

Avaliação da Segurança de Sistemas de Informação nas Autarquias Locais: Um Estudo de Caso num Município do Médio Tejo

Célio Gonçalo Marques¹, Sofia Cassis², Carlos Trigacheiro³

celiomarques@ipt.pt; sofia.cassis@gmail.com; carlostrigacheiro@ipt.pt

¹ Laboratório de Inovação Pedagógica e Educação a Distância (LIED.IPT), Instituto Politécnico de Tomar, Portugal Centro de Administração e Políticas Públicas (CAPP), Universidade de Lisboa, Portugal

² Instituto Politécnico de Tomar, Portugal

³ Instituto Politécnico de Tomar, Portugal

Pages: 1-16

Resumo: Numa Era caracterizada pela importância da informação, a generalidade das organizações depende fortemente dos Sistemas de Informação para o desempenho da sua missão. Para as Autarquias Locais, onde se verificam constantes mudanças nos processos organizacionais com o objetivo de uma melhor utilização económica, eficiente e equitativa dos recursos públicos, os Sistemas de Informação são um fator-chave. Ao lidarem diariamente com informação confidencial estão sujeitas a obrigações de conformidade ética e legal que geram grande responsabilidade na gestão da informação que tratam e produzem. Com este estudo de caso pretendeu-se aferir, através da aplicação de um inquérito por questionário baseado na ISO/IEC 27002:2013 associado a um modelo de maturidade qual o grau de maturidade dos controlos de segurança do Sistema de Informação num Município do Médio Tejo (MMT). A aplicação destas ferramentas permitiu identificar quais as áreas mais críticas e formas de melhorar os processos.

Palavras-chave: Autarquias Locais; ISO/IEC 27002:2013; modelo de maturidade; Segurança da Informação.

Evaluation of Information Systems Security in Local Municipalities: a Case Study in a Médio Tejo Municipality

Abstract: In a time characterized by the importance of information, most organizations strongly depend on information systems for the fulfilment of their mission. For local Municipality Halls, where there are constant changes in organizational processes aimed at economically, efficiently and equitably improving the usage of public resources, information systems are key factors. Dealing daily with confidential information, they are subject to obligations of ethical and legal conformity that imply great responsibility in the management of the information they process and generate. This study aimed at understanding, through a questionnaire based on ISO/IEC 27002:2013 associated with a maturity model,

what is the degree of maturity of the security controls in the information system of a municipality in the Médio Tejo region (MMT). The application of these tools allowed the identification of the most critical areas and ways to improve processes.

Keywords: Local Municipality Hall; ISO/IEC 27002:2013; maturity model, information security.

1. Introdução

Numa Era em que todas as organizações lidam no seu dia a dia com informação dos seus colaboradores, fornecedores, parceiros, utilizadores, etc., esta tornou-se um ativo essencial, que precisa de ser adequadamente protegido.

Gouveia e Ranito (2004) referem que para as autarquias locais, que tratam com dados muito sensíveis e oficiais, a pressão é ainda maior, uma vez que as comunicações eletrónicas com o cidadão/município, criam portas de entrada potencialmente perigosas, se não forem devidamente acauteladas.

A par da evolução das tecnologias da informação e comunicação, da dependência crescente entre o bom funcionamento das organizações e o normal funcionamento dos Sistemas de Informação, está o aumento da criminalidade Informática, que se manifesta através de técnicas de intrusão e aproveitamento de vulnerabilidades, impondo melhorias constantes aos paradigmas da segurança.

Beal (2005) refere que as organizações precisam adotar controlos de segurança (medidas de proteção que abrangem uma grande diversidade de iniciativas) que sejam capazes de proteger adequadamente dados, informações e conhecimentos.

A Segurança da Informação é conseguida através da implementação de um conjunto de controlos adequados (políticas, procedimentos, processos, estruturas organizacionais) que têm de ser estabelecidos, implementados, monitorizados, revistos e melhorados continuamente de forma a proteger o Sistema de Informação impedindo o acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados da informação, preservando a confidencialidade, integridade/autenticidade e disponibilidade da informação.

De acordo com Gouveia e Ranito (2004) sendo a informação umas das preocupações mais dominantes da sociedade é necessário que as organizações atribuam uma parcela aceitável do seu esforço no desenvolvimento infraestruturas adequadas para a sua recolha, armazenamento, processamento, representação e distribuição.

Nos últimos anos tem-se verificado um desenvolvimento de normas e frameworks, reconhecidas internacionalmente, que definem princípios, conceitos, controlos e componentes de gestão de segurança de informação, que visam apoiar as organizações na implementação de um Sistema de Gestão de Segurança da Informação.

Pedro (2010) refere que, devido aos novos Sistemas de Informação que estão a ser adotados por muitas organizações, foi necessária a evolução das normas técnicas de boas práticas ou standards relacionados com as Tecnologias de Informação e Comunicação de forma a acompanharem esta nova realidade.

O mesmo autor considera ainda que estes novos standards técnicos podem ser utilizados em auditoria como referenciais para avaliação comparativa de conformidade e controlo dos Sistemas de Informação e procedimentos instituídos, pois ilustram procedimentos aceites generalizadamente.

Estas normas e frameworks são aplicáveis às Autarquias Locais, representam baixos custos e são uma ótima opção, pois podem ser aplicadas pelos recursos internos, não sendo necessário recorrer à contratação de serviços externos.

Com este estudo de caso pretende-se:

- Efetuar uma análise de segurança aos controlos de segurança do Sistema de Informação do Município baseada nos controlos previstos na norma ISO/IEC 27002;
- Classificar o nível de maturidade dos controlos utilizando um modelo de maturidade de segurança;
- Apresentar resultados sob a forma quantitativa permitindo de forma simples identificar as áreas mais críticas.

No domínio da investigação observa-se a existência de um número razoável de estudos sobre Segurança de Sistemas de Informação e sobre a aplicação da ISO 27002, contudo, o número de estudos aplicados a Autarquias Locais em Portugal é praticamente inexistente, com este trabalho visa contribuir-se para colmatar esta lacuna.

O Município não possui um método de avaliação da adequação dos controlos de segurança do Sistema de Informação implementados, este facto pode levar a que os controlos adotados não sejam os ideais, originando uma maior exposição ao risco.

Este estudo irá contribuir para uma melhoria dos procedimentos atuais de proteção da informação no Município, pois uma avaliação baseada na ISO/IEC 27002:2013 permite uma visão abrangente de todo o Sistema de Informação, possibilitando uma melhor perceção da adequação dos controlos utilizados e se necessário melhorá-los de forma a obter um Sistema de Informação mais robusto.

Esta avaliação pode também ser utilizada como suporte para a tomada de decisões relacionadas com melhorias e investimento necessários para assegurar a Segurança da Informação, bem essencial da organização.

Por uma questão de segurança e confidencialidade, o nome do Município foi omitido, sendo usada a designação Município do Médio Tejo (MMT).

Começamos por efetuar um breve enquadramento teórico do trabalho, onde se destaca a apresentação da norma ISO 27002:2013. Segue-se a descrição das opções metodológicas e a apresentação dos resultados, onde é feita uma análise dos diferentes pontos da norma. Terminamos com as considerações finais do estudo.

2. Fundamentação Teórica

Com o aumento da dependência em relação às tecnologias de informação também a Administração Pública Local se deparara com um conjunto de questões que, até ao momento, não se colocavam.

Carneiro (2002) refere que é necessária a aplicação de diferentes mecanismos de proteção, deteção e reação, bem como a formulação de políticas de segurança que contribuam para a preservação da confidencialidade, integridade e disponibilidade da informação.

Os municípios esperam que as autarquias modernizem os seus Sistemas de Informação, disponibilizando serviços que melhorem o seu bem-estar e a sua qualidade de vida.

Torna-se necessário que os Sistemas de Informação utilizados transmitam confiança aos municípios, sendo para isso necessário garantir a existência de segurança nos portais de acesso, a proteção das redes de transmissão e tecnologias de suporte à informação e comunicação e, a confidencialidade das bases de dados.

Lopes (2012) refere que 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 atividades de planeamento e desenvolvimento de SI.

Analisadas algumas das principais metodologias utilizadas na área de gestão de Segurança da Informação (ISO 27002:2013, COBIT e ITIL) concluiu-se que aquela que mais se adequava à realização deste trabalho é a ISO 27002:2013.

A ISO 27002:2013 é um código de boas práticas para a gestão da segurança dos Sistemas de Informação. Esta norma estabelece diretrizes e procedimentos para iniciar, implementar, manter e melhorar a gestão de segurança de uma organização e, em conjunto com um modelo de maturidade de segurança, permite medir a performance da Segurança da Informação nas organizações.

“Trata-se, no fundo, de um código de boas práticas que inclui um extenso conjunto de controlos que indicam a forma de atuação para que os objetivos definidos nas políticas possam ser atingidos” (Carvalho, 2018, p. 18).

O facto de ser integralmente fundamentada na Segurança da Informação torna-a a solução mais completa e abrangente, a sua amplitude e facilidade de aplicação tornaram esta norma não apenas alvo de destaque, mas a primeira escolha para uma análise mais aprofundada.

Esta norma tem como objetivo fornecer diretrizes para práticas de gestão de Segurança da Informação e normas de Segurança da Informação para as organizações, incluindo a seleção, a implementação e gestão de controlos, levando em consideração os ambientes de risco da Segurança da Informação da organização (ISO/IEC 27002:2013, 2013).

A norma está estruturada em 19 secções, do 0 a 4 são a introdução, a partir da 5 são sobre Segurança da Informação. Estas 14 secções contêm 35 objetivos de controlo e 114 controlos.

As 14 secções sobre Segurança da Informação, abrangem a Segurança da Informação em todos os seus aspetos, tratando de ferramentas, processos e pessoas, envolvendo soluções tecnológicas, documentação de processos e consciencialização de pessoas.

A utilização de um modelo de maturidade permite identificar lacunas que representam riscos de segurança e pontos de melhoria, é como um guia para avaliar e perceber em

que ponto a organização se encontra e orientar melhorias de forma a chegar a um nível de maturidade mais elevado, sempre em busca da excelência.

A utilização destes modelos insere o fator tempo no processo de gestão da Segurança da Informação, o que incute transparência ao processo, permitindo a comparação entre ciclos de avaliação e, até mesmo, entre organizações (benchmark).

O modelo utilizado, de Trigacheiro (2012), define seis níveis para medir a maturidade dos processos de TI.

0 - Inexistente – A organização não reconhece a existência de um processo a ser seguido.

1 – Inicial / ad hoc – O processo de segurança está deficientemente definido. Há evidências de que a organização reconhece que o processo existe, no entanto, os processos não estão normalizados, isto é, são aplicados de forma ad-hoc e casuística.

2 – Repetitivo / consistente – Abordagem repetitiva e disciplinada à realização do processo de segurança. Os processos são desenvolvidos de forma semelhante por pessoas que desenvolvem a mesma tarefa. Não há uma política de formação e comunicação de procedimentos normalizados. Há um alto grau de dependência do conhecimento dos indivíduos e, portanto, os erros são prováveis.

3 – Definido / integrado – Existem procedimentos para melhorar e aprofundar a segurança dos Sistemas de Informação. Os processos estão normalizados e documentados e são divulgados em formação. É obrigatório que os processos sejam seguidos, pelo que é improvável que sejam detetados desvios. Os processos não são sofisticados, mas existe a formalização das práticas existentes.

4 – Gerido e mensurado – Os procedimentos de segurança estão interligados e suportam o planeamento estratégico da organização. A gestão faz a monitorização e mensuração da conformidade com os procedimentos e toma medidas quando os procedimentos não atuam efetivamente. Os processos são melhorados frequentemente de acordo com as boas práticas. São usados automatismos e ferramentas de forma limitada e fragmentada.

5 - Otimizado – Processo de melhoria contínua. Os processos são refinados ao nível das boas práticas, baseados nos resultados de contínuas melhorias e de modelagem de maturidade com outras organizações. As tecnologias de informação são usadas de forma integrada para automatizar o fluxo de trabalho, fornecendo ferramentas para melhorar a qualidade e eficácia, tornando a organização rápida na adaptação

3. Metodologia

Num trabalho a definição do método de investigação está diretamente relacionada com o problema a ser estudado. Nesta situação específica recorreu-se ao estudo de caso por ser a opção metodológica que nos conduz ao alcance do objetivo preconizado para a investigação: avaliação da segurança de Sistemas de Informação num Município do Médio Tejo.

As técnicas de recolha de dados utilizadas neste estudo foram o inquérito por questionário (fonte principal) e a análise documental (fonte secundária, principalmente de apoio à compreensão do enquadramento da temática no Município).

Foi elaborado um questionário fundamentado na norma ISO/IEC 27002:2013, ao qual se associou um modelo de maturidade como escala, obtendo assim um questionário de resposta fechada, cujo preenchimento ficou a cargo do próprio respondente.

A cada controlo (114 no total) fez-se corresponder uma questão cuja resposta apresenta numa escala de Likert entre 0 e 5, correspondendo à classificação do grau da maturidade. Foram fornecidas as diretrizes de implementação e a tabela com a discriminação dos seis níveis de maturidade para apoiar a resposta.

A estrutura do questionário (figura 2) foi baseada na estrutura da norma (figura 1).

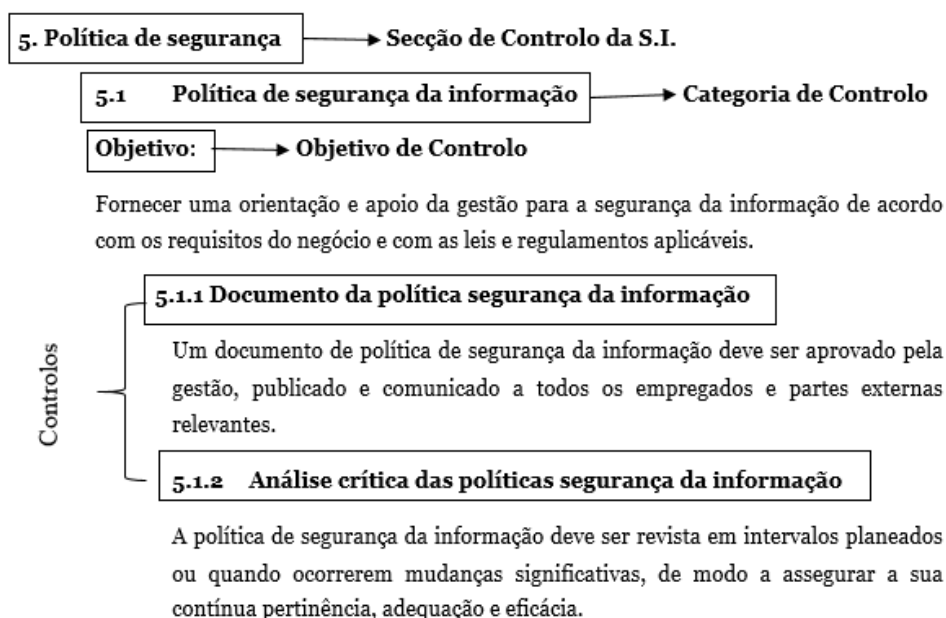


Figura 1 – Estrutura da norma

A análise dos questionários e tratamento de dados foi efetuada recorrendo-se ao auxílio de uma folha de cálculo (Microsoft Excel), onde foi efetuada a estatística descritiva. Com base nas respostas chegou-se a um nível de maturidade médio por categoria de controlo, por secção de controlo e geral. A partir dos resultados obtidos é possível perceber em que ponto se encontra o Município em termos de Segurança dos Sistemas de Informação, efetuar uma análise detalhada e verificar quais as lacunas, as vulnerabilidades, as áreas mais fracas e as mais fortes, bem como identificar os pontos de melhoria.

A.5 Política de segurança

A.5.1 Política de segurança da informação

Objetivo: Proporcionar uma orientação e apoio da gestão para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações aplicáveis.

Standard	Controlo	Nível CMMI
A.5.1.1	Documento da política de segurança da informação Um documento de política de segurança da informação deve ser aprovado pela gestão, publicado e comunicado a todos os empregados e partes externas relevantes. Notas:	0 1 2 3 4 5 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
A.5.1.2	Análise crítica das políticas de segurança da informação A política de segurança da informação deve ser revista em intervalos planeados ou quando ocorrerem mudanças significativas, de modo a assegurar a sua contínua pertinência, adequação e eficácia. Notas:	0 1 2 3 4 5 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Figura 2 – Estrutura do questionário

4. Análise de Resultados

Os resultados da análise efetuada ao Município estão evidenciados na tabela 1, onde é apresentada a maturidade média por controlo e a maturidade média geral.

Secção	Descrição	Maturidade Média	Maturidade Média Geral
A.5	Política de segurança	3,00	
A.6	Organização da segurança da informação	3,15	
A.7	Segurança em Recursos Humanos	3,00	
A.8	Gestão de ativos	2,83	
A.9	Controlo de acesso	3,90	
A.10	Criptografia	3,50	
A.11	Segurança física e do ambiente	3,19	
A.12	Segurança nas operações	4,00	3,21
A.13	Segurança das comunicações	3,67	
A.14	Aquisição, desenvolvimento e manutenção de sistemas	3,11	
A.15	Relação com fornecedores	2,58	
A.16	Gestão de incidentes de segurança de informação	2,14	
A.17	Aspetos da Segurança da Informação na gestão da continuidade do negócio	3,50	
A.18	Conformidade	3,37	

Tabela 1 – Avaliação geral e por secção, efetuada com base no modelo de maturidade

Através da análise dos resultados obtidos no inquérito, verifica-se que o MMT possui um nível de maturidade médio de 3,21, o que significa que, em média, os seus procedimentos de segurança estão definidos, mas existem procedimentos a melhorar para aprofundar a segurança dos Sistemas de Informação. Os processos estão normalizados e documentados e são divulgados em formação. É obrigatório que os processos sejam seguidos, pelo que é improvável que sejam detetados desvios. Os processos não são sofisticados, mas existe a formalização das práticas existentes.

Para cada secção será feita uma análise dos pontos que se destacam e que mais contribuem para a caracterização do estado atual da Segurança da Informação do MMT, sempre que se detetem fragilidades recomendar-se-ão ações corretivas.

4.1. A.5 - Política de segurança

Verifica-se que o MMT possui um documento onde estão definidas as políticas de segurança (Regulamento Interno da Informática), este documento foi aprovado em reunião de câmara e é do conhecimento de todos os colaboradores. No entanto, o mesmo não é revisto com regularidade, apesar de as políticas de segurança serem ajustadas sempre que necessário o documento não acompanha estas atualizações.

Recomenda-se que o regulamento seja revisto e atualizado, de forma a espelhar a realidade das políticas de segurança adotadas, só assim se assegura a sua contínua pertinência, adequação e eficácia.

4.2.A.6 - Organização da Segurança da Informação

Relativamente às orientações desta secção verifica-se que no MMT as responsabilidades pela Segurança da Informação estão atribuídas e bem definidas, mas não formalmente.

Seguindo as recomendações do controlo A.6.1.1 o MMT deverá definir claramente as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de Segurança da Informação específicos, deverá ainda associar orientações detalhadas às responsabilidades.

O mesmo controlo recomenda ainda que as pessoas com responsabilidades definidas pela Segurança da Informação devem delegar as tarefas de Segurança da Informação para outros, continuando responsáveis por verificar se as tarefas delegadas estão a ser executadas corretamente. Esta delegação de tarefas não se verifica no MMT.

A segregação de funções é uma preocupação no MMT e encontra-se bem implementada.

Verifica-se que o MMT não possui um procedimento que especifique quando e quais as autoridades a ser contactadas em caso de incidente de Segurança da Informação, situação que deverá ser corrigida.

O MMT mantém um reduzido contacto com associações, grupos especializados ou fóruns da área de Segurança da Informação, situação que deverá ser colmatada pois estes contactos são muito úteis para ampliar conhecimentos sobre as melhores práticas, para os especialistas do MMT se manterem atualizados, receberem previamente alertas, ter acesso a consultoria especializada em Segurança da Informação.

A Segurança da Informação na gestão de projetos é sempre considerada pela Informática, no entanto, os promotores dos projetos nem sempre têm esta preocupação, situação que deverá ser melhorada através de sensibilização e formação interna.

No que se refere ao trabalho remoto falta identificar e documentar por escrito as regras e políticas para que sejam incluídas no Regulamento Interno da Informática, esta questão revelou-se de grande importância na situação pandémica que se está a viver.

4.3.A.7 - Segurança em Recursos Humanos

A seleção e as condições de contratação são procedimentos devidamente instituídos na instituição e obedecem a regras bem definidas decorrentes de obrigações legais.

Recomenda-se uma maior consciencialização para a problemática da Segurança da Informação através de ações de formação interna para todos os recursos humanos do MMT.

Ao nível do processo disciplinar verifica-se que não está documentado nem prevista a existência de um processo formal, situação que deverá ser revista, uma vez que as boas práticas recomendam a existência de um processo disciplinar implementado e comunicado a aplicar a funcionários que cometam uma violação de Segurança da Informação.

Relativamente à rescisão ou mudança de contrato verifica-se que nem sempre a Informática é informada quando estas ocorrerem, o que pode implicar, durante algum período, falhas no controlo da segurança neste ponto. Deverá ser definido um circuito interno e identificados os responsáveis por informar a Informática quando ocorrem rescisões ou mudanças de contrato, este procedimento deverá ser incluído no Regulamento Interno da Informática.

4.4.A.8 - Gestão de Ativos

Esta secção apresenta um nível da maturidade médio de 2,83, sendo uma das secções que está abaixo da média.

Relativamente aos ativos associados à informação, os chamados ativos primários (processos e atividades de negócio, informação) é utilizado um sistema de gestão documental onde estão contidos todos os documentos gerados na execução dos processos, permitindo a associação de qualquer ficheiro em formato eletrónico. Este sistema de gestão permite constituir um arquivo digital corrente, intermédio e histórico de acordo com as normas legais estabelecidas.

Associada a cada documento integrado no sistema de gestão documental acima referido existe uma classificação da informação, no entanto esta está a ser revista e melhorada, o que implica que, provavelmente, nem toda a informação tem a classificação mais adequada.

Por sua vez, os ativos associados aos recursos de processamento da informação, os designados ativos secundários, (hardware, software, rede, etc...) encontram-se todos inventariados, com um responsável associado e com regras de utilização e devolução definidas no Regulamento Interno da Informática.

O objetivo A.8.3 tem a classificação de 1, situação que se deve ao facto de não existir um procedimento documentado relativo à utilização de dispositivos amovíveis de armazenamento de dados, situação que deverá ser corrigida

Deverão ser documentados e implementados procedimentos que definam as regras desde a utilização até à eliminação de dispositivos amovíveis de armazenamento de dados de forma a prevenir a divulgação não autorizada, a modificação, remoção ou destruição de informação armazenada nestes dispositivos.

4.5.A.9 - Controlo de Acesso

A secção A.9 é a segunda secção mais bem classificada, com um nível médio de maturidade de 3,90.

Os recursos humanos do MMT apenas têm acesso à informação e aos recursos de processamento da informação que a Informática autoriza. O fornecimento dos acessos necessários é solicitado, por escrito, pelos superiores hierárquicos à Informática e as configurações dos acessos são efetuadas pelos técnicos responsáveis em cada sistema informático.

Tal como já referido na análise à secção A.7 – segurança de recursos humanos, verifica-se que, por vezes, quando ocorrem situações de cessação de emprego, contrato ou acordo, a Informática não é informada no imediato, podendo assim eventualmente implicar, durante algum período, falhas no controlo de segurança.

Recomenda-se que seja definido um circuito interno e identificados os responsáveis por informar a Informática quando ocorrem situações de cessação de emprego, contrato ou acordo. Este procedimento deverá ser incluído no Regulamento Interno da Informática.

Relativamente à responsabilidade dos utilizadores verificam-se algumas situações de post-it com passwords colados no ecrã.

Recomenda-se uma maior consciencialização para a importância da proteção das informações de autenticação através de ações de formação interna para todos os recursos humanos do MMT.

O acesso aos sistemas e às aplicações é feito através de *login/password* que obrigam a políticas de *password* segura impedindo o uso de *passwords* simples e exigindo a sua alteração frequente.

4.6.A.10 - Criptografia

O MMT utiliza controlos criptográficos para a proteção da informação, estando atualmente em curso a migração de sistemas em falta, sobretudo de acesso externo para sistemas com criptografia.

Os certificados das chaves criptográficas são alterados em períodos inferiores a 3 meses.

4.7.A.11 - Segurança Física e do Ambiente

O MMT possui edifícios distribuídos pela cidade, verificando-se que, em alguns deles, não existe um adequado controlo de acesso e circulação de pessoas externas.

As salas com equipamento informático crítico, centro de dados e salas técnicas têm meios de controlo de acesso restritos, possuem alarme e o acesso é permitido apenas aos técnicos responsáveis pela administração de sistemas.

Sugere-se que sejam aplicadas, a todos os edifícios do MMT, medidas que assegurem que apenas pessoas autorizadas entram e circulam nas instalações.

Nem todos os equipamentos estão protegidos contra falhas de energia elétrica e alguns edifícios, mais antigos, não estão preparados para ter cablagem que permita uma proteção adequada contra intercetção, interferência ou danos.

As medidas de segurança para ativos que operem fora das dependências do MMT requerem melhorias.

A política mesa limpa e ecrã limpo ainda não foi interiorizada pelos recursos humanos do MMT, pelo que se recomenda uma maior consciencialização para a importância desta temática através da realização de ações de formação interna.

4.8.A.12 - Segurança nas Operações

No MMT esta é uma área em que, em média, os procedimentos de segurança são monitorizados, é mensurada a conformidade com os procedimentos instituídos e são efetuadas melhorias frequentes.

A Informática tem adotado como forma de atuação, sempre que surgem novos procedimentos ou a necessidade de alteração de procedimentos já existentes, a publicação, na intranet e em local de destaque, de manuais de utilização, garantindo assim que todos os utilizadores têm conhecimento imediato dos novos procedimentos.

O *backup* é feito ao longo do dia do servidor instalado no centro de dados do MMT para um servidor que está noutra localização. Ao fim de semana, este servidor cria uma réplica, das cópias de segurança alojadas, para banda magnética. No início da semana seguinte esta réplica é armazenada numa terceira localização segura. Desta forma, são seguidas as melhores práticas de *Disaster Recovery*. Caso ocorram situações de catástrofe ou desastre que tornem o centro de dados indisponível é possível garantir a recuperação dos dados.

4.9.A.13 - Segurança das Comunicações

No MMT existem procedimentos e controlos estabelecidos para manter a Segurança da Informação transferida dentro da organização e com entidades externas.

No entanto, recomenda-se que os acordos de confidencialidade e não divulgação sejam analisados criticamente de forma a que reflitam as necessidades de proteção das informações confidenciais nas relações do MMT com as partes externas e funcionários.

Os acordos de confidencialidade e não divulgação têm como objetivo proteger as informações do MMT e informam os signatários das suas responsabilidades, para proteger, usar e divulgar a informação de forma responsável e autorizada. Pode ser necessária a utilização de diferentes formas de acordos de confidencialidade ou de não divulgação, devendo ser considerados as diretrizes de implementação associada ao controlo A13.2.4.

4.10. A.14 - Aquisição, Desenvolvimento e Manutenção de Sistemas

Como pontos frágeis nesta secção destacam-se os controlos A.14.2.7, A.14.2.8 e A.14.2.9, verificando-se que os testes de segurança e de aceitação efetuados, de uma forma geral, resumem-se ao mínimo necessário para que se possa avançar com a sua utilização.

Relativamente ao desenvolvimento de sistemas por entidades externas (outsourcing) devem ser tidos em conta as diretrizes de implementação do controlo A.14.2.7

No que respeita aos testes de segurança do sistema (A14.2.8) convém que sejam realizados testes de funcionalidades de segurança durante o desenvolvimento de sistemas.

Novos sistemas ou atualizações requerem verificação e testes completos durante o processo de desenvolvimento, incluindo a preparação de um programa de atividade detalhado, com testes de entrada e de saída esperados sob determinadas condições. A abrangência do teste deve ser proporcional à importância e natureza do sistema.

Relativamente aos testes de aceitação de sistemas (A.14.2.9) devem ser efetuados para novos sistemas e novas versões. Devem incluir testes de requisitos de Segurança da Informação (A.14.1.1 e A.14.1.2) e adesão às práticas de desenvolvimento seguro de sistemas (A.14.2.1).

Os testes devem ser realizados em ambiente de teste realístico, de forma a assegurar que os testes são confiáveis e que o sistema não irá introduzir vulnerabilidades no ambiente do MMT.

4.11. A.15 - Relação com Fornecedores

Os controlos, o A.15.1.3 e o A.15.2.1 são os que apresentam maturidade mais baixa, merecendo assim especial atenção.

Relativamente ao controlo A.15.1.3 não existe um procedimento normalizado para aplicar ao fornecimento de produtos e serviços de Tecnologia de Informação e Comunicação. Existe uma preocupação a este nível, mas não havendo um procedimento documentado, que tenha de ser obrigatoriamente seguido, é provável que ocorram falhas.

Sugere-se que, na revisão dos acordos com os fornecedores, sejam tidos em consideração as diretrizes de implementação.

Relativamente à monitorização e análise crítica dos serviços fornecidos, controlo A.15.2.1, apesar de existir uma preocupação com este controlo não existe um procedimento documentado e implementado, nem é efetuado em intervalos regulares.

A monitorização e análise crítica dos serviços fornecidos deve garantir que os termos e condições incluídos nos acordos de Segurança da Informação são cumpridos e que os incidentes e problemas de segurança são geridos de forma apropriada.

O relacionamento entre o MMT e os fornecedores devem obedecer a um processo de gestão que permita:

- a. monitorizar os níveis de desempenho de serviço para verificar conformidade aos acordos;

- b. analisar criticamente os relatórios de serviços produzidos por fornecedores e agendamento de reuniões de progresso conforme requerido pelos acordos;
- c. realizar auditorias aos fornecedores, em conjunto com a análise crítica dos relatórios de auditoria independente, quando disponíveis, bem como o acompanhamento das questões identificadas;
- d. fornecer informações sobre incidentes de segurança de informação e analisar criticamente tais informações, conforme requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiem;
- e. analisar criticamente os circuitos de auditoria do fornecedor e registos de eventos de Segurança da Informação, problemas operacionais, falhas, investigação de falhas e interrupções relativas ao serviço entregue;
- f. resolver e gerir quaisquer problemas identificados;
- g. analisar criticamente os aspetos de Segurança da Informação na relação dos fornecedores com seus próprios fornecedores;
- h. garantir que o fornecedor mantém capacidade de serviço suficiente em conjunto com planos de trabalho desenhados para assegurar que os níveis de continuidade do serviço acordados são mantidos, no caso de um desastre ou falha dos serviços principais (A.17).

4.12. A.16 - Gestão de Incidentes de Segurança de Informação

A secção A.16 destaca-se, por ser a secção com classificação mais baixa, encontrando-se abaixo do nível médio de maturidade.

O MMT não possui um documento formal que estabeleça as responsabilidades e os procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas em caso de incidentes de Segurança da Informação. Os procedimentos existem, mas não estão normalizados.

O facto de não existir um documento formal faz com que os controlos incluídos na secção sejam classificados maioritariamente com o nível 2, o que significa que os procedimentos são realizados de forma repetitiva e geralmente sempre pela mesma pessoa, mas não há um processo normalizado.

O primeiro passo para melhorar o nível de maturidade desta secção é a implementação de um procedimento documentado e de seguimento obrigatório, que estabeleça as responsabilidades e os procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas em caso de incidentes de Segurança da Informação, devendo para isso ser consideradas as diretrizes de implementação associadas ao controlo A.16.1.1

4.13. A.17 - Aspetos da Segurança da Informação na Gestão da Continuidade do Negócio

Verifica-se que o MMT tem presente a preocupação de não permitir a interrupção das atividades e proteger os processos críticos contra as consequências de falhas ou desastres significativos, tendo como objetivo o desenvolvimento contínuo de processos com vista à melhoria da proteção dos processos críticos face aos riscos existentes.

Recomenda-se, no entanto, que o MMT defina, documente, implemente e mantenha processos, procedimentos e controlos para assegurar o nível requerido de continuidade para a Segurança da Informação, durante uma situação adversa, devendo para isso assegurar-se que:

- a. está implementada uma estrutura de gestão adequada para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência;
- b. o pessoal designado para dar resposta em caso de incidente tem a necessária responsabilidade, autoridade e competência para gerir um incidente e garantir a Segurança da Informação;
- c. estejam desenvolvidos e aprovados planos documentados, procedimentos de recuperação e resposta, detalhando como a organização irá gerir um evento de interrupção e como manterá a sua Segurança da Informação num nível pré-determinado, com base nos objetivos de continuidade da Segurança da Informação aprovado pela direção (A.17.1.1).

Em função dos requisitos de continuidade de Segurança da Informação, convém que a organização estabeleça, documente, implemente e mantenha:

- a. controlos de Segurança da Informação dentro dos processos de recuperação de desastre ou de continuidade do negócio, procedimentos e ferramentas e sistemas de suporte;
- b. processos, procedimentos e mudança de implementação para manter os controlos de Segurança da Informação existentes durante uma situação adversa;
- c. controlos compensatórios para os controlos de Segurança da Informação que não possam ser mantidos durante uma situação adversa.

Tendo em conta o controlo A.17.1.3 o MMT deverá ainda verificar, em intervalos regulares, se os controlos definidos e implementados para a continuidade da Segurança da Informação, continuam válidos e eficazes em situações adversas.

4.14. A.18 - Conformidade

O objetivo da secção A.18 é evitar a violação de qualquer lei, estatuto, regulamento ou obrigação contratual relacionadas com a Segurança da Informação e de quaisquer requisitos de segurança.

Para garantir o cumprimento destes requisitos o MMT deverá efetuar a normalização dos processos referidos nas anteriores seções, de forma a que estes se tornem formalmente aceites e de seguimento obrigatório, evitando assim a violação de qualquer lei, estatuto, regulamento ou obrigação contratual relacionadas com a Segurança da Informação e de quaisquer requisitos de segurança.

5. Conclusões

A utilização da ISO/IEC 27002:2013 combinada com um modelo de maturidade constituem uma boa ferramenta de autoavaliação da segurança de Sistemas de Informação.

A análise dos resultados obtidos, demonstram que o MMT possui um nível de maturidade médio geral de 3 o que significa que, em média, os seus procedimentos de segurança estão normalizados, documentados, são divulgados em formação e têm de ser seguidos obrigatoriamente.

No entanto, apesar de os princípios e políticas inerentes à ISO/IEC 27002:2013 serem uma preocupação, verifica-se a falta de normalização de alguns processos, de forma a que estes se tornem formalmente aceites de seguimento obrigatório e divulgados em formação.

A utilização de uma escala de maturidade permitiu de forma simples e direta identificar as áreas que estão abaixo da média (áreas críticas) e que necessitam de melhoria, são elas, A.8 – Gestão de ativos (2,83), A.15 Relação com fornecedores (2,58) e A.16 Gestão de incidentes de Segurança da Informação (2,14). A classificação abaixo da média nestas secções deve-se fundamentalmente ao facto de não existirem procedimentos documentados nestas áreas. Apesar de existir uma preocupação e serem realizados procedimentos, não há um procedimento documentado, que seja de seguimento obrigatório, aumentando a probabilidade de ocorrência falhas.

Os processos informais dão lugar a que nem sempre sejam aplicados, pois não são obrigatórios nem existe um procedimento específico a seguir, podendo também ocorrer que, para a mesma tarefa, dois funcionários executem procedimentos diferentes, por uma ordem diferente e/ou sem o mesmo rigor, podendo originar vulnerabilidades que podem ser exploradas por ameaças específicas.

A utilização deste método de avaliação proporciona uma visão abrangente de todo o Sistema de Informação, permitindo perceber se os controlos utilizados são os mais adequados e quais necessitam de ser melhorados.

A aplicação, de forma periódica, desta ferramenta permite a melhoria continua dos processos de segurança de informação através da identificação da necessidade de ajustamentos, sempre com o objetivo de melhorar a sua eficiência e eficácia e elevar o grau de maturidade dos Sistemas de Informação do Município.

Os resultados obtidos com esta avaliação podem também ser utilizados como suporte para a tomada de decisões relacionadas com melhorias e investimento necessários para assegurar a Segurança da Informação, bem essencial do Município.

Referências

- Beal, A. (2005). *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. São Paulo: Atlas.
- Carneiro, A. (2002). *Introdução à Segurança dos Sistemas de Informação*. Lisboa: FCA.
- Carvalho, C. M. (2018). *Segurança e Auditoria em Sistemas de Informação e Comunicação - Implementação numa entidade pública*. Projeto de Mestrado, Universidade da Madeira.
- Gouveia, L. B., & Ranito, J. (2004). *Sistemas de Informação de Apoio à Gestão*. Porto: SPI - Sociedade Portuguesa de Inovação.

ISO/IEC 27002:2013. (2013). ISO/IEC 27002 - Information Technology - Security Techniques - Code of Practice for Information Security - Controls. Standardization, International Organization for Standardization.

Lopes, I. M. (2012). *Adopção de Políticas de segurança de Sistemas de Informação na administração Pública Local em Portugal*. Tese de Doutoramento, Universidade do Minho.

Pedro, J. M. (junho de 2010). *Livro Comemorativo dos 80 Anos da IGF-Autoridade de Auditoria - Sinais de inovação nas metodologias de controlo - Standards internacionais relacionados com o controlo interno na perspectiva dos sistemas de informação* (1.ª ed.). (I. G. Finanças, Ed.)

Trigacheiro, C. F. (02 de 2012). *O impacto das tecnologias de informação na avaliação dos sistemas de controlo interno das organizações*. Instituto Politécnico de Tomar, Escola Superior de Gestão.