidente da Câmara Municipal a fim de serem apuradas as responsabilidades do respectivo funcionário/utilizador.

O segundo artigo é designado de “Segurança”, sendo composto por catorze pontos, que abordam aspectos como por exemplo:

- Os utilizadores não podem revelar qualquer informação relativa às facilidades das Tecnologias de Informação do Município perante qualquer pessoa ou entidade exterior, sem a autorização expressa do Director de Departamento Administrativo Jurídico e Financeiro e mediante parecer do Gabinete de Informática.
- A todos os utilizadores de computadores são consignados um nome de utilizador e uma *password* que são únicas e que não devem ser partilhadas com qualquer outro utilizador.
- As *passwords* não devem ser escritas, ou deixadas onde outros as possam encontrar, apenas o Gabinete de Informática terá acesso às mesmas e o respectivo utilizador. As *passwords* devem ser mudadas em intervalos regulares (não é especificada a periodicidade para a alteração).
- Os utilizadores não devem deixar um computador ligado à rede com a sessão aberta quando se ausentam.
- É considerado crime tentar ter acesso deliberado a um sistema para o qual não tenha autorização.
- O Gabinete de Informática verifica regularmente todos os sistemas e eventuais tentativas de acesso não autorizado aos mesmos. Qualquer tentativa de acesso não autorizado é investigada.
- Os utilizadores devem fazer periodicamente cópias de segurança das suas informações (não é especificada a periodicidade com que devem ser feitas).

- A responsabilidade de todos os dados que se encontram nos servidores de rede é do Gabinete de Informática, que assegurará que as cópias de segurança serão executadas regularmente e armazenadas em local seguro.
- Só a funcionários afectos ao Gabinete de Informática é permitido mover qualquer equipamento, dentro ou fora dos serviços ou para outro local.
- Nenhum dispositivo periférico de qualquer tipo (máquinas fotográficas digitais, PDA's, etc.) podem ser instalados ou configurados em qualquer computador do Município, sem o devido conhecimento do Gabinete de Informática.

O terceiro artigo é designado de "Correio Electrónico", sendo composto por dezoito pontos, onde se podem destacar os seguintes:

- O uso pessoal, acidental e ocasional de correio electrónico é permitido pelo Município, com a compreensão que as mensagens pessoais serão tratadas como as mensagens profissionais.
- O uso pessoal do sistema de correio electrónico nunca deverá afectar o fluxo de tráfico normal do correio electrónico do Município. O Município reserva-se o direito de remover o correio electrónico pessoal identificável para preservar a integridade dos sistemas de correio electrónico.
- Nenhum utilizador deve usar o sistema de correio electrónico de forma a que o mesmo possa ser interpretado como um insulto ou ofensivo a qualquer outra pessoa ou funcionário, ou sob qualquer forma que possa ser prejudicial para a imagem do Município.
- É proibido incluir no sistema de correio electrónico do Município o seguinte material: Mensagens sexualmente explícitas, imagens, caricaturas ou anedotas; proposições mal recebidas, pedidos para datas ou cartas de amor; profanação, obscenidade, difamação ou calúnia; pronúncias indistintas étnicas, religiosas ou raciais; convicções políticas ou comentários; ou qualquer outra mensagem que possa ser interpretada como assédio sexual ou depreciação de outros baseado no sexo deles/delas, etnia, orientação sexual, idade, origem nacional, inaptidão ou convicções religiosas ou políticas, etc.
- Nenhuma mensagem deve ser enviada ou recebida cujo conteúdo tenha a ver com actividades ilegais.
- O sistema não pode ser utilizado para ganhos financeiros pessoais.
- É proibido o envio de cartas para cadeias de solidariedade, caridade, concursos ou outros ganhos pessoais. O correio electrónico de origem desconhecida ou de conteúdo suspeito não deve ser aberto ou reenviado para qualquer funcionário, dentro ou fora do Município, devendo ser solicitada a ajuda do Gabinete de Informática.
- O utilizador que se ligar a um computador será considerado como o autor de qualquer mensagem enviada desse computador.
- Os funcionários/utilizadores não devem abrir anexos de correio electrónico executáveis (ficheiro.exe ou ficheiro.com), a menos que conheçam o seu conteúdo.

Por último, o quarto artigo, que é designado por "Internet", é composto por onze pontos, que focam aspectos como por exemplo:

- Os utilizadores não podem colocar na Internet qualquer mensagem que possa comprometer o Município, por ser ofensiva ou abusiva, ou cujo conteúdo

contenha material considerado como proibido ou ofensivo dos bons costumes.

- Todos os sítios visitados pelos utilizadores são registados centralmente, pelo Gabinete de Informática no servidor de *proxy*.
- Os utilizadores não devem envolver-se em qualquer actividade ilegal enquanto utilizam a Internet.
- O sistema não pode ser usado para ganhos financeiros pessoais, nem poderá alojar qualquer *Website*.
- É proibida a participação em jogos *on-line* ou ter canais activos incluindo qualquer canal de conversação, como por exemplo o Messenger para uso que não seja estritamente profissional.
- Os utilizadores não devem visitar locais da *Web* que exibam conteúdos de natureza pornográfica ou que contenham material que possa ser considerado ofensivo.
- Os utilizadores não devem descarregar qualquer ficheiro da Internet, ou capturar qualquer imagem que é exibida, pois daí poderão advir problemas relativamente a direitos de autor, vírus e ao funcionamento global dos computadores.
- O utilizador que está ligado na rede será considerado como a pessoa que está a explorar a Internet.
- O utilizador deve fechar a sessão de trabalho sempre que se ausente do seu local de trabalho.
- O Município faz o controlo de todos os acessos feitos pelos funcionários reservando-se o direito de tornar público o relatório desta informação.

O capítulo II, designado por "Disposições Finais", é composto por três artigos. O primeiro artigo é intitulado de "Dúvidas e omissões" e define que todas as dúvidas de interpretação e integração de lacunas que possam surgir na implementação deste regulamento serão resolvidas de acordo com os princípios gerais de direito.

O segundo artigo aborda as responsabilidades e define que a "violação das normas do presente regulamento, sem prejuízo do previsto noutra legislação, constituiu infracção disciplinar e determina que seja instaurado, contra o seu responsável, o competente procedimento disciplinar".

O último artigo deste capítulo define a entrada em vigor do regulamento que é quinze dias após a sua publicação em Diário da República.

Componentes em falta

O regulamento em análise no Caso 19 é muito específico no que diz respeito á parte tecnológica. Considerando que é um documento que inclui as directivas da Autarquia em matéria de SSI, nota-se a omissão da identificação do responsável pela manutenção do documento. Relativamente a sanções que o Município possa impor aos utilizadores são mais do que uma vez referenciadas no texto. Não é feita a identificação da entidade que aprovou o documento, bem como a data de aprovação.

Caso 20

Conteúdo do documento

A folha de rosto do documento contém o logótipo da Câmara, a designação completa da Câmara e a deliberação de aprovação das Normas de utilização de sistemas de informação em reunião de Câmara, bem como a data de aprovação.

A parte intitulada "Utilização do equipamento informático" tem dois parágrafos introdutórios onde é apresentada a estrutura do documento e o propósito para a Autarquia das presentes normas que "visam informar todo o pessoal a prestar serviço no Município de … das suas responsabilidades no manuseamento e protecção da tecnologia e informação do Município, de forma a que todos cooperativamente possam oferecer um melhor serviço aos utentes, trabalhem com mais facilidade e por outro lado aumentem a segurança e diminuam o risco de perda de informação".

Relativamente a este primeiro ponto, é composto por oito pontos, que abordam aspectos como:

- O utilizador é responsável pelo equipamento que utiliza e a abertura do equipamento para proceder a reparações deve ser feita em local próprio e por um técnico responsável;
- O utilizador não pode proceder à ligação de novos equipamentos à rede informática sem prévio conhecimento e autorização dos Serviços de Informática;
- O utilizador não pode usar os recursos da Autarquia para tentar aceder ilegalmente a sistemas informáticos de outras instituições;
- O Utilizador não pode reproduzir ou divulgar informação armazenada nos sistemas do Município;
- O utilizador não pode instalar aplicações nem alterar a configuração das aplicações ou sistemas instalados, sem a devida autorização.

A parte designada por "Utilização da Rede" é composta por cinco pontos, e foca aspectos como a obrigatoriedade dos utilizadores terem uma senha, e os cuidados a terem em relação às suas senhas (*login* e *password*) não serem do conhecimento de terceiros e a salvaguarda para os computadores não ficarem com a sessão aberta se o utilizador se afasta do seu posto de trabalho. Um dos pontos chama a atenção para a informação colocada nos servidores ser só referente ao trabalho e nunca de âmbito pessoal e também que os utilizadores periodicamente deverão fazer a manutenção da directoria pessoal, retirando material inútil do servidor da rede.

A parte intitulada por "Utilização do Correio Electrónico (e-mail)" é composta por seis pontos, que estipulam comportamentos a observar ou a evitar na utilização dos recursos informáticos, como por exemplo que os utilizadores que têm e-mail da instituição não devem usá-lo para fins pessoais. Restrições na utilização do correio electrónico são listadas, nomeadamente no diz respeito ao envio de informação e documentos internos para o exterior que só é permitido com a devida autorização do Presidente da Câmara Municipal. Relativamente às contas de correio electrónico, aspectos referentes à sua configuração e tamanho limite para envio são aqui focados.

A parte designada por "Utilização da Internet" é composta por oito parágrafos, onde responsabilidades, restrições e comportamentos a adoptar por parte dos utilizadores são descritos. Podem-se listar as seguintes:

- É da responsabilidade de cada chefe de Divisão/Serviço aprovar os sites que os funcionários sob sua responsabilidade podem aceder;
- Os softwares de comunicação instantânea (Messenger, Sykpe, etc.) só poderão ser utilizados para fins de trabalho e autorizados superiormente;
- O acesso a *sites* com conteúdo de natureza pornográfica, racista e ofensivo é proibido;
- É proibido ouvir música, ver televisão e vídeos através da Internet;
- Os utilizadores não podem descarregar ficheiros da Internet (*downloads*) e programas informáticos, bem como fazer a sua instalação sem autorização superior.

Por último, a parte designada de "Solicitações dos utilizadores aos Serviços de Informática" descreve o modo como os utilizadores devem comunicar com o serviço de informática, para os seguintes fins: colocação de dúvidas, comunicação de avarias e necessidades e pedidos de ajudas pontuais.

Componentes em falta

Considerando que é um documento que inclui as directivas da Autarquia em matéria de SSI, nota-se a omissão da identificação do responsável pela manutenção do documento, não há qualquer referência a sanções que a Autarquia possa impor a quem não cumprir aquilo que o documento estabelece e falta uma identificação clara dos destinatários do documento.

Caso 21

Conteúdo do documento

O cabeçalho do documento contém o logótipo da Câmara, a designação completa da Câmara, a designação do gabinete que elaborou o documento e o título. No canto superior direito está o despacho manuscrito do Presidente da Câmara a que o documento diz respeito.

A parte intitulada "Finalidades dos Recursos Informáticos" indica que os recursos de tecnologias de informação disponibilizados pela autarquia são destinados exclusivamente às actividades da instituição.

A parte designada por "Utilizadores da Internet" identifica quem pode utilizar a Internet, que são os funcionários, estagiários (com a devida autorização da chefia) e prestadores de serviços para fins relacionados com a actividade da Câmara Municipal.

A parte referente ao "Direito à Propriedade" refere-se aos programas informáticos homologados, indicando que são propriedade exclusiva da Câmara Municipal, sendo vedada a sua cópia parcial ou integral.

A parte intitulada por “Regras para Utilização da Rede Interna da Câmara Municipal” composta por sete pontos, inclui orientações que os utilizadores devem seguir no âmbito da utilização da rede interna da Autarquia. São definidos os comportamentos a observar ou a evitar na utilização na rede interna, tais como:

- A utilização dos recursos da rede de computadores exclusivamente para fins profissionais;
- As contas e *passwords* são pessoais, pelo que os utilizadores respondem pelo uso exclusivo e intransmissibilidade das *passwords*;
- Apagar todos os ficheiros que não tenham fins profissionais;
- Os computadores da Câmara devem ter antivírus instalado e actualizado periodicamente, sendo proibido desinstalar e utilizar computadores sem antivírus instalado;
- A proibição de ligar computadores pessoais ou de terceiros à rede da Câmara;
- A proibição de abrir as caixas dos computadores da Câmara.

Restrições na utilização da rede interna são também listadas, nomeadamente o espaço partilhado no servidor tem limite de tamanho, mas que em casos de maior necessidade de espaço poder-se-á contactar os serviços de informática.

A parte intitulada por “Regras para Utilização do Correio Electrónico (e-mail)” composta por oito pontos, embora difira da anterior, a natureza dos seus conteúdos não é muito diversa, uma vez que ambas estipulam comportamentos a observar ou a evitar na utilização dos recursos informáticos. Restrições na utilização do correio electrónico são listadas, nomeadamente no que diz respeito às contas de correio electrónico. Podem-se destacar os seguintes pontos:

- A Câmara fornece, de acordo com indicação das chefias, contas de correio electrónico aos funcionários;
- As mensagens de correio electrónico interno e externo devem ser exclusivamente de carácter profissional;
- É proibido configurar e/ou manter configuradas contas de correio electrónico de servidores externos;
- É proibida a utilização do e-mail para fins ilegais, transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis;
- É proibida a utilização de e-mail para transmitir mensagens como *Spam*, *Junkmail*, correntes de e-mail ou a distribuição de mensagens em massa não solicitadas;
- É definido o limite em MB da caixa de correio electrónico, bem como os limites de tamanho para os ficheiros enviados.

A parte designada por “Regras para a Utilização da Internet” é composta por oito pontos, embora a sua abrangência seja diferente das duas partes anteriormente focadas, não difere muito dessas. Informações, restrições e comportamentos a adoptar por parte dos utilizadores são aqui descritos, nomeadamente:

- A indicação de que todos os acessos à Internet são controlados com a realização de auditorias nas páginas consultadas, podendo vir a ser desenvolvidos relatórios a enviar às chefias;
- A não permissão do acesso a *sites* de Internet com conteúdo pornográfico, jogos, *chat*, *blogger*, *cartoons*, música, *hacker* ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia ou senhas;

- A utilização do MSN Messenger poderá ser autorizada, após requerimento ao gabinete de informática e modernização administrativa, só para comunicações entre colaboradores da Câmara.

Proibições de utilização de programas de troca de mensagens instantâneas são também aqui apresentadas, bem como impedimentos de alteração das configurações da rede e de acesso à Internet.

Na última parte – "Penalidades" – está indicado que todos os utilizadores são responsáveis pelo uso correcto das ferramentas informáticas propriedade da Câmara e que todas as práticas que representam ameaça à segurança da informação serão tratadas com a aplicação de sanções disciplinares.

Componentes em falta

O documento que se analisa no Caso 21, no que concerne às suas componentes, apresenta uma estrutura bastante completa. A indicação de quem contactar em caso de dúvidas é feita, contudo não é indicado quem contactar para o envio de sugestões de actualização, pedidos de excepção ou comunicação de incidentes detectados.

É possível uma identificação clara dos destinatários do documento, contudo, podem-se apontar outras omissões no conteúdo do documento, designadamente a do Propósito e Objectivos, uma vez que não se elabora sobre estas componentes em qualquer parte da política.

Caso 22

Conteúdo do documento

O ponto 1, denominado por "Objecto", define que a Carta do Utilizador estabelece os direitos e deveres dos utilizadores registados como funcionários ou agentes da Câmara e que a autarquia tem como objectivo oferecer aos utilizadores através da Internet diversos serviços.

O ponto 2, designado por "Adesão aos Serviços – Procedimentos" menciona que a adesão aos serviços por parte do utilizador far-se-á através do preenchimento de um formulário e da aceitação das cláusulas contratuais gerais constantes na presente Carta do Utilizador.

O ponto 3, intitulado "Identificação do Utilizador Registado", aborda que o utilizador do serviço, após a adesão à Carta do Utilizador, passa a dispor de um *login* e de uma *password* que, sob sua responsabilidade, deverá ser mantida confidencial.

O ponto 4, intitulado "Qualidade do Utilizador", define que os utilizadores só podem ser pessoas pertencentes ao quadro de pessoal ou contratados.

O ponto 5, designado por "Regras Técnicas", define que para o bom funcionamento técnico da Internet deverão ser respeitadas certas regras pelos utilizadores, que estão definidas na Carta do Utilizador e disponíveis no Sector de Informática, sendo as mesmas entregues aos utilizadores.

O ponto 6, denominado por “Serviços”, é estruturado em quatro partes: Serviço de conteúdos, *Sites* de acesso restrito, *Shareware – Freeware* e Serviços de e-mail é definido um conjunto alargado de proibições e restrições dentro destas quatro temáticas.

O ponto 7, designado por “Conteúdos”, define que o utilizador é o único e exclusivo responsável pela sua conta de utilizador, respectivos conteúdos e inerente utilização que deles faça. O utilizador obriga-se ao integral cumprimento da Lei aplicável à utilização, comunicação e difusão de e-mails e mensagens produzidas.

O ponto 8, intitulado “Direitos de Propriedade Intelectual”, define que por toda e qualquer utilização de obras sujeitas a propriedade intelectual de terceiros, seja ela a que título for e independentemente da sua natureza, como sejam direitos de marcas, direitos de autor e direitos conexos, o utilizador obriga-se a obter as respectivas autorizações prévias dos titulares de tais direitos, nos devidos termos legais e, nomeadamente, antes de qualquer reprodução, cópia, apresentação e comunicação pública, responsabilizando-se por todo e qualquer uso indevido.

O ponto 9, intitulado “Bases de Dados Constituídas Pelos Utilizadores”, define que todos os procedimentos feitos pelos utilizadores deverão respeitar integralmente todas as disposições legais relacionadas com a protecção de dados pessoais.

O ponto 10, designado por “Utilização dos Serviços”, menciona que é expressamente vedado aos utilizadores a utilização do nome da autarquia para quaisquer fins comerciais, sendo proibida a comercialização de quaisquer serviços ou produtos, bem como, de forma geral, a obtenção de qualquer remuneração, directa ou indirecta, por parte do utilizador.

O ponto 11, designado por “Publicidade”, define que é expressamente proibido no âmbito dos serviços toda e qualquer mensagem de natureza publicitária, de promoção do utilizador ou de terceiros, seja qual for a sua forma e natureza.

O ponto 12, intitulado “E–Marketing e E–Commerce”, define que é expressamente proibido aos utilizadores efectuarem qualquer tipo de transacção comercial pela Internet.

O ponto 13, denominado por “Dados Pessoais”, menciona que o Sector de Informática obriga-se ao cumprimento das regras legais vigentes na Lei Portuguesa aplicáveis a bases de dados pessoais, conferindo ao utilizador o direito de oposição, acesso e rectificação dos respectivos dados, nos termos legais.

O ponto 14, designado por “Termos de Aceitação”, menciona que os utilizadores depois de lerem a Carta de Utilizador e aceitarem as condições apresentadas, deverão dirigir-se ao Sector de Informática para requisitar os seus *logins* e *passwords* de acesso.

Componentes em falta

Não é identificado do responsável pela manutenção do documento, bem como as sanções que a Câmara Municipal pode impor a quem não cumprir aquilo que o documento estabelece.

Caso 23

Conteúdo do documento

O documento inicia-se com uma página de texto que se considerou que constituirá a "Introdução". Alguns aspectos são aqui abordados, desde a listagem do conjunto de recursos informáticos que a Câmara disponibiliza aos funcionários para apoio às actividades, bem como a forma como devem ser usados.

O Artigo I, denominado por "Âmbito e Aplicação", define que o presente regulamento aplica-se a equipamentos, estrutura lógica e infra-estruturas e às pessoas enquanto utilizadores dos recursos informáticos.

O Artigo II, designado por "Acesso aos Recursos e Serviços de Informática", aborda aspectos relacionados com os direitos que os utilizadores têm para aceder aos recursos e serviços de informática, destacando-se os seguintes:

- Todos os elementos do pessoal da autarquia, seja qual for o tipo de vínculo laboral, enquanto este permanecer.
- Funcionários, com registo activo no Sistema da autarquia, seja qual for o seu grau, proveniência ou período de frequência.
- Pessoal envolvido em projectos de investigação ou com protocolos de colaboração, enquanto possuir registo válido nos serviços da autarquia.
- Outras pessoas, desde que com justificação apropriada.
- Para obter autorização de acesso o utilizador deve registar-se, estando este registo condicionado à expressa aceitação do presente regulamento.
- A autorização de acesso aos recursos informáticos da autarquia mantém-se enquanto se mantiver válido o respectivo direito de acesso.
- A autorização de acesso pode ser temporariamente suspensa, ou mesmo cancelada, por razões de segurança, ou por suspensão do direito de acesso correspondente.

O Artigo III, denominado por "Propriedade, Privacidade e Confidencialidade", define que os dados depositados nos sistemas informáticos da autarquia são propriedade e responsabilidade dos seus autores ou dos utilizadores que lhes deram origem. Os serviços responsáveis pela sua gestão zelarão para assegurar a sua inviolabilidade, privacidade e confidencialidade.

O Artigo IV, designado por "Serviços e Recursos", aborda aspectos como:

- A instalação de recursos e aplicações informáticas deve respeitar todas as condições de legalidade, nomeadamente quanto a licenciamentos e protecção dos direitos de autor.
- A ligação ou instalação de quaisquer equipamentos que interfiram com as infra-estruturas de rede da autarquia carecem de uma autorização prévia.

O Artigo V, designado por “Ética e Regras de Utilização”, define um conjunto de pontos que estabelecem o que não é permitido realizar em sistemas informáticos da autarquia, sendo os utilizadores punidos se não os respeitarem. O uso, ou tentativa de uso, não autorizado, ilegítimo ou fraudulento de qualquer recurso informático, nomeadamente, computadores, redes, equipamentos periféricos, aplicações ou dados, constituem uma violação do regulamento e é punível.

O Artigo VI, intitulado “Normas”, é composto por três pontos: Normas de Utilização da Rede/Internet Informática da Câmara Municipal, Normas de Utilização da Internet da Câmara Municipal e Normas de Utilização do Correio Electrónico da Câmara Municipal.

Componentes em falta

O regulamento analisado, no que concerne as suas componentes, não refere quem é o responsável pela manutenção do documento, outras omissões no conteúdo do documento, são visíveis, designadamente a do Propósito e Objectivos. Outra omissão que se verifica neste documento é a falta de identificação da entidade que aprovou o regulamento.

Caso 24

Conteúdo do documento

No Preâmbulo do documento, o primeiro parágrafo remete para o regulamento orgânico da Câmara Municipal onde faz parte das missões da autarquia um serviço de informática. Seguidamente, é definido o que se pretende com o presente regulamento de informática. É de referir que este documento é mais que uma política de SSI, na medida em que se trata de um documento mais abrangente, constituindo-se em um instrumento regulador de todo o serviço de informática desta Câmara Municipal.

O capítulo I, intitulado “Disposições Gerais”, é composto por dois artigos, o primeiro refere-se à integração orgânica e designação do serviço, onde se define que o serviço de informática desta Câmara faz parte dos instrumentos transversais de apoio à gestão. O segundo artigo define o serviço de informática como elemento essencial de apoio à decisão de todos os serviços da autarquia e que tem como núcleo técnico especializado o designado Núcleo de Apoio de Informática.

O capítulo II, designado “Estrutura e competências”, é composto por três artigos. O primeiro artigo é designado de “estrutura” e define a hierarquia do serviço de informática no organograma da Câmara Municipal. O segundo artigo deste capítulo é designado de “competências” e é composto por quatro pontos e um conjunto de subpontos, onde estão descritas ao pormenor as competências do responsável pelo pelouro da informática, do Departamento de Planeamento e Administração, do Núcleo de Apoio da Informática e caso a Câmara recorra a uma assessoria especializada de informática as competências desta. O terceiro e último artigo deste capítulo define as funções primordiais do responsável pelo Núcleo de Apoio de Informática.

O capítulo III, intitulado "Identificação e solicitações ao Núcleo de Apoio de Informática", é composto por três artigos. O primeiro, que é o artigo 6.º, é intitulado "Identificação dos utentes" e estabelece que os utentes são identificados pela utilização de uma ou mais palavras de identificação (*login*), directamente relacionadas com o seu nome, e por uma ou mais palavras senha (password), directamente associadas a cada uma delas. O segundo artigo diz respeito à forma como os utentes devem comunicar com o Núcleo de Apoio de Informática, para efeitos de colocação de dúvidas, comunicação de avarias, necessidades ou apoios pontuais. O terceiro e último artigo deste capítulo é similar ao anterior, diferindo no facto deste ser só para pedido de novos equipamentos ao Núcleo de Apoio de Informática.

O capítulo IV, intitulado "Direitos, deveres e proibições", é composto por dez artigos e três secções e é sem dúvida o capítulo maior e no que à SSI diz respeito, o que mais se relaciona com a temática.

No primeiro e no segundo artigos deste capítulo estão minuciosamente explicados os direitos e os deveres dos utentes. Como deveres podem-se dar os seguintes exemplos:

- O utente tem direito à liberdade no âmbito do processamento informático dos seus dados pessoais e no âmbito do trabalho técnico de sua responsabilidade e autoria;
- Direito de acesso aos dados que sejam registados a seu respeito, sem demoras ou custos excessivos;
- Direito de rectificação e eliminação quanto ao tratamento dos seus dados pessoais;
- Direito de oposição.

Como deveres podem-se dar os seguintes exemplos:

- O utente deve respeitar sempre a liberdade e a privacidade alheias;
- Os utilizadores são responsáveis pelo correio electrónico originado com a sua identificação.

O terceiro artigo aborda as proibições relacionadas com os acessos de cada utente, onde está definido que o utente não pode ceder os seus privilégios de acesso, nem pode usar os privilégios de outros utentes e que caso decida partilhar os seus dados com outra pessoa, o utente é considerado o único responsável pelo uso da sua identificação informática.

O quarto artigo também define proibições, sendo composto por dezasseis pontos, que focam aspectos como por exemplo:

- O utente só pode utilizar os recursos informáticos para os quais possua a devida autorização;
- Em nenhuma circunstância deve aceder ou tentar aceder a recursos que lhe estão vedados;
- O utente não pode usar os recursos da Câmara Municipal para tentar aceder ilegalmente a sistemas informáticos de outras instituições;

- O utente não pode interferir com dados, programas ou sistemas nem interceptar informação de outros utentes ou da Câmara Municipal;
- O utente deve abster-se de atitudes que possam causar prejuízos morais ou materiais aos restantes utentes, ao sistema informático instituído ou à Câmara Municipal;
- O utente não pode, em circunstância alguma, proceder à ligação de novos equipamentos à rede informática sem prévio conhecimento e autorização de quem de direito;
- O utente não pode visualizar ou armazenar informação ofensiva ou obscena nem enviar ou receber mensagens do mesmo teor;
- O utente não pode usar os recursos informáticos da Câmara Municipal para a execução de jogos, passatempos ou outros fins que não estejam de alguma forma ligados à sua actividade profissional;
- O utente não pode instalar aplicações nem alterar a configuração das aplicações ou sistemas instalados, sem autorização prévia;
- O utente não pode realizar qualquer acção deliberada, não autorizada, que venha a danificar ou corromper um equipamento informático;
- O utente não pode apagar, examinar, copiar ou modificar ficheiros de dados ou qualquer tipo de informação pertencentes a outros utilizadores sem o seu expresso consentimento;
- O utente não pode utilizar computadores, recursos partilhados, impressoras ou outro material informático para fins não autorizados.

A Secção I deste capítulo, que engloba dois artigos, é designada “Do correio electrónico (e-mail)”, e define os condicionantes à utilização do correio electrónico. No primeiro artigo, é feita a definição de procedimentos interditos à utilização de correio electrónico, nomeadamente falsificar mensagens de correio electrónico e tentar ler, apagar, copiar ou modificar o correio electrónico de outros utentes, outro aspecto é a possível alteração do tamanho predefinido para a caixa de correio electrónico e algumas recomendações. O segundo artigo define entre outros aspectos, que o acesso preferencial às caixas de correio electrónico deverá ser feito através da intranet.

A Secção II, que engloba dois artigos, é definida como “Da utilização das aplicações Internet”. O primeiro artigo desta secção define o acesso à Internet, nomeadamente no que diz respeito à informação de que por razões de segurança e de elaboração de estatísticas de uso interno, todos os acessos à Internet são registados informaticamente e mantidos durante um período de um mês, sendo posteriormente eliminados, salvo determinação superior em contrário.

O segundo artigo desta secção aborda dois aspectos, um primeiro que define o que é interdito aos utentes a quem for facultado o acesso à Internet, nomeadamente a cópia de materiais protegidos por direitos de autor, tais como programas licenciados sem autorização expressa do proprietário ou a propriedade da licença adequada, o segundo aspecto é permitir apenas o acesso para fins de pesquisa temática relacionada com o trabalho, comunicação e formação, sendo ainda vedado o acesso a portais ou *sites* na Internet com conteúdo que, por exemplo, estimulem a prática de condutas ilícitas ou contrárias à moral e aos bons costumes; que permitam a descarga de ficheiros de filmes ou vídeos alheios às actividades normais desenvolvidas na Câmara Municipal, assim como ficheiros de música, jogos e passatempos; violem a

lei, a moral, os bons costumes, a propriedade intelectual, os direitos à honra, à vida privada, à intimidade pessoal e familiar; violem o sigilo das comunicações; coloquem à disposição ou possibilitem o acesso a programas informáticos ilegais, mensagens, produtos ou serviços ilícitos, violentos, pornográficos ou degradantes.

A secção III, que se denomina "Da utilização das aplicações administrativas e outras em rede", é composta por dois artigos que abordam o acesso às aplicações administrativas e outras em rede e as condicionantes da utilização das aplicações administrativas e outras em rede. No primeiro, o conteúdo é idêntico ao já referido na secção anterior para o acesso à Internet, podendo-se destacar os seguintes aspectos:

- O acesso às aplicações administrativas ou a outras em rede só é permitido aos utentes que o tenham requerido por escrito ao responsável do pelouro da informática, de onde constem a sua completa identificação e a justificação para o seu pedido;
- Por razões de segurança, os utilizadores deverão periodicamente proceder à alteração da sua *password*.
- Por razões de segurança e de elaboração de estatísticas de uso interno, todos os acessos às aplicações administrativas e outros em rede são registados informaticamente.

O segundo artigo lista o que está interdito aos utentes a quem for facultado o acesso às aplicações administrativas ou a outras em rede, tais como:

- Efectuar qualquer tentativa de descodificação das *passwords* de acesso aos sistemas, áreas ou recursos de outros utentes, bem como de qualquer recurso não especificamente autorizado;
- Copiar material protegido por direitos de autor, tais como programas licenciados;
- Tentar bloquear o funcionamento de recursos informáticos;
- Tentar substituir ou modificar as aplicações e serviços disponibilizados pela Câmara Municipal.

O capítulo V, designado de "Auditoria e regime disciplinar", é composto por dois artigos, um intitulado "Auditoria" e outro "Regime disciplinar". O primeiro artigo define que a actividade realizada pelos utentes no equipamento informático da Câmara Municipal poderá em qualquer altura ser objecto de auditoria pelo Núcleo de Apoio de Informática, de forma a garantir o cumprimento das normas de utilização e de modo a assegurar a qualidade e o bom funcionamento da prestação do serviço de informática. O segundo artigo regista que o não cumprimento das normas do presente regulamento pode determinar a abertura dos competentes procedimentos de natureza disciplinar, nos termos da lei.

Por último, o capítulo VI – "Disposições finais" – é composto por cinco artigos, que abrangem desde a avaliação de desempenho do Núcleo de Apoio de Informática, à revisão do presente regulamento que define o que será revisto por iniciativa ou proposta dos órgãos municipais competentes, é definida a entrada em vigor do regulamento e como resolver as dúvidas e omissões do presente regulamento.

Componentes em falta

Para além da identificação clara do seu propósito, estão claramente identificadas as entidades que o aprovaram, há referência a sanções que a Câmara Municipal pode impor a quem não cumprir aquilo que o regulamento estabelece. Este regulamento apresenta uma estrutura que se identifica com o conteúdo de uma política de SSI, conforme o previsto na revisão da literatura sobre esta temática, contudo não está claramente definido quem são os destinatários do regulamento, ou seja o seu público-alvo, bem como a identificação do responsável pela manutenção do documento.

Caso 25

Conteúdo do documento

A folha de rosto do documento contém o logótipo e a designação do Município. O tipo de documento é identificado no centro do quadro do cabeçalho como "Comunicação Interna", é feita a indicação do remetente e do destinatário, que neste caso é enviado pelo especialista de informática do Departamento de Administração Geral – Divisão de Informática e Tecnologia para a directora de Departamento de Administração Geral. No canto superior direito do quadro do cabeçalho existe uma série de campos, nomeadamente o registador, o número, o número de folhas, o processo e a data. Seguidamente tem um segundo quadro com o assunto da comunicação interna que é: "Proposta – Regras para utilização dos meios informáticos" e um espaço em branco para o despacho.

Ainda na folha de rosto, segue-se o texto do documento que justifica o propósito do documento, que é "dar a conhecer a todos os utilizadores algumas regras básicas pelas quais o Departamento de Administração Geral – Divisão de Informática e Tecnologia, baseia a sua actividade diária, de forma a esclarecer os mesmos, quanto aos deveres enquanto utilizadores dos Sistemas Informáticos da Câmara".

A parte intitulada "Normas Gerais" é composta por cinco pontos, que abordam aspectos como de quem é a responsabilidade da criação de utilizador informático e de comunicar a saída de um utilizador ou transferência para outro serviço; a proibição de instalação de software sem a prévia autorização e a salvaguarda de que todas as situações que forem detectadas de utilização duvidosa dos meios informáticos disponíveis serão comunicadas aos superiores hierárquicos e tomadas as medidas adequadas para garantir os níveis de segurança necessários.

A parte designada de "Utilizadores" indica que cada utilizador tem de ter um nome de acesso (*login*) único e exclusivo para acesso aos computadores, pastas, servidores e aplicações. Outro ponto orienta os utilizadores no sentido de não abandonarem os computadores ligados à rede sem terminar as sessões de trabalho ou sem ter procedido ao respectivo bloqueio. Por último, é referido que todos os ficheiros de trabalho devem ser guardados nas pastas dos servidores da Câmara Municipal existentes para o efeito.

A parte intitulada "PC´s" é composta por quatro pontos, que informam os utilizadores para o facto de que os equipamentos informáticos são para uso

exclusivamente profissional e responsabiliza-os quanto ao conteúdo existente nos computadores, bem como pela efectuação de cópias de segurança dos ficheiros de trabalho que se encontram guardados no disco rígido.

A parte designada de "Rede" é composta por dois pontos. O primeiro determina que qualquer mudança de localização de equipamento tem de ser coordenada previamente com a Divisão de Informática e Tecnologia. O segundo ponto define que os bloqueios dos equipamentos ligados à rede informática por motivo de mudança de localização são da inteira responsabilidade dos utilizadores que os executarem.

A parte intitulada por "Correio Electrónico" é composta por oito pontos que abordam aspectos como: a existência para todos os utilizadores de uma caixa de correio electrónico interno para contactos na rede interna da Câmara, para uso exclusivamente profissional; a existência também de uma caixa de correio externo para ser utilizado como meio de contacto oficial, e de que a Divisão de Informática e Tecnologia efectuará os filtros de conteúdos necessários a assegurar a correcta segurança e normal funcionamento da Câmara Municipal.

Componentes em falta

O documento que se analisa no Caso 25, no que diz respeito às suas componentes, apresenta uma estrutura simples, incidindo o seu conteúdo directamente nos pontos normalmente abordados neste tipo de documento. A indicação de quem contactar em caso de dúvidas é feita ao longo do documento, contudo não é indicado quem contactar para o envio de sugestões de actualização, pedidos de excepção ou comunicação de incidentes detectados, bem como o responsável pela implementação e manutenção do documento.

Não são identificados claramente os destinatários do documento, nem o seu objectivo. Outra omissão é a não especificação de sanções a aplicar aos utilizadores que não cumpram o estipulado. Pode-se apontar ainda uma outra omissão no conteúdo do documento, que é a não definição dos objectivos da política.

Apêndice I – Proposta Base de Políticas de SSI

Neste apêndice é apresentada a proposta de dois modelos de Política de SSI. O modelo A é destinado aos dirigentes e técnicos informáticos, enquanto, que o modelo B é dirigido aos utilizadores do sistema de informação do Município (as componentes destas propostas foram já referidas no Capítulo 8 deste trabalho). Os Modelos seguintes foram elaborados com base na legislação e literatura existente sobre a temática, mas principalmente recorrendo às políticas disponibilizadas pelas Câmaras, complementando a elaboração com a aprendizagem nos meios já referidos.

Política de Segurança dos Sistemas de Informação
Câmara Municipal de …
Modelo A

Preâmbulo

Com a presente política de segurança de sistemas de informação pretende-se estabelecer, de forma clara, princípios que contribuam para a uniformização de procedimentos e configurações, a optimização dos recursos de rede e dos equipamentos a ela conectados, bem como da melhoria acentuada no atendimento e resolução de problemas por parte do Sector de Informática, no que concerne à segurança de sistemas de informação.

CAPÍTULO I
Disposições gerais

Artigo 1.º
Objectivo

Este documento tem por finalidade definir um conjunto de regras/normas básicas que definem de forma clara as responsabilidades do Gabinete de Informática (GI), com vista a uma gestão cuidada e precisa do parque informático, bem como a defesa dos direitos de autor, os incidentes e suas consequências, a aprovação da política e a sua revisão, garantindo a segurança dos sistemas de informação do Município.

Artigo 2.º
Definições

Segurança de Sistemas de Informação – Enquadramento organizacional de cultura, políticas, estruturas organizacionais e ambiente operacional utilizado para assegurar a integridade, disponibilidade e confidencialidade da informação de uma organização.

Política de Segurança de Sistemas de Informação – Documento que orienta ou regula as acções das pessoas ou sistemas no domínio da segurança dos sistemas de informação.

CAPÍTULO II
Responsabilidades do GI

Artigo 3.º
Medidas de segurança

O director do GI, ou caso este não exista o chefe de divisão ou funcionário responsável pelo GI da autarquia, é responsável pela implementação de medidas de segurança necessárias para garantir a confidencialidade, integridade e disponibilidade da informação, independentemente da maneira pela qual esteja armazenada e comunicar superiormente o desrespeito por qualquer norma.

Artigo 4°
Defesa de direitos de autor

O município defenderá os direitos de autor (copyright), as leis que regulamentam o acesso e o uso de informações e as regras de organizações que fornecem informações, razão pela qual somente o GI está habilitado a instalar software e hardware nos computadores.

Artigo 5°

Deveres do director/chefe de divisão/funcionário

1 – Cabe ao responsável do GI a responsabilidade de:

a) Assegurar o cumprimento deste regulamento;

b) Manter e actualizar dados de todos os utilizadores autorizados;

c) Manter no município um registo de ocorrências de violação dos regulamentos;

d) Garantir a segurança dos meios e dos dados;

e) Controlar o acesso físico aos equipamentos sob sua responsabilidade;

f) Não permitir que software licenciado para o município seja copiado por terceiros ou instalado em equipamentos não autorizados;

g) Zelar para que sejam feitas cópias de segurança e verificar da sua integridade;

h) Adoptar medidas apropriadas de segurança em relação a software e rotinas;

i) Preservar informações confidenciais como, por exemplo, ficheiros de utilizadores e códigos de acesso ao sistema;

j) Administrar devidamente o acesso, regularizar de maneira rápida e precisa as permissões de acesso para utilizadores transferidos ou que tiveram o acesso cancelado;

k) Verificar os logins, acessos e registos de auditoria dos sistemas para controlar tentativas de violação e quebra de segurança;

l) Manter as ligações e o roteamento de transmissão de dados em funcionamento;

m) Manter registos de todas as acções empreendidas nos diversos computadores (instalação de software, instalação/substituição de componentes, rotação de activos, etc.);

n) Respeitar e seguir os procedimentos padronizados para a administração de recursos informáticos e de rede normalmente aceites ou definidos pelos órgãos do município.

Artigo 6°

Competências gerais

1 – É competência do responsável pelo pelouro da informática:

1.1 – Analisar e aprovar os relatórios periódicos que os técnicos lhe fazem chegar, com o resumo das ocorrências verificadas e procedimentos efectuados dentro das competências que lhes estão afectas.

1.2 – Autorizar ou não os requerimentos que lhes são dirigidos solicitando o acesso ao sistema informático da Câmara.

CAPÍTULO III

Identificação e solicitações ao GI

Artigo 7.º

Identificação dos utilizadores

1 – Do ponto de vista informático, o utilizador é identificado pela utilização de uma ou mais palavras de identificação *(login)*, directamente relacionadas com o seu nome, e por uma ou mais palavras senha *(password)*, directamente associadas a cada uma delas.

2 – Estas palavras são indispensáveis para o acesso aos principais serviços em rede, sendo atribuídas pelo GI, a requerimento dos utilizadores, dirigido ao responsável pelo pelouro da informática, com excepção do *e-mail*, que poderá ser pedido directamente ao GI.

Artigo 8.º

Solicitações dos utilizadores ao GI

1 – A comunicação preferencial com o GI para efeitos de colocação de dúvidas, avarias ou necessidades deverá ser feita através do preenchimento do formulário electrónico próprio, disponível na intranet da Câmara Municipal.

2 – Este procedimento dará origem a um registo informático automático numa aplicação própria do serviço, para execução pelos técnicos e controlo interno.

3 – Poderão ser solicitadas ajudas pontuais de recurso imediato sempre que se verifique que o serviço do utilizador se encontra paralisado por força de problema no sistema operacional informático, ou outro que se relacione directamente com o respectivo computador pessoal e que perturbe o normal funcionamento da globalidade de um serviço ou ainda que esteja em causa a segurança do sistema informático.

CAPÍTULO IV

Disposições finais

Artigo 9°

Responsabilidade pela segurança e incidentes

1 – Todos os utilizadores e administradores do sistema têm o dever de comunicar superiormente qualquer tentativa de acesso não autorizado ou qualquer outro uso indevido de recursos informáticos.

2 – Ao testemunhar ou tomar conhecimento (por quaisquer meios) de problemas relacionados com a segurança ou uso abusivo de recursos incluindo o desrespeito por este documento, o utilizador deve tomar imediatamente as providências necessárias que estiverem ao seu alcance, para garantir a segurança e a conservação dos recursos e avisar os seus superiores ou o GI.

Artigo 10°

Incidentes e suas consequências

Os incidentes envolvendo utilizadores são comunicados ao Administrador de Sistemas que deles dará conhecimento ao Vereador do Pelouro.

Artigo 11.º

Avaliação de desempenho do GI

A avaliação de desempenho do GI é efectuada mediante a elaboração de um relatório anual, tendo como base o respectivo plano de actividades, apresentado ao executivo da Câmara Municipal.

Artigo 12.º

Aprovação da Política

A aprovação da política deverá ser em Reunião de Câmara. Nessa aprovação deverá ser indicado quem foi o proponente do documento, ou seja, o autor da política. Deve também ser indicada a data da elaboração bem como a data de aprovação.

Artigo 13.º

Revisão do presente regulamento

O presente regulamento será revisto por iniciativa ou proposta dos órgãos municipais competentes, bem como a aprovação dessa revisão. Este processo é acompanhado da elaboração de um programa de revisão que ficará como histórico de revisões. A revisão do documento deverá ser definida pelo executivo.

Artigo 14.º

Dúvidas e omissões

As dúvidas e omissões do presente regulamento serão resolvidas por recurso à interpretação da legislação habilitante, com base em critérios de equidade, mediante decisão da Câmara Municipal de … .

Artigo 15.º

Entrada em vigor

O presente documento entre em vigor no … dia útil seguinte ao da deliberação de aprovação pela Câmara Municipal.

Política de Segurança dos Sistemas de Informação
Câmara Municipal de …
Modelo B

Preâmbulo

Com a presente política de segurança de sistemas de informação pretende-se garantir a confidencialidade, integridade e disponibilidade da informação, para tal, com este documento ambiciona-se especificar os direitos e deveres dos utilizadores do Sistema de Informação da Câmara Municipal de … em todas as suas componentes e consequente responsabilidade disciplinar ou criminal, delimitação do poder de auditoria e regime disciplinar, independentemente do vínculo à Câmara Municipal, modos de interacção com os utilizadores na sua qualidade de trabalhadores da edilidade.

CAPÍTULO I
Disposições gerais

Artigo 1.º
Objectivo

A política de segurança dos sistemas de informação aplica-se a todos os utilizadores autorizados do sistema de informação da Câmara Municipal de …, com o objectivo de orientar ou regular as acções dos utilizadores no domínio da segurança dos sistemas de informação.

Artigo 2.º
Definições

Segurança de Sistemas de Informação – Enquadramento organizacional de cultura, políticas, estruturas organizacionais e ambiente operacional utilizado para assegurar a integridade, disponibilidade e confidencialidade da informação de uma organização.

Política de Segurança de Sistemas de Informação – Documento que orienta ou regula as acções das pessoas ou sistemas no domínio da segurança dos sistemas de informação.

Artigo 3.º
Utilizadores autorizados

Consideram-se utilizadores autorizados para efeitos do presente documento, os funcionários do município, os contratados e os colaboradores em regime de prestação de serviços.

CAPÍTULO II
Direitos, deveres e proibições

Artigo 3.º
Direitos dos utilizadores

1 – O utilizador tem direito à liberdade e privacidade no âmbito do processamento informático dos seus dados pessoais e no âmbito do trabalho técnico de sua responsabilidade e autoria.

2 – Conforme instruções disponibilizadas na página da Internet da Comissão Nacional de Protecção de Dados (CNPD), o utilizador tem ainda os seguintes direitos:

2.1 – Direito de informação quanto à recolha de dados pessoais no momento em que os seus dados são recolhidos, ou, caso a recolha de dados não seja feita directamente junto de si, logo que os dados sejam tratados, tem o direito de ser informado sobre:
a) Qual a finalidade do tratamento;
b) Quem é responsável pelo tratamento dos dados;
c) A quem podem ser comunicados os seus dados;
d) Quais as condições em que pode aceder e rectificar os seus dados;
2.2 – Direito de oposição:
a) O utilizador tem o direito de se opor a que os seus dados pessoais sejam comunicados a terceiros, salvo disposição legal em contrário;
b) O utilizador tem o direito de se opor, nos casos previstos na lei, a que os seus dados sejam objecto de tratamento, por razões ponderosas e legítimas relacionadas com a sua situação particular;
c) O utilizador tem o direito de se opor a que os seus dados pessoais sejam utilizados para fins de prospecção ou publicidade;
3 – Todos os trabalhadores da edilidade têm direito à utilização de uma conta de correio electrónico, a ser fornecida pelo GI, mediante o envio de um pedido escrito ou o preenchimento de um formulário próprio, disponível na intranet.

Artigo 4.º

Deveres dos utilizadores

1 – O utilizador deve respeitar sempre a liberdade e a privacidade alheias.
2 – Os utilizadores são responsáveis pelo correio electrónico originado com a sua identificação.
3 – Às proibições constantes do artigo seguinte ou estabelecidas em outros preceitos do presente documento corresponderá o correlativo dever, ainda que não expressamente enunciado.

Artigo 5.º

Proibições relacionadas com os acessos de cada utilizador

1—O utilizador não pode ceder os seus privilégios de acesso nem pode usar os privilégios de outros.
2—O utilizador é o único responsável pelo uso indevido dos seus privilégios de acesso e deverá comunicar imediatamente ao seu superior hierárquico, em cadeia, bem como ao GI, em caso de suspeita desse facto.
3—Caso decida partilhar os seus dados com outra pessoa, o utilizador é considerado o único responsável pelo uso da sua identificação informática.

Artigo 6.º

Proibições relativas aos utilizadores

1 – O utilizador só pode utilizar os recursos informáticos para os quais possua a devida autorização.
2 – Em nenhuma circunstância deve aceder ou tentar aceder a recursos que lhe estão vedados.
3 – O utilizador não pode usar os recursos da Câmara Municipal para tentar aceder ilegalmente a sistemas informáticos de outras instituições, e, caso o faça, o seu comportamento será averiguado em sede própria, assumindo inteira responsabilidade pelos actos que praticar.
4 – O utilizador não pode interferir com dados, programas ou sistemas nem interceptar informação de outros utilizadores ou da Câmara Municipal.
5 – O utilizador deve abster-se de atitudes que possam causar prejuízos morais ou materiais aos restantes utilizadores, ao sistema informático instituído ou à Câmara Municipal.

6 – O utilizador não pode, em circunstância alguma, proceder à ligação de novos equipamentos à rede informática sem prévio conhecimento e autorização do GI, já que, ao fazê-lo, poderá colocar em risco o funcionamento de toda rede ou serviços lnternet.
7 – O utilizador não pode visualizar ou armazenar informação ofensiva ou obscena nem enviar ou receber mensagens do mesmo teor.
8 – O utilizador não pode usar os recursos informáticos da Câmara Municipal para a execução de jogos, passatempos ou outros fins que não estejam de alguma forma ligados à sua actividade profissional.
9 – O utilizador não pode utilizar estes mesmos recursos informáticos para fins comerciais nem vender ou ceder a terceiros o trabalho desenvolvido com recurso à Internet.
10 – O utilizador não pode reproduzir ou divulgar informação armazenada nos sistemas da Câmara Municipal, a não ser que esta seja da sua responsabilidade, ou que não esteja abrangida por direitos de autor, sem prejuízo dos deveres profissionais a que se encontra adstrito.
11 – O utilizador não pode instalar aplicações nem alterar a configuração das aplicações ou sistemas instalados, sem autorização prévia do GI ou dos órgãos municipais competentes.
12 – O utilizador não pode apagar, examinar, copiar ou modificar ficheiros de dados ou qualquer tipo de informações pertencentes a outros utilizadores sem o seu expresso consentimento.
13 – O utilizador não pode penalizar os outros utilizadores através de um uso abusivo dos recursos existentes, após ter sido avisado de tal situação.
14 – Utilizar computadores, recursos partilhados, impressoras ou outro material informático para usos não autorizados.

SECÇÃO I
Do correio electrónico *(e-mail)*

Artigo 7.º
Condicionantes à utilização do correio electrónico *(e-mail)*

1 – São interditos na utilização de correio electrónico os seguintes procedimentos:
a) Falsificar mensagens de correio electrónico;
b) Tentar ler, apagar, copiar ou modificar o correio electrónico de outros utilizadores;
c) Enviar correio electrónico de âmbito comercial, correio em cadeia *(chain letters)* ou correio electrónico de conteúdo duvidoso *(junk mail);*
d) Enviar mensagens colectivas de correio electrónico *(spam mails)* a grupos de utilizadores da Câmara Municipal ou de outras entidades, públicas ou privadas;
e) Utilizar o correio electrónico oferecendo produtos ou serviços de qualquer natureza, próprios ou de outrem, que não sejam de interesse dos destinatários ou que não tenham o expresso consentimento destes;
f) Enviar mensagens contaminadas por vírus ou outros elementos físicos ou electrónicos que possam danificar ou impedir o normal funcionamento da rede, do sistema ou dos equipamentos informáticos *(hardware* e *software)* de terceiros ou que possam danificar os documentos electrónicos e arquivos armazenados nestes equipamentos informáticos.
2 – Todas as caixas de correio electrónico são criadas, por defeito, com um tamanho máximo predefinido, sendo possível requerer o seu aumento, quando devidamente justificado.

3 – Para evitar a situação a que se alude no número anterior, o utilizador tem o dever de se preocupar com a manutenção da sua caixa de correio, eliminando as mensagens mais antigas ou de menor interesse.

Artigo 8.º

Acesso ao serviço de correio electrónico *(e-mail)*

1 – O acesso preferencial às caixas de correio electrónico deverá ser feito através da intranet.

2 – São possíveis outros tipos de acesso, nomeadamente através dos programas de correio electrónico disponíveis no mercado.

3 – O acesso por terceiros aos dados das caixas de correio de cada utilizador está reservado, em exclusivo, ao responsável do GI, que para tal deverá ter a devida autorização do responsável do pelouro de informática e apenas para efeitos de manutenção do sistema.

4 – O disposto no preceito anterior não poderá pôr em causa o disposto na lei sobre direitos, liberdades e garantias dos utilizadores.

SECÇÃO II

Da utilização das aplicações Internet

Artigo 9.º

Acesso à Internet

1 – O acesso à Internet ou a outras redes de dados só é permitido aos utilizadores que o tenham requerido por escrito ao responsável pelo pelouro da informática, de onde constem a sua completa identificação e a justificação para o seu pedido.

2 – Autorizado o acesso à Internet nos termos do número anterior, os utilizadores receberão uma identificação informática através do uso de duas palavras de identificação *(login* e *password)* atribuídas pelo GI.

3 – Por questões de segurança, os utilizadores deverão periodicamente proceder à alteração da sua palavra senha *(password).*

4 – Poderá ainda o GI, sempre que se justificar, solicitar aos utilizadores que alterem as suas palavras senha *(passwords)* para poderem continuar a utilizar os serviços em rede.

5 – Por razões de segurança e de elaboração de estatísticas de uso interno, todos os acessos à Internet são registados informaticamente e mantidos durante um período de um mês, sendo posteriormente eliminados, salvo determinação superior em contrário.

6 – O acesso a esta informação está reservado ao responsável do GI, sendo-lhe vedada a divulgação de qualquer informação que permita a ligação da mesma a um dado utilizador, sem o consentimento deste, podendo ainda tal suceder a pedido expresso, por escrito, do responsável do pelouro da informática no uso dos poderes disciplinares que a lei lhe confere ou ainda a pedido das autoridades policiais, devidamente mandatadas.

Artigo 10.º

Condicionantes do acesso à Internet

1 – Aos utilizadores a quem for facultado o acesso à Internet é interdito:

a) Efectuar qualquer tentativa de descodificação das palavras senha *(passwords)* de acesso aos sistemas, áreas ou recursos de outros utilizadores, bem como de qualquer recurso não especificamente autorizado;

b) Copiar materiais protegidos por direitos de autor, tais como programas licenciados sem a autorização expressa do proprietário ou a propriedade da licença adequada;

c) Tentar bloquear o funcionamento de recursos informáticos nacionais ou internacionais;
d) Tentar obter níveis de privilégios superiores aos atribuídos no uso dos recursos informáticos disponibilizados;
e) Introduzir ou propagar, intencionalmente, vírus informáticos ou quaisquer outros programas destrutivos dos sistemas informáticos, tanto internos como externos, à Câmara Municipal;
f) Instalar e disponibilizar aplicações ou serviços destinados à Internet sem o conhecimento e autorização prévia do GI ou dos órgãos municipais competentes;
g) Tentar substituir ou modificar as aplicações e serviços disponibilizados pela Câmara Municipal.
2—O acesso à Internet só é permitido para fins de pesquisa temática relacionada com o trabalho, comunicação e formação, sendo ainda vedado o acesso a portais ou *sites* na Internet com conteúdos que:
a) Violem a lei, a moral, os bons costumes, a propriedade intelectual, os direitos à honra, à vida privada, à imagem e à intimidade pessoal e familiar;
b) Estimulem a prática de condutas ilícitas ou contrárias à moral e aos bons costumes;
c) Incitem à prática de actos discriminatórios em razão de sexo, raça, religião, crenças, idade ou qualquer outra condição;
d) Coloquem à disposição ou possibilitem o acesso a programas informáticos ilegais, mensagens, produtos ou serviços ilícitos, violentos, pornográficos ou degradantes;
e) Que permitam a descarga de ficheiros de filmes ou vídeos alheios às actividades normais desenvolvidas na Câmara Municipal, assim como ficheiros de música, jogos e passatempos;
f) Constituam publicidade ilícita, enganosa ou desleal; em geral, que configurem concorrência desleal;
g) Veiculem, incitem ou estimulem a pedofilia.

SECÇÃO III
Da utilização das aplicações administrativas e outras em rede

Artigo 11.º
Acesso às aplicações administrativas e outras em rede

1 – O acesso às aplicações administrativas ou a outras em rede só é permitido aos utilizadores que o tenham requerido por escrito ao responsável do pelouro da informática, de onde constem a sua completa identificação e a justificação para o seu pedido.
2 – Autorizado o acesso nos termos do número anterior, os utilizadores receberão uma identificação informática através do uso de duas palavras de identificação *(login* e *password)* atribuídas pelo GI.
3 – Por questões de segurança, os utilizadores deverão periodicamente proceder à alteração da sua palavra senha *(password).*
4 – Poderá ainda o GI, sempre que se justificar, solicitar aos utilizadores que alterem as suas palavras senha *(passwords)* para poderem continuar a utilizar os serviços em rede.
5 – Por razões de segurança e de elaboração de estatísticas de uso interno, todos os acessos às aplicações administrativas e outras em rede são registados informaticamente.

Artigo 12.º

Condicionantes da utilização das aplicações administrativas e outras em rede

1 – Aos utilizadores a quem for facultado o acesso às aplicações administrativas ou a outras em rede, é interdito:

a) Efectuar qualquer tentativa de descodificação das palavras senha *(passwords)* de acesso aos sistemas, áreas ou recursos de outros utilizadores, bem como de qualquer recurso não especificamente autorizado;

b) Copiar materiais protegidos por direitos de autor, tais como programas licenciados sem a autorização expressa do proprietário ou a propriedade da licença adequada;

c) Tentar bloquear o funcionamento de recursos informáticos;

d) Tentar obter níveis de privilégios superiores aos atribuídos no uso dos recursos informáticos disponibilizados;

e) Introduzir ou propagar, intencionalmente, vírus informáticos ou quaisquer outros programas destrutivos dos sistemas informáticos;

f) Tentar substituir ou modificar as aplicações e serviços disponibilizados pela Câmara Municipal.

CAPÍTULO III

Auditoria e regime disciplinar

Artigo 13.º

Auditoria

1 – A actividade realizada pelos utilizadores no equipamento informático da Câmara Municipal poderá em qualquer altura ser objecto de auditoria pelo GI, de forma a garantir o cumprimento das normas de utilização e de modo a assegurar a qualidade e o bom funcionamento da prestação do serviço de informática.

2 – As auditorias são realizadas pelo GI a pedido do responsável do pelouro da informática.

3 – A informação constante do relatório da auditoria não pode ser utilizada para outros fins sem o prévio conhecimento dos utilizadores interessados e a autorização do responsável do pelouro da informática.

Artigo 14.º

Regime disciplinar

O não cumprimento das normas do presente regulamento pode determinar a abertura dos competentes procedimentos de natureza disciplinar, nos termos da lei, sem prejuízo da responsabilidade criminal que vier a ser apurada nessa sede.

CAPÍTULO IV

Disposições finais

Artigo 15.º

Procedimento, alvo de comunicação e localização da política

1 – O presente documento será entregue depois de devidamente aprovado pelo executivo da Câmara a todas as chefias, que por sua vez o entregam a todos os utilizadores. Os utilizadores têm obrigatoriamente que assinar o termo de compromisso anexo a este documento.

2 – Os termos de compromisso devidamente assinados, bem como o documento aprovado estará sempre disponível para consulta na intranet, o original ficará no GI, entidade responsável pela política.

Artigo 16°

Incidentes e suas consequências

Os incidentes envolvendo utilizadores são comunicados ao Administrador de Sistemas que deles dará conhecimento ao Vereador do Pelouro.

Artigo 17.º

Aprovação da Política

A aprovação da política deverá ser em Reunião de Câmara. Nessa aprovação deverá ser indicado quem foi o proponente do documento, ou seja, o autor da política. Deve também ser indicada a data da elaboração bem como a data de aprovação.

Artigo 18.º

Revisão do presente regulamento

O presente regulamento será revisto por iniciativa ou proposta dos órgãos municipais competentes, bem como a aprovação dessa revisão. Este processo é acompanhado da elaboração de um programa de revisão que ficará como histórico de revisões.

Artigo 19.º

Dúvidas e omissões

As dúvidas e omissões do presente regulamento serão resolvidas por recurso à interpretação da legislação habilitante, com base em critérios de equidade, mediante decisão da Câmara Municipal de … .

Artigo 20.º

Entrada em vigor

O presente documento entre em vigor no … dia útil seguinte ao da deliberação de aprovação pela Câmara Municipal.

ANEXO I

TERMO DE COMPROMISSO

O Utilizador _____

Declara ter conhecimento da Política de Segurança dos Sistemas de Informação do Município de … cujo conteúdo se compromete respeitar e fazer respeitar.

Município de … , _____ de _____ de _____

O utilizador _____

Referências

ACL (2001) Dicionário de Língua Portuguesa Contemporânea da Academia das Ciências de Lisboa, Lisboa, Verbo.

Aidar, M. (2003) A institucionalização da gestão e do desempenho organizacional por meio do Prêmio Nacional da Qualidade, Tese de Doutoramento em Administração de Empresas, Fundação Getúlio Vargas, Escola de Administração de Empresas de São Paulo, São Paulo.

Alavi, M. e Carlson, P. (1992) A review of MIS research and disciplinary development, Journal of Management Information Systems, 8(4), 45-62.

Alter, S. (1999) Information Systems: a Management Perspective, 3 edition, Addison-Wesley.

Amaral, L. A. M. (1994) PRAXIS: Um Referencial para o Planeamento de Sistemas de Informação. Tese de Doutoramento, Universidade do Minho, Braga.

Angell, I. O. e S. Smithson (1991) Information Systems Management: Opportunities and Risks, Information Systems Series. London: Macmillan Press.

ANMP (2007) Associação Nacional de Municípios Portugueses, (Acedido em 1 de Agosto de 2007 e 2 de Janeiro de 2012) http://www.anmp.pt/

Archer, M. (1988) Culture and agency, The place of culture in social theory, Cambridge University Press.

Aronowitz, S. (1992) The Politics of Identity: Class, Culture and Social Movements, New York: Routledge, Chapman and Hall.

Babbie, E.,1999. Métodos de Pesquisa de Survey. Belo Horizonte: Ed. da UFMG.

Babbie, E., 2010. The Practice of Social Research (Twelfth Ed.). Thomson Learning Inc.

Backhouse, J., Hsu, C. e Silva, L. (2006) Circuits of Power in Creating de Jure Standards: Shaping an International Information Systems Security Standard, MIS Quarterly, Vol. 30 Special Issue, 413 – 438.

Bardin, L., 2009. Análise de Conteúdo. Edições 70.

Barman, S. (2001) Writing Information Security Policies. Indianapolis: New Riders.

Baron, J., Dobbin, F. e Jennings, P. (1986) War and peace, the evolution of modern personnel administration in U.S. industry, American Journal of Sociology, 92, 384-411.

Banville, C. (1991) A Study of Legitimacy as a Social Dimension of Organizational Information Systems. In H.-E. Nissen, H. K. Klein e R. Hirschheim (Eds.), Information Systems Research: Contemporary Approaches & Emergent Traditions, Amsterdam, pp. 107–129. North-Holland.

Barry, C.A. (1998) Choosing Qualitative Data Analysis Software: Atlas/ti and Nudist Compared, Sociological Research Online, vol.3, n.3, (Acedido em 20 de Agosto de 2008)
http://www.socresonline.org.uk/3/3/4.html

Baskerville, R. e Siponen M. (2002) An information security meta-policy for emergent organizations. Logistics Information Management 15 (5/6), 337–346.

Bastos, E. R. (2002) Política de Segurança – Usuário Final, (Acedido em 24 de Junho de 2007)
http://www.secforum.com.br/article.php?sid=1244

Beatson, J. G. (1992) Information Security: The Impact of End User Computing. In G. G. Gable e W. J. Caelli (Eds.), IT Security: The Need for International Cooperation — Proceedings of the IFIP TC11 Eighth International Conference on Information Security, Amsterdam, pp. 35–45. Elsevier.

Benbasat, I., Goldstein, D. e Mead, M. (1987) The Case Research Strategy in Studies of Information Systems, MIS Quarterly, 11 (3), 369-386.

Berelson, B., 1952. Content Analysis in Communications Research. New York: Free Press.

Berger, P. e Luckmann, T. (2001) A construção social da realidade, tratado de sociologia do conhecimento, 20a. ed. Petrópolis: Vozes.

Björck, F. (2004) Institutional Theory, A New Perspective for Research into IS/IT Security in Organisations, HICSS, p. 70186b, Proccedings of the 37th Annual Hawaii International Conference on System Sciences, Track 7.

Bonoma, T (1985) Case research in marketing: Opportunities, Problems, and Process, Journal of Marketing Research, Vol XXII, May.

Bowden, S. (2003) Security Policy: What it is Why – The Basics, SANS Institute.

Brown, S. e Eisenhardt, K. (2004) Estratégia competitiva no limiar do caos: uma visão dinâmica para as transformações corporativas, São Paulo, Cultrix.

Buckingham, R., Hirschheim, R., Land, F. e Tully, C. (1987) Information Systems Curriculum: A basis for course design, in Buckingham, R., Hirschheim, R., Land, F. e Tully, C. (Eds.), Information Systems Education: Recommendations and Implementation, Cambridge University Press.

BS7799 (1996) Code of practice for information security management, London.

BSI (2008a) 100-1 1.5 – BSI Standard 100-1 Information Security Management Systems.

BSI (2008b) 100-2 2.0 – BSI Standard 100-2 IT-Grundschutz Methodology.

Caldeira, M. e Romão, B. (2002) Estratégias de Investigação em Sistemas de Informação Organizacionais - A Utilização de Métodos Qualitativos, Estudos de Gestão - Portuguese Journal of Management Studies, VII(1), 77-97.

Calhoun, C. (1991) The problem with identity in collective action, In Macro-Micro Linkages in Sociology, edited by Joan Huber (51-75), Beverly Hills, Sage.

Carneiro, A. (2002) Introdução à Segurança de Sistemas de Informação, FCA., Lisboa.

Carvalho, J. A. (1999) Information System? Which One Do You Mean? Págs. 259–280 of: Falkenberg, E., Lyytinen, K., e Verrijn-Stuart, A. (eds), ISCO 4 - Information Systems Concepts: An Integrated Discipline Emerging. Leiden, Holanda: Kluwer Academic.

Carvalho, J., Fernandes, M.J., Camões, P., Jorge, S. (2006) Anuário Financeiro dos Municípios Portugueses 2005, Câmara dos Técnicos Oficiais de Contas.

Carvalho, J., Fernandes, M.J., Camões, P., Jorge, S. (2011) Anuário Financeiro dos Municípios Portugueses 2009, Ordem dos Técnicos Oficiais de Contas.

Casola, V., Preziosi, R., Rak, M. e Troiano, L. (2005) A reference model for security level evaluation: Policy and fuzzy techniques, Journal of Universal Computer Science 11(1) 150-174.

Caupers, J. (1998) Direito Administrativo - Guia de Estudo, Editorial Notícias, Terceira Edição, Lisboa.

Chatterjee, D., Grewall, R. e Sambamurthy, V. (2002) Shaping up for E-commerce: Institutional enablers of the organizational assimilation of web technologies, MIS Quarterly, 26 (2), 65-89.

Checkland, P. e Holwell, S. (1998) Information, Systems and Information Systems: making sense of the field, Chichester: John Wiley & Sons.

Christensen, S., Karnoe, J., Pedersen, J. e Dobbin, F. (1997) Action in Institutions, American Behavioral Scientist, 40, 389-538.

COBIT (2007) COBIT 4.1 – Control and Audit for Information and Related Technology, IT Governance Institute.

Commons, J. (1950) The economics of collective action, Madison, University of Wisconsin.

Comunidade Portuguesa de Segurança da Informação (Acesso em 29 de Setembro de 2007)
http://ismspt.blogspot.com/2005/11/as-novidades-da-iso-27001.html

CRP (2002) Constituição da República Portuguesa por Gomes Canotilho e Vital Moreira, Coimbra Editora, 6º Edição.

CRP (2005) Constituição da República, Diário da República – I Série – A, nº 155, de 12 de Agosto.

Creswell, J. W (2003) Research design: Qualitative, quantitative, and mixed method approaches, Sage Publications, Thousand Oaks, California, second edition.

Cunha, P. R. (2000) Projecto de Sistemas de Informação para a realidade emergente: proposta baseada num modelo de carteira de soluções, Tese de Doutoramento, Universidade de Coimbra, Coimbra, Portugal.

Darke, P., Shanks, G. e Broadbent, M. (1998) Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism, Information Systems Journal, 8 (4) 273-289.

Denzin, N. K. e Lincoln, Y.S., (2000), Part III - Strategies of Inquiry, in Handbook of Qualitative Research, Eds. Denzin, N.K. e Lincoln, Y.S., pp. 365-378, Sage Publications, Thousand Oaks, Second edition.

Dhillon, G. (1997) Managing Information System Security, Information Systems Series, Macmillan Press, London.

Dhillon, G. e Backhouse J. (1997) Managing for secure organizations: a critique of information systems security research approaches. Relatório Técnico, London School of Economics Computer Security Research Centre, London.

Dhillon, G e Backhouse, J. (2000) InformationSystem Security Management in the New Millennium, Communications of ACM, 43 (7), 125-128.

Dhillon, G. (2007) Principles of Information Systems Security: Text and Cases, John Wiley & Sons, Hoboken.

DiMaggio, P. e Powell, W. (1983) The iron cage revisited, institutional isomorphism and collective rationality in organizational fields, American Sociological Review, 48, 147-160.

DiMaggio, P. e Powell, W. (1991) Introduction, The New Institutionalism in Organizational Analysis, edited by Powell W.W. e DiMaggio P. J., Chicago, University of Chicago Press.

Diver, S. (2007) Information Security Policy – A Development Guide for Large and Small Companies. SANS Institute.

Doherty, N. e Fulford, H. (2006), Aligning the information security policy with the strategic information systems plan, Computers & Security 25(1), 55-63.

Edelman, L. (1992) Legal ambiguity and symbolic structures, organizational mediation of civil rights law, American Journal of Sociology, 97,1531-1576.

Ein-Dor, P. e Segev E. (1993) A Classification of Information Systems: Analysis and Interpretation. Information Systems Research 4 (2), 166–204.

Emirbayer, M. e Mische, A. (1998) What is agency? American Journal of Sociology, 103, 962-1023.

Falkenberg, E. D., Hesse, W., Lindgreen, P., Nilsson, B. E., Oei, J. L. H., Rolland, C., Stamper, R. K., Assche, F. M. V., Verrijn-Sturart, A. A. e Voss, K. (1996), FRISCO - A framework of Information System Concepts. Relatorio Tecnico. IFIP.

Falkenberg, E. D., Hesse, W., Lindgreen, P., Nilsson, B. E., Oei, J. L. H., Rolland, C., Stamper, R. K., Assche, F. M. V., Verrijn-Sturart, A. A., e Voss, K. (2001) FRISCO - A framework of Information System Concepts. Relatorio Tecnico, IFIP.

Fligstein, N. (1985) The spread of the multidivisional form among large firms, 1919-1979, American Sociological Review, 50, 377-391.

Fligstein, N. (2001) Social skill and the theory of fields, Sociological Theory, 19, 105-125.

Forcht, K. e Ayers, W. (2001) Developing a Computer Security Policy For organizational Use And Implementation. Journal of Computer Information Systems; 41 (2), 52-57.

Freitas do Amaral, D. (1989) Curso de Direito Administrativo, Vol. I, Livraria Almedina, Coimbra.

Fulford, H. e Doherty, N. F. (2003) The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security & Computer Security 11 (3), 106-114.

Galliers, R. (1987) Information Analysis: Selected Readings, Addison-Wesley. ISBN 0-201-19244-6.

Gaunt, N. (1998) Installing an appropriate information security policy, International Journal of Medical Informatics 49(1) 131-134.

GDLP (1991) Grande Dicionário de Língua Portuguesa, Lisboa, Circulo de Leitores.

Ghiglione, R. and Matalon, B., 1997. O Inquérito: Teoria e Prática. 3ª Ed. (Trad Portuguesa). Oeiras: Celta Editora.

GIAC (2001) GIAC Basic Security Policy, V. 1.4 February 27, SANS Institute.

Giddens, A. (1979) Central Problems in Social Theory, Action, Structure and the Contradiction in Social Analysis, Berkeley, University of California.

Giddens, A. (1984) The Constitution of Society, Berkeley, University of California Press.

Gilbert, C. (2003) Guidelines for an Information Sharing Policy, SANS Institute.

Greenwood, R. e Hinings, C. (1996) Understanding radical organizational change, Bringing together the old and new institutionalism, Academy of Management Review, 21, 1022-1105.

Greif, A. (2006) Institutions and the path to modern economy: lessons from medieval trade, Cambridge, Cambridge University Press.

Guel, M, (2007) A short Primer for Developing Security Policies, SANS, (Acedido em 1 de Junho de 2008)
https://www.sans.org/resources/policies/Policy_Primer.pdf.

Hartley, J. (1994) Case Studies in Organizational Research, in Cassall, C. E Symon, C. (Eds.), Qualitative Methods in Organizational Research: A Practical Guide, Sage Publications, 208-229.

Hartley, B. e Locke, A. (2001) The Process of Security, Business Security Advisor, 22-24, USA.

Herkner, W., 1974. Inhaltsanalyse. In Jürgen von Koolwijk & Maria Wieken-Mayser (Eds.). Techniken der empirischen Sozialforschung, Vol. 3. pp. 158-191

Higgins, H. N. (1999) Corporate system security: towards an integrated management approach. Information Management & Computer Security 7 (5), 217–222.

Holsti, Ole R., 1968. Content Analysis, in Gardner Lindzey & Elliot Aronson (Eds.), The Handbook of Social Psychology, (2nd edn), Vol. 2, pp. 596-692.

Höne, K. e Eloff, J. (2002a) Information security policy — what do international information security standards say?, Computers & Security 21 (5), 402–409.

Höne, K. e Eloff, J. (2002b) What makes an effective security policy?, Network Security 6 (1), 14–16.

Hong, K.S., Chi, Y. P., Chão L. R. e Tang J. H. (2003). An integrated system theory of information security management. Information Management & Computer security 11(5), 243-248.

Humphreys, T. (2000, December). Finding a language to address information security management. (Acedido em 30 de Agosto de 2007)
http://www.iso.org/iso/en/commcentre/pdf/ISMlanguage0012.pdf

Infopédia (2008) Enciclopédia e dicionários, Porto Editora. (Acedido em 13 de Dezembro de 2008)
http://www.infopedia.pt/

ISF (2007) The Standard of Good Practice for Information Security, Information Security Forum.

ISO/IEC 17799 (2005) International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, International Organization for Standardization/International Electrotechnical Commission.

ISO/IEC 27001 (2005) Information technology — Security techniques — Information security management systems — Requirements, International Organization for Standardization/International Electrotechnical Commission.

ISO/IEC 27002 (2005) Information technology — Security techniques — Information security management systems — Requirements, International Organization for Standardization/International Electrotechnical Commission.

ISSA (2004) GAISP V. 3.0—Generally Accepted Information Security Principles.

JISC (2001) Developing an Information Security Policy. Joint Information Systems Committee (JISC), (Acedido em 16 de Junho de 2007).
http://www.jisc.ac.uk/uploaded_documents/smbp13.pdf

Justicia, J. M. (2005) Análisis cualitativo de datos textuales con ATLAS.ti 5, Universidade Autònoma de Barcelona, Noviembre, Versão 3.03.

Kamens, D. (1977) Legitimating myths and educational organization: the relationship between organizational ideology and formal structure, American Sociological Review, 42, 208-19.

Karyda, M., Kiountouzis, E. e Kokolakis, S. (2005) Information systems security policies: a contextual perspective, Computers & Security 24 (3) 246-260.

Kee, C. (2001) Security Policy Roadmap – Process for Creating Security Policies, SANS Institute.

Khazanchi, D., e Munkvold, B. E. (2000) Is Information Systems a Science? An Inquiry into the Nature of the Information Systems Discipline. Data Base For Advances In Information Systems, 31(3), 24–42.

King, C. M., Dalton, C. E. e Osmanoglu T. E. (2001) Security Architecture: Design, Deployment, and Operations. Berkeley: Osborne/McGraw-Hill.

King, J. , Gurbaxani, V., Kraemer, L.,McFarlan, W., Raman, S. e Yap, S. (1994) Institutional factors in information technology innovation, Information Systems Research, 5(2), 139-169.

Klein, H. e Myers, M. (1999) A Set Principles for Conducting and Evaluating Interpretive Field studies in Information Systems, MIS Quarterly, 23 (1), 67-93.

Knapp, K., Marshall, R., Rainer, K e Ford, N. (2006) Information Security: Management's Effect on Culture and Policy, Information Management & Computer Security, 11 (1), 24-36.

Kotulic, A. e Clark, J. (2004) Why there aren't more information security research studies, Information & Management, 41 (5), 597-607.

KPMG (2002) KPMG 2002 Global Information Security Survey. (Acedido em 24 de Junho de 2007).
http://www.kpmg.com/microsite/informationsecurity/issurvey.html

Lacity, M., Janson, M. (2001) Understanding Qualitative Data: A Framework of Text Analysis Methods, Journal of Management Information Systems/Fall 1994, 11 (2), 137-155.

Le Moigne, Jean-Louis (1990) La théorie du système general – Théorie de la modélisation, 3 Edition, na Versão Portuguesa "A Teoria do Sistema Geral", 1996, Instituto Piaget, Lisboa.

Lee, A. (1989) A scientific methodology for MIS case studies, MIS Quarterly, 13 (1), 33-50.

Lee, A. (1991) Integrating Positivist and Interpretive Approaches to Organizational Research, Organization Science, 2 (4), 342-365.

Lee, D. (2001) Developing Effective Information Systems Security Policies", SANS Institute.

Lexiciteca (1985) Lexiciteca, Lisboa, Circulo de Leitores.

Locke, L. F., Spirduso, W.W. e Silverman, S. J. (2007) Propostas That Work: A Guide for Planning Dissertations and Grant Propostas, SAGE Publications, Newburg Park, 5th edition.

Macartney, L. A. (2005). "Information Security Harmonisation – Classification of Global Guidance", Information Systems Audit and Control Association, USA.

Macedo, P., Zacarias, M. e Tribolet, J. (2006) Técnicas e Métodos de Investigação em Engenharia Organizacional: Projecto de Investigação em Modelação de Processos de Produção, (Acedido em 4 de Dezembro de 2006).
www.inesc-id.pt/ficheiros/publicacoes/2650.pdf

MacNealy, M. S. (1997) Toward Better Case Study Research, IEEE Transactions on Professional Communication 40(3), 182-196.

MacQueen, K.; McLellan, E.; Kay, K. e Milstein, B. (1998) Codebook Development for Team-Based Qualitative Analysis. Cultural Anthropology Methods 10(2), 31-36.

Mamede, H. (2006) Segurança Informática nas Organizações, FCA, Lisboa.

March, J. Olsen, J. (1989) Rediscovering Institutions, Organizational Basis of Politics, New York.

Marcos, E. (2006) Investigación en Ingeniería del Software vs Desarrollo Software, Universidade Rey Juan Carlos, Grupo KYBELE, (Acedido em 4 de Dezembro de 2006) http://kybele.escet.urjc.es/MIFISIS2002/Articulos%5CArt11.pdf

Marta, R. e Santiago, M. (2004) Segurança de sistemas de informação: O puzzle sempre incompleto, Palestra promovida pela FEUP e SecurNet, (Acedido em 20 de Agosto de 2007).
www.fe.up.pt/~jvv/Assuntos/palestras/securnet/RuiMarta.ppt

McClintock , C., Brannon, D. e Maynard-Moody, S. (1979) Applying the Logic of Sample Surveys to Qualitative Case Studies: The Case Cluster Method, Administrative Science Quarterly, 24 (4), 612-629.

Meneses, A. (2008) Autarquias, QREN e o Mercado de Tecnologias de Informação, e-Business Report – Casos de Sucesso na Modernização da Administração Pública, nº441/nº31 de 15 de Maio.

Merten, K.,1983. Inhaltsanalyse. Einführung in Theorie, Methode und Praxis, Opladen: Westdeutscher Verlag.

Meyer, J., Boli, J. e Thomas, G. (1994) Ontology and rationalization in the western cultural account, In Scott, R. Meyer, J., Institutional Environments and Organizations, London, Sage.

Meyer, J. e Rowan, B. (1977) Institutionalized organizations: formal structure as yth and ceremony, American Journal of Sociology, 83, 340-63.

Meyer, J. e Rowan, B. (1992) Institutionalized organizations: formal structures as myth and ceremony, Sage, 21-44.

Meyer, J. e Scott, R. (1983) Organizational Environments, Ritual and Rationality, Berverly Hills, Sage.

Mingers, J., e Stowell, F. (1997) Information Systems: An Emerging Discipline?, McGraw-Hill.

Mintzberg, H., Ahlstrand, B. e Lampel, J. (2000) Safári de estratégias, Porto Alegre, Bookman.

Myers, M. D. (2007) Qualitative Research in Information Systems, (Acedido em 19 de Março de 2007).
http://www.qual.auckland.ac.nz

Nelson, R. e Soete, L. (1988) Policy Conclusions, in G. Dosi et al., Technical Change and Economic Theory, Pinter Publishers, New York, 631-636.

Nelson, R. e Winter, S. (1982**)** An Evolutionary Theory of Economic Change, Cambridge, Mass., Harvard Univ, Press.

NIST (1995, October) NIST SP800-12 – An Introduction to Computer Security: The NIST Handbook.

NIST (2006, October) Information Security Handbook: A Guide for Managers, Recommendations of the National Institute of Standards and Technology.

NIST (2007, March) NIST SP800-100 – Information Security Handbook: A Guide for Managers.

NIST (2009, August) NIST SP800-53 – Recommended Security Controls for Federal Information Systems and Organizations.

North, D. (1990) Institutions, institutional change and performance, Cambridge, University Press, Cambridge.

Oliver, C. (1991) Strategic Responses to Institutional Processes, Academy of Management Review, 16 (1), 145-179.

Oliver, C. (1992) The Antecedents of Deinstitutionalization. Organization Studies, 13(4), 563-588.

OOIT (2007) Office of Information Technology, Information Security Guidelines for NSW Government Agencies, (Acedido em 16 de Junho de 2007). http://www.gcio.nsw.gov.au/documents/Information%20Security%20Guideline%20V1.1.pdf

Orlikowski, J. (1992) The duality of technology: Rethinking the concept of technology in organizations, Organization Science: A Journal of the Institute of Management Sciences, 3(3), 398-426.

Orlikowski, J.,Yates, J.,Okamura, K. e Fujimoto, M. (1995) Shaping electronic communication, The metastructuring of technology in use, Organization Science 6(4), 423–444.

Orlikowski, W. J. e Baroudi, J. J. (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions, Information Systems Research (2), 1-28.

Ortner, S. (1997) Making gender, The politics and erotics of culture, Beacon Press.

OSIC e UMIC (2004) Inquérito à Utilização das Tecnologias da Informação e da Comunicação nas Câmaras Municipais 2004, Observatório da Sociedade da Informação e do Conhecimento e Agência para a Sociedade do Conhecimento.

OSIC e UMIC (2006) Inquérito à Utilização das Tecnologias da Informação e da Comunicação nas Câmaras Municipais 2006, Observatório da Sociedade da Informação e do Conhecimento e Agência para a Sociedade do Conhecimento.

Patrick, W. F. (2001) Creating an Information Systems Security Policy", SANS Institute.

Peltier, T. R. (1999) Information Security Policies, Procedure: a practitioner's reference, CRC Press.

Peltier, T. R. (2002) Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications.

Pereira, H. B. (2002) Análises experimental de los criterios de evaluación de usabilidad de aplicaciones multimédia en entornos de educación y formación a distancia, Tesis Doctoral, Universitat Politécnica de Catalunya.

Pierson, P. (2004) Politics in Time, History, Institutions, and Social Analysis, Princeton, Princeton University Press.

Pintos, J e Romanos, P. (2007) Experiencias en el cumprimento de la DA 669/04, Ministerio da Justicia y Derechos Humanos, (Acedido em 2 de Julho de 2007). http://www.arcert.gov.ar/ncursos/material/experiencias_da/presentacion_Justicia_DA669.pdf

Polis (1983) Enciclopédia VERBO da Sociedade e do Estado, Antropologia, Direito, Economia, Ciências Políticas, 1 – A.C, Editorial Verbo, Lisboa.

Portal Cidades Digitais (2008) Projecto Cidades e Regiões Digitais, (Acedido em 18 de Agosto de 2008).
http://www.cidadesdigitais.pt

Portal do Governo (2008) Plano Tecnológico, (Acedido em 18 de Agosto de 2008)
http://www.governo.gov.pt/NR/rdonlyres/F746C341-BDA9-4FCF-AE25-25A72A89C9CC/0/UCTP_15.pdf

Portal do Governo (2011) Programa do XIX Governo Constitucional, (Acedido em 30 de Dezembro de 2011)
http://www.portugal.gov.pt/media/130538/programa_gc19.pdf

Porter, M. (1998) Clusters and the New Economics of Competition, in Havard Bussiness Review, November-December.

POSI / UMIC (2003) Guia de Operacionalização – Cidades e Regiões Digitais, Programa Operacional Sociedade da Informação e Unidade da Missão Inovação e Conhecimento.

Powell, W. e DiMaggio, P. (1991) The new institutionalism in organizational analysis, University of Chicago Press, Chicago and London.

Prates, A. (2000) Organização e instituição no velho e novo institucionalismo, In: Rodrigues, S. e Cunha, M., Novas perspectivas na administração de empresas: uma colectânea luso-brasileira, São Paulo, Iglu, 2000.

Premkumar, G., Ramamurthy, K. e Crum, M (1997)Determinants of EDI Adoption in the Transportation Industry. European Journal of Information Systems, 6, 107-121.

Rossman, G. B. e Rallis, S. F. (1998) Learning in the field: An introduction to qualitative research. Thousand Oaks, CA: Sage.

Rowan, B. (1982) Organizational structure and the institucional environmente: the case of public schools, Administrative Science Quarterly, 27, 259-279.

Santos, L. e Amaral, L. (2008) Presença na internet das câmaras municipais portuguesas em 2007: estudo sobre local eGovernment em Portugal, Gávea, Guimarães.

de Sá-Soares, D. (2009) Interoperabilidade entre Sistemas de Informação na Administração Pública, Tese de Doutoramento em Tecnologias e Sistemas de Informação, Engenharia e Gestão de Sistemas de Informação, Universidade do Minho, Guimarães.

de Sá-Soares, F. (2005) Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção, Tese de Doutoramento em Tecnologias e Sistemas de Informação, Engenharia e Gestão de Sistemas de Informação, Universidade do Minho, Guimarães.

de Sá-Soares, F. (2010) A Codebook for Coding Information Security Policies, Technical Report, University of Minho, Guimarães.

Schneier, B. (2000) Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons.

Schweitzer, J. A. (1982) Managing Information Security: A Program for the Electronic Information Age, Butterworth-Heinemann, Boston.

Scott, M. e Lyman, S. (1968) Accounts, American Sociological Review, 33, 46-62.

Scott, W., Ruef, M., Mendel, P. e Caronna, C. (2000) Institutional Change and Healthcare Organizations: From Profissional Dominance to Managed Care, Chicago, University of Chicago Press.

Scott, W. (1995) Institutions and organizations, Thousand Oaks, Sage.

Scott, W. (2001) Institutions and organizations, Thousand Oaks, Sage.

Scott, W. (2003) Institutional carriers, Reviewing modes of transporting ideas over time and space and considering their consequences, Industrial and Corporate Change 12, 879-894.

Scott, W. (2004) Institutional theory in Encyclopedia of Social Theory, George Ritzer, Thousand Oaks, Sage, 408-414.

Scott, W. (2008) Institutions and organizations – Ideas and Interests, Third Edition, Sage.

Sewell, W. (1992) A theory of structure: Duality, agency, and transformation, American Journal of Sociology, 98, 1-29.

Shorten, B. (2004) Information Security Policies from the Ground Up. In H. F. Tipton e M. Krause (Eds.), Information Security Management Handbook (Fifth ed.), 917–924. Boca Raton: Auerbach.

Silbermann, A., 1974. Systematische Inhaltsanalyse. In René König (Ed.). Handbuch der empirischen Sozialforschung, Vol. 4, pp. 253-339.

Silva, J. (2007) Institucionalização de Práticas Organizacionais em Organizações Inovadoras, Universidade do Vale do Rio dos Sinos – UNISINOS, Programa de pós-graduação em Administração Nível Mestrado, São Leopoldo.

Siponen M. (2000a) A conceptual foundation for organizational information security awareness, Information Management and Computer Security, 8(1) 31-41.

Siponen M. (2000b) Policies for construction of information systems security guidelines, In: Qing S, Eloff JHP, Information security for global information infrastructures, Kluwer Academic Publishers, 112-120.

Somers, A. e Gibson, G. (1994) Reclaiming the epistemological “other”: Narrative and the social constitution of identity, Oxford.

Stake, R. E. (2000) Case Studies, in Norman K. Denzin e Yvonna S. Lincoln (ed.), Handbook of Qualitative Research, Sage Publications, Thousand Oaks, capítulo 16, 435-454, Second edition.

STAPE (2008a) Recenseamento Eleitoral, publicado no Mapa nº 11/2008, do Diário da República, II série de 4-Março-2008.

(Acesso em 7 de Julho de 2008) http://www.stape.pt/recensel/resultados.htm

STAPE (2008b) Secretariado Técnico dos Assuntos Para o Processo Eleitoral, Registo dos Eleitos para os Órgãos das Autarquias Locais, Eleições de 09 de Outubro de 2005, Ministério da Administração Interna.
(Acesso em 7 de Julho de 2008). http://www.stape.pt/autarquias/registel06.htm

Stemler, S., 2001. An overview of content analysis. Practical Assessment, Research & Evaluation, Vol. 7, No. 17.

Strang, D. (1990) From dependency to sovereignty: an event history analysis of decolonization 1870-1987, American Sociological Review, 55, 846-60.

Strang, D. e Meyer, J. (1993) Institutional conditions for diffusion, Theory and Society, 22, 487-511.

Teo, H., Wei, K e Benbasat, I (2003) Predicting intention to adopt interorganizational linkages: An institutional perspective, MIS Quarterly, 27(1), 19-49.

Titscher, S. et al, 2000. Methods of Text and Discourse Analysis (First ed.). Sage Publications.

Tobert, P. e Zucker, L. (1983) Institutional sources of change in the formal structure of organizations: the diffusion of civil service reform, 1880-1935, Administrative Science Quarterly, 28, 22-39.

Tolbert, P. e Zucker, L. (1999) A Institucionalização da Teoria Institucional, Clegg, S.; Hardy, C. e Nordy, W., Handbook de Estudos Organizacionais, Atlas.

Tudor, J, K. (2001) Information Security Architecture: Na Integrated Approach to Security in the Organization, CRC Press LLC.

Veblen, T. (1994) The theory of the leisure class, Dover Thrift editions.

Veiga, P. (2004) Tecnologias e Sistemas de Informação, Redes e Segurança, Edições SPI – Principia, Porto.

Visala, S. (1991) Broadening the Empirical Framework of Information Systems Research. In H.-E. Nissen, H. K. Klein e R. Hirschheim (Eds.), Information Systems Research: Contemporary Approaches & Emergent Traditions, Amsterdam, pp. 347–364. North-Holland.

Walsham, G. (1993) Interpreting Information Systems in Organizations, Wiley Series in Information Systems, Chichester: John Wiley & Sons.

Walsham, G. (1995) Interpretive Case Studies in IS Research: Nature and Method, European Journal of Information Systems, 4 (2), 74-81.

Walton, J. P. (2002) Developing an Enterprise Information Security Policy, SIGUCCS, 153-156.

Weber, R., 1990. Basic Content Analysis (Second ed.). Sage University Paper.

Weick, K. (1979) The social Psychology of Organizing, 2nd ed., Reading, Addison-Wesley.

Weick, K. (1995) Sensemaking in Organizations, Thousand Oaks, Sage.

Weick, K. (2003) Enacting an Environment: The Infrastructure of Organizing, in: Debating Organization, Point-Counterpoint in Organization Studies, R. Westwood and S. Clegg, Blackwell Publishing, London.

Weingast, B. (2002), Rational choice institutionalism. In The State of the Discipline, Ira Katznelson and Helen Milner, W. W. Norton, New York, 660-692.

Whitman (2004) In defense of the realm: Understanding threats to information security, Informational Journal of Information Management, 24, 3-4.

Whitman, M. e Mattord, H. (2005) Principles of Information Security, Course Technology, US, Second edition.

Whitman, M., Townsend, A. e Aalberts, R. (2001) Information Systems Security and the Need for Policy, In: Dhillon, G. "Information security management: global challenges in the new millennium", Idea Group Publishing.

Wills, L. (2002) Security Policies: Where to Begin, Security Essentials, 1(4b).

Wood, C. C. (1995) Writing InfoSec Policies, Computers & Security, 14 (8), 667-674.

Wood, C. C. (1999) Information Security Policies Made Easy, Baseline Software, San Rafael.

Yin, R. (1989) Case Study Research. Design and Methods, Sage Publications, London.

Yin, R. (1994) Case Study Research. Design and Methods, Sage Publications, Thousand Oaks, Second edition.

Zhou, X. (1993) Occupational power, state capacities, and the diffusion of licensing in the American states: 1890-1950, American Sociological Review, 58, 536-52.

Zucker, L. (1987) Institutional theories of organization, Annual Review of Sociology, 13(1), 443-464.

Zucker, L. G. (1988) Where do institutional patterns come from? Organizations as actors in social systems, in Lynne G. Zucker (ed.), Institutional patterns and organizations: Culture and environment, Cambridge, Mass., Ballinger, 23-49.