AUDITORIA À SEGURANÇA DA INFORMAÇÃO DA ORGANIZAÇÃO

de

Álvaro José Campelo de Magalhães

Instituto Politécnico da Maia

2022

AUDITORIA À SEGURANÇA DA INFORMAÇÃO DA ORGANIZAÇÃO

de

Álvaro José Campelo de Magalhães

Dissertação para obtenção do título de ESPECIALISTA

Área de Especialidade: 481 – Ciências Informáticas

Submetida ao **Instituto Politécnico da Maia**

2022

Agradecimentos

Agradeço ao ISTEC, à Câmara Municipal de Paços de Ferreira e ao ISPGAYA por me terem proporcionado as condições para desenvolver e apresentar esta dissertação.

Agradeço especialmente ao Eng.º António Veiga pela amizade e pelo apoio na realização deste trabalho. Sem este apoio, teria sido difícil concretizá-lo e não teria, certamente, a mesma qualidade.

Agradeço, também, à minha família pelo apoio, incentivo e compreensão manifestados, principalmente à Anabela, ao José Alberto e à Maria Francisca, a quem dedico este trabalho.

Prefácio

Álvaro José Campelo de Magalhães ficou Mestre pela Universidade do Minho, em Julho de 2003, na Escola de Engenharia, na área de Sistemas de Informação, sendo atualmente Especialista de Informática na câmara Municipal de Paços de Ferreira.

Após ter cumprido o serviço militar obrigatório nos paraquedistas em Tancos e S. Jacinto, entre 1989 e 1991, como Furriel Miliciano Paraquedista, ingressou no ISTEC onde conclui o Bacharelato em Informática, tendo concluído a licenciatura no ISMAI em Informática de Gestão em1997.

Nessa altura, estava a trabalhar na Câmara Municipal de Paredes como responsável pelo Gabinete de Informática. Colaborou em vários projetos, nomeadamente na implementação dos Sistemas de Informação Geográfica.

Na Câmara de Paços de Ferreira, como o responsável pelo gabinete de informática, está inserido em vários projetos nesta área, como, por exemplo, apoio ao Sistema de Informação Geográfica, Serviços Online, entre outros. Foi também o principal responsável, pela migração de todos os servidores para o DataCenter do Vale do Sousa Digital, área a que pertence o Município de Paços de Ferreira.

Desde o ano letivo de 2000 / 2001, é formador no ISTEC Porto, nas Licenciaturas de Informática e Engenharia Multimédia e nos Cursos Superiores Técnicos.

A escolha do tema deste trabalho deve-se, fundamentalmente, ao facto de ter desenvolvido grande parte da sua atividade na área de segurança dos sistemas de informação do município, com o levantamento de todas as necessidades ao nível da segurança.

Resumo

A Câmara Municipal de Paços de Ferreira, com a sua história e atividade económica, inscreveu o seu nome no mercado virtual das novas tecnologias, proporcionando uma acentuada divulgação não só das iniciativas de índole cultural, recreativa e desportiva, como também da riqueza e diversidade do património histórico. Pretende, assim, assegurar a apresentação de informações atualizadas acerca da atividade produtiva de um concelho que tem à sua frente um futuro promissor, tendo a sua estrutura de sistemas e tecnologias de informação como plataforma privilegiada de atuação. Numa altura em que se constata que as ameaças aos sistemas e redes informáticas não param de crescer e se mostram cada vez mais criminosas e lucrativas, é natural afirmar-se que questões que se prendem com a segurança da plataforma tecnológica estão na ordem do dia. Neste sentido, constitui uma razão essencial a realização de uma avaliação de segurança e sistemas de informação sobre a plataforma tecnológica da Câmara Municipal de Paços de Ferreira.

Apresenta-se, neste documento, um plano macro, que visa evidenciar as questões que deverão ser objeto de melhoria, assim como diversas ações a serem realizadas, com a finalidade de resolver os principais problemas, identificados perante a análise realizada.

Com a avaliação de segurança dos SI/TI, na Câmara Municipal de Paços de Ferreira, pretende-se proporcionar uma visão diferente, refletora das melhores práticas da indústria, que identifiquem os principais problemas a nível de segurança dos Sistemas e Tecnologias de Informação da organização, posicionando-nos junto do cliente, para uma futura definição da estratégia de SI/TI a seguir.

A Câmara Municipal de Paços de Ferreira possui uma equipa de recursos humanos com vasta experiência nos mais variados domínios dos Sistemas e Tecnologias de Informação, o que constitui a sua posição distintiva, diferenciadora. Contribui para isto, como fator complementar, a experiência e conhecimentos acumulados ao longo de vários anos, corporizada por especialistas que há muito se dedicam, em exclusivo, ao domínio dos Sistemas de Informação, cujo valor acrescentado é de grande significado.

Este trabalho foi baseado na norma ISO17799/27001.

Abstract

The City Hall of Paços de Ferreira, with its history and economic activity, registered its name in the virtual market of new technologies, providing a strong dissemination of initiatives of a cultural, recreational and sports nature, richness and diversity of historical heritage. It aims to ensure the presentation of up-to-date information about the Productive Activity of a county that has a promising future ahead, with its structure of information systems and technologies as the preferred platform for action. At a time when threats to computer systems and networks are constantly growing and increasingly criminal and profitable, it is natural to say that security issues on the technology platform are on the order of the day. In this sense, it is an essential reason, the realization of a safety assessment and information systems on the technological platform of the City Hall of Paços de Ferreira.

A macro plan is presented in this document, which aims to highlight the issues that must be addressed, as well as several actions to be taken, with the purpose of solving the main problems identified in the analysis performed.

With the safety evaluation of the IS / IT at the City Hall of Paços de Ferreira, it is intended to provide a different vision, reflecting the best practices in the industry, identifying the main problems in the security of Information Systems and Technologies of the organization, positioning ourselves with the client, for a future definition of the IS / IT strategy to follow.

The City Council of Paços de Ferreira has a human resources team with vast experience in the most varied fields of Information Systems and Technologies, which is its distinguishing position. Functioning as a complementary factor to the experience and knowledge accumulated over several years, embodied by specialists who have long been dedicated exclusively to the field of Information Systems, whose added value is of great significance.

This work was based on the ISO17799/27001 standard.

Índice

Índice de figuras

Lista de Abreviaturas

DMZ	*Demilitarized zone*
QoS	Quality of Service
SIG	Sistemas de Informação Geográfica
IP ADDRESS	Internet Protocol address
VPNs	Virtual Private Networks
APs	Access Points
LOGs	Processo de Registo de Eventos
AD	Active Directory
SI/TI	Sistema de Informação / Tecnologia da Informação
LAN	Local Area Network
WAN	Wide Area Network
ISP	Internet Service Provider
ACLs	Access Control Lists
GP	Group Policies
DDE	Dynamic Data Exchange
FTP	File Transfer Protocol
SNMP	Simple Network Management Protocol
RPC	Remote Procedure Call
IMAP	Internet Message Access Protoco
WEB	World Wide Web
HTTP	Hypertext Transfer Protocol
TCP	Transmission Control Protocol
RDP	Remote Desktop Protocol
MFA	Multi Factor Authentication

Glossário

Vulnerabilidade Uma fraqueza em qualquer recurso ou sistema de controlo da empresa que pode ser explorada por uma ou mais ameaças

Segurança da informação Define-se como a proteção conferida a um sistema de informação, a fim de atingir os objetivos aplicáveis à preservação da integridade, disponibilidade e confidencialidade dos recursos do sistema de informação

Ameaça Potencial causa de um incidente no qual pode resultar danos a um sistema ou organização

1. Introdução

1.1. Contexto

A informação é um bem que, à semelhança de todos os restantes bens de uma organização, tem um valor acrescentado para a mesma, devendo ser salvaguardada de forma idêntica. A segurança da informação protege dados de uma grande variedade de ameaças existentes, assegurando a continuidade da empresa e do negócio, minimizando perdas e maximizando o retorno do investimento e oportunidades da organização.

Independentemente do formato que a informação apresente e da forma como é divulgada ou armazenada, esta deverá ser sempre devidamente protegida.

A segurança da informação tem-se mostrado como um importante desafio para a maioria das organizações. Saber quanto e como se deve investir em segurança é uma questão fulcral para qualquer organização. Face aos incidentes diários de ataques informáticos às redes das empresas, hoje ninguém duvida de que é necessário investir na segurança informática.

Garantir a segurança da informação exige muito mais do que, simplesmente, instalar a ferramenta ou tecnologia mais poderosa disponível no mercado. Muitas organizações adotam uma visão estreita de segurança, concentrando a atenção exclusivamente na questão dos riscos de tecnologia da informação (TI). Essa abordagem, embora compreensível perante a crescente dependência em relação a redes, sistemas e bases de dados para desempenhar processos de negócio, é insuficiente para mitigar uma série de ameaças graves a que os recursos de informação estão expostos.

1.2. Motivação

A segurança da informação não é um assunto novo, sendo possível encontrar referências ao seu estudo desde que a informação começou a ser tecnologicamente tratada. Mas, à medida que a informação foi aumentando de valor e as técnicas de armazenamento, processamento e transmissão lhe conferiram uma enorme flexibilidade, a sua segurança tornou-se cada vez mais um objetivo estratégico essencial.

Mesmo com todos os esforços já realizados, deve-se ter consciência de que não existe uma segurança plena, sabendo-se, contudo, que se deve estar seguro, face a uma ameaça ou a um risco. A ideia de risco depende da sensação de medo e, por vezes, lida-se com essa sensação de uma forma branda e descontraída.

Perante a ocorrência de um evento, reage-se e assumem-se comportamentos defensivos. Rapidamente nos adaptamos ao ambiente e, se não existirem outros estímulos, relaxamos esses comportamentos defensivos. Segundo Howard, a mente humana não está “preparada” para conviver com o medo de forma permanente (Howard and Prince 2011). Uma consequência óbvia desta observação é que diferentes agentes, em diferentes contextos, caracterizarão o mesmo estado de segurança de forma diferente, dificultando os esforços de normalização. Todos sentirão, em algum momento, alguma insegurança. Por outro lado, qualquer indivíduo que não reconheça uma situação de risco potencial sentir-se-á seguro, naturalmente.

1.3. Objetivos e enquadramento

1.3.1. Enquadramento

Atualmente, a sociedade está cada vez mais em constante mutação e, por isso mesmo, as organizações necessitam de ter sempre disponível a informação necessária e útil para desenvolver, de uma forma rápida e eficaz, as suas atividades no dia-a-dia.

Garantir a segurança da informação é um fator fundamental para sustentar a sua continuidade e sucesso. O objetivo deste trabalho prendeu-se com a necessidade de fazer um levantamento dos sistemas de informação e implementar um sistema de segurança de dados no Município de Paços de Ferreira, dado que, aliado à rápida evolução dos sistemas de informação, deu-se também um rápido crescimento da "pirataria". Estariam, assim, os sistemas mais vulneráveis a ataques, caso não houvesse o cuidado necessário, como houve, desde a realização deste trabalho, até à data de hoje, em que se foi melhorando e implementado medidas de segurança.

Sem uma análise de risco que fundamente os projetos de segurança, as organizações gastariam dinheiro em equipamento, software e *know-how* sem uma clara expectativa de retorno em redução do risco. O risco é caracterizado pela probabilidade de uma ocorrência, multiplicada pelo impacto que essa ocorrência terá para a organização. Uma vez que estamos a falar de segurança da informação, as ocorrências de que falamos significam a concretização de ameaças ao controlo de acesso, à confidencialidade, à integridade, à disponibilidade ou à auditoria da informação.

Figura 1 – Segurança da Informação (Fonte: desconhecida)

A Segurança da Informação caracteriza-se pela preservação dos seguintes elementos:

Confidencialidade: Assegurar que a informação apenas é disponibilizada a quem tem a devida autorização;

Integridade: Assegurar a consistência e veracidade da informação e respetivos métodos de processamento;

Disponibilidade: Assegurar que a informação está disponível a utilizadores com a devida autorização, sempre que este acesso for necessário;

Auditoria: Os dados e informações corporativas e/ou de negócio devem ser registados, compilados, analisados e revelados de modo a permitir que auditores internos ou provedores de garantia externos possam atestar a sua veracidade;

Rastreabilidade: Assegurar a capacidade de recuperação do histórico das ações concretizadas, através de um registo que deverá estar atualizado e disponível em qualquer momento.

Qual é a necessidade da Segurança da Informação?

A informação e os seus processos de apoio, sistemas e redes, são bens essenciais ao negócio de uma organização. Confidencialidade, integridade e disponibilidade da informação são elementos essenciais para preservar a competitividade, a fatoração, a rentabilidade e a imagem de uma organização no mercado.

Atualmente, a segurança dos sistemas da informação das organizações é cada vez mais colocada à prova por diversos tipos de ameaças de diversificadas origens, em que se incluem as tão frequentes fraudes eletrónicas, nomeadamente a espionagem, a sabotagem, o vandalismo, *hackers* e ataques dos "*denial of servisse",* que se tornam cada vez mais sofisticados e ambiciosos.

A dependência dos sistemas e serviços de informação leva a crer que as organizações estão cada vez mais vulneráveis às ameaças de segurança. O uso simultâneo de redes públicas e privadas e a partilha de recursos de informação são fatores que contribuem para o acréscimo da dificuldade em controlar os acessos e a respetiva segurança dos mesmos.

Como estabelecer os requisitos de segurança?

É essencial, para uma organização, identificar os seus requisitos de segurança. Através da realização de uma análise de risco, são identificadas as principais ameaças, assim como as vulnerabilidades e a avaliação da probabilidade da sua ocorrência, bem como o potencial impacto para a organização.

Os requisitos de segurança deverão ser identificados através de uma avaliação sistemática dos seus riscos. Os investimentos na gestão da segurança da informação deverão ser efetuados de acordo com o impacto causado no negócio, através de eventuais falhas de segurança.

As análises críticas de risco não devem ser executadas em diferentes níveis de exigências, dependendo dos resultados das avaliações de risco efetuadas anteriormente e das alterações nos níveis de riscos que a organização considera aceitáveis para o seu negócio.

Com cariz prioritário, as avaliações de segurança deverão ser direcionadas aos recursos críticos da organização de uma forma generalista, avançando, posteriormente, para um nível de detalhe específico, onde são desenvolvidas análises para solucionar questões relacionadas com riscos específicos.

Uma vez identificados os requisitos de segurança, devem ser selecionados e implementados controlos para garantir que os riscos sejam mitigados a um nível considerado aceitável. Os controlos podem ser selecionados a partir de normas existentes ou de outro conjunto de controlos que sejam desenvolvidos para atender a necessidades específicas, quando apropriado. É conveniente que os controlos sejam selecionados com base no custo da sua implementação, face ao grau de risco identificado e ao impacto na ocorrência de perda de informação.

A Segurança da Informação é conseguida através da implementação de controlos de diversas vertentes, como tecnológica (*firewalls*, sistemas de deteção de intrusão, antivírus, etc.), administrativa (planos, políticas e procedimentos de segurança) e operacional (práticas de gestão de segurança e resposta a incidentes), realizados de uma forma periódica e permanente.

Nesse sentido, é da responsabilidade dos órgãos máximos da Câmara Municipal de Paços de Ferreira definir objetivos claros na implementação de uma doutrina de segurança e demonstrar não só apoio, mas total empenho e dedicação na implementação e manutenção de uma política de segurança da informação em toda a organização.

Como tal, deve a Câmara Municipal de Paços de Ferreira dotar, tanto a direção como os responsáveis dos sistemas de informação da organização, de meios, competências e autoridade necessários para cumprir os seguintes objetivos estratégicos:

- proteção dos Recursos Tecnológicos e de atividade da Organização: assegurar a confidencialidade, disponibilidade e integridade da informação e dos sistemas que a suportam;

- proteção Legal da Organização: garantir que são cumpridas as obrigações legais da organização no quadro de segurança dos sistemas de informação;

- proteção Legal dos Colaboradores: garantir a privacidade dos colaboradores, de acordo com a legislação nacional e comunitária em vigor. Especificamente, devem ser

observadas as restrições à recolha e tratamento de dados pessoais, à vigilância eletrónica e à monitorização de correio eletrónico.

1.3.2. Objetivos

A Segurança Informática ainda é frequentemente vista, em muitas organizações, como uma relação "Segurança - Tecnologia", mas, na verdade, não só a tecnologia, vista de um modo singular, assegura a informação. Deverá ser adotado um plano de segurança estratégico global, internamente na organização.

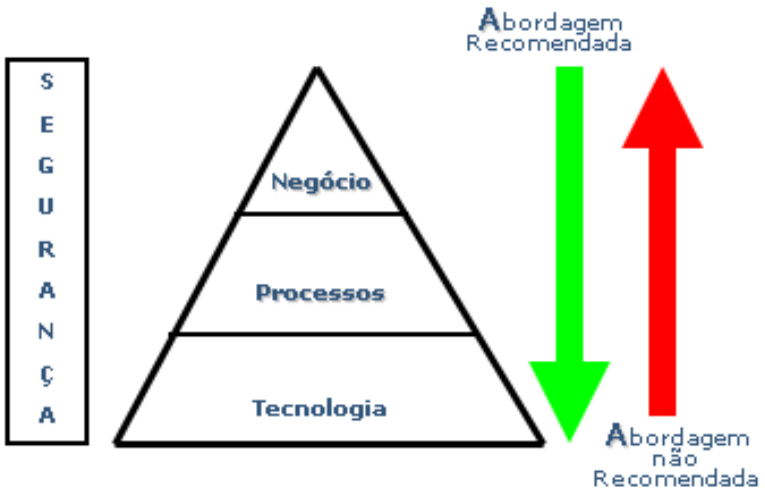

Figura 2 – Pirâmide da Segurança (relatório de segurança elaborado pela VisionWare, 2011)

Na maioria das organizações, a segurança informática é encarada exclusivamente através da aquisição de tecnologia, quando a perspetiva correta deveria passar por uma abordagem inicial ao próprio negócio, caracterizando as vulnerabilidades e avaliando as potenciais ameaças (que variam de organização para organização). Em função destes dois fatores, obtém-se uma avaliação do risco a que a empresa está exposta.

Em função do risco caracterizado, deverão ser dimensionados os investimentos a realizar, com o objetivo de o reduzir, através da definição de:

Plano de Segurança: alinhado com a estratégia da organização;

Política/Procedimentos de Segurança: alinhado com o negócio e os processos que o sustentam;

Tecnologia: meios técnicos auxiliares de suporte dos procedimentos de segurança.

A utilização eficiente da informação deve ser parte indissociável da doutrina e prática quotidiana de uma organização, sendo considerada como componente vital para o êxito do trabalho.

As políticas e normas corporativas de segurança da informação abrangem bases de dados, todos os ambientes de informática, documentos, arquivos e restantes ferramentas tecnológicas. As informações restritas, e de interesse exclusivo dos colaboradores, deverão ser tratadas internamente, com sigilo absoluto, devendo receber total proteção.

A verificação da segurança efetuada teve como principal objetivo identificar o estado atual de sistemas e segurança lógica e física da organização, programando, assim, os próximos passos evolutivos na manutenção da infraestrutura tecnológica da Câmara Municipal de Paços de Ferreira.

2. Metodologia

2.1. Metodologia Utilizada

A norma ISO17799/27001, é um padrão reconhecido internacionalmente na área da segurança da informação, amplamente utilizada para esboçar políticas de segurança, com o objetivo de proporcionar uma base comum para o desenvolvimento de um padrão organizacional e uma prática efetiva na gestão da segurança da informação.

A verificação de segurança foi realizada de uma forma abrangente, tendo em mente os objetivos anteriormente identificados, estando a mesma alinhada com a norma de segurança ISO17799/27001, para assim se garantir um valor acrescentado ao serviço.

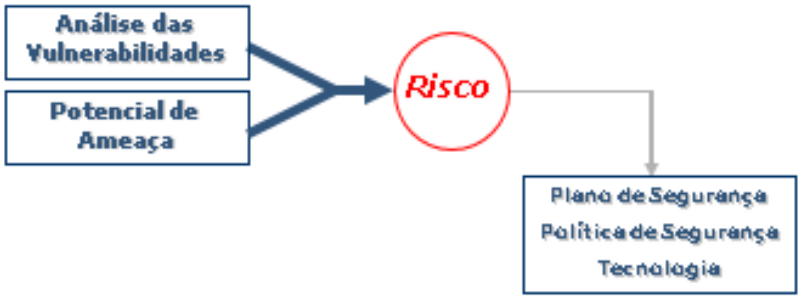

Figura 3 – Risco (relatório de segurança elaborado pela VisionWare, 2011)

São diversos os fatores que asseguram o sucesso da implementação de um sistema que permita manter a informação segura, dentro de uma organização, destacando-se as seguintes referências:

- Uma política e um método de implementação de segurança da informação que reflitam os objetivos da organização;
- Um bom entendimento entre os requisitos de segurança, avaliação e gestão do risco;
- Comunicação efetiva dos assuntos relacionados com a segurança da informação a todas as pessoas que constituem a organização;

- Distribuição de guias, contendo a política e padrões de segurança da informação da empresa, a todos os empregados e fornecedores;

- Formação adequada a todos os membros da organização;

- Um sistema adequado de avaliação da efetividade da gestão da segurança da informação que proporcione retorno e sugestões para implementação de melhorias futuras.

A metodologia de levantamento da informação utilizada está baseada num processo padrão, completo e rigoroso, através do qual é realizada uma análise à segurança da informação, fazendo uso de várias ferramentas de análise, reunindo diversas vezes com as pessoas responsáveis pela infraestrutura tecnológica da organização e acedendo aos sistemas e configuração do mesmo.

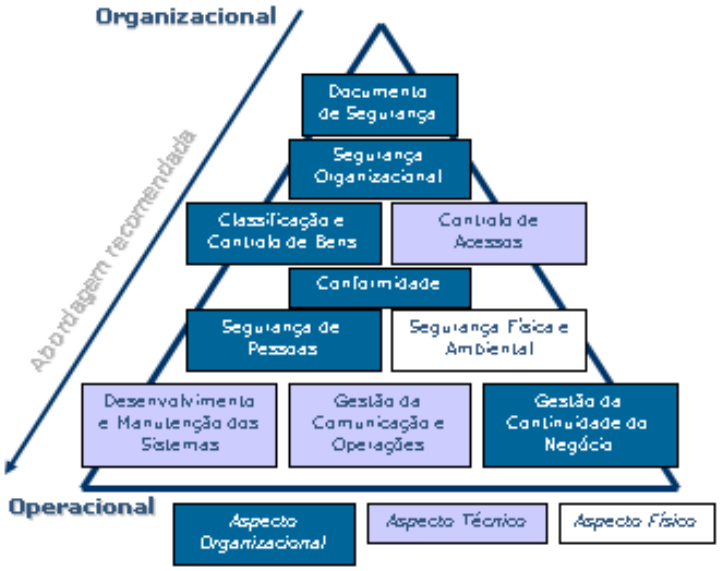

Figura 4 – Abordagem organizacional vs operacional (relatório de segurança elaborado pela VisionWare, 2011)

Os métodos utilizados, nesta auditoria, garantem uma avaliação independente e transversal da segurança dos sistemas de TI que suportam o negócio.

Este documento constitui uma ferramenta de trabalho para a implementação de medidas que, por um lado, reduzem o risco de ocorrência de incidentes de segurança e, por

outro, fornecem pistas para a alocação de recursos às áreas mais críticas para a continuidade do negócio, contribuindo para o alinhamento das políticas de segurança com a atual legislação e com as melhores práticas do mercado.

De forma a inferir as conclusões descritas, foram analisadas diversas áreas, como:

- Política de Segurança da Informação;
- Segurança da infraestrutura física;
- Classificação da Informação;
- Disposição da arquitetura tecnológica;
- Deteção e resposta a incidentes de segurança e avarias;
- Dispositivos de segurança existentes;
- Cultura e organização de segurança existente.

2.2. Análise de Risco

Uma análise de risco define-se como sendo um processo de avaliar em que medida é que um determinado contexto, que incluí ameaças, vulnerabilidades e o valor a proteger, é ou não aceitável para uma organização.

A análise de risco efetuada pretende identificar, qualificar e quantificar esses mesmos riscos associados, face aos critérios de aceitação e aos objetivos considerados como relevantes para a organização. Os resultados obtidos deverão ser considerados como referência para se atingirem os controlos de segurança necessários à sua implementação, de forma a mitigar rapidamente os riscos da segurança de informação verificados.

Este processo de análise de risco e respetiva implementação de controlos de segurança deverão ser efetuados de forma periódica para, deste modo, possibilitar a abrangência de diversos sectores da organização ou de sistemas de informação específicos.

A análise de risco incluí a aproximação sistemática de estimar a dimensão e impacto de riscos inerentes à segurança da informação na organização, assim como o processo de comparação entre os riscos estimados face ao critério de determinação do impacto dos mesmos na organização.

A avaliação dos riscos identificados no campo da segurança da informação deverá ter um alcance claramente definido, com o objetivo de ser eficaz. Se apropriado, deverá conter a avaliação dos riscos de outras áreas da organização.

Os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança, que deverá ser efetuada. Os investimentos com a implementação dos controlos de segurança deverão ser analisados de acordo com os danos causados ao negócio da organização, que poderão ser gerados pelas potenciais falhas na segurança.

Para que fosse determinado o risco a que a organização está exposta, foi considerado como sendo indispensável:

- Identificar e classificar os recursos de informação;
- Identificar as ameaças aos referidos recursos;
- Identificar as vulnerabilidades que poderão expor os recursos às ameaças.

Recursos de informação poderão ser os sistemas que salvaguardam e processam informação crítica para a organização, assim como as infraestruturas de que dependem esses sistemas;

Ameaças poderão ser acessos não autorizados, quebra de confidencialidade, adulteração ou destruição da informação, indisponibilidade de sistema crítico para o negócio, entre outras.

Vulnerabilidades poderão ser a falta de segregação de responsabilidades, a inexistência de políticas, a existência de vulnerabilidades de software nos sistemas críticos para o negócio, entre outros.

Face à identificação dos riscos existentes, a organização deve definir uma estratégia de gestão do risco existente.

Cada risco identificado poderá ser:

Assumido: Há riscos que, pela sua baixa probabilidade de ocorrência ou impacto, poderão ser assumidos conscientemente pela organização;

Transferido: O risco pode ser transferido para uma outra organização, através da contratação de seguros ou da transferência de responsabilidades;

Mitigado: A mitigação do risco implica a execução de projetos de segurança, sejam modificações organizacionais, implementação de processos ou instalação de tecnologia.

Os projetos de mitigação de risco visam a redução da probabilidade de ocorrência de cada ameaça ou o impacto que essa concretização de ameaça possa ter sobre os ativos de informação. A sua implementação causará uma redução do risco que, apesar de não ser possível eliminar completamente, deverá ser mantido dentro de parâmetros aceitáveis.

O principal valor da análise de risco está na quantificação das medidas de redução de risco, permitindo identificar os projetos que, com um menor investimento, resultam numa maior redução do risco para a organização.

3. Avaliação Formal

A segurança dos sistemas de informação, mais do que um simples produto ou tecnologia que se pode adquirir, aplicar e esquecer, deverá ser encarada de forma integrada com o negócio da empresa, como um processo em permanente evolução que requer uma enorme capacidade para provocar e gerir mudanças, tanto nos hábitos e comportamentos como nas infraestruturas organizativas e tecnológicas.

A opinião dos auditores visa identificar e evidenciar as questões que deverão ser objeto de melhoria. O que se pretendeu fazer foi um plano macro, mas com ações concretas, para resolver os principais problemas, de segurança da informação da organização, em linha com o objetivo fundamental de reforçar a sua posição competitiva e preservar os níveis de confiança dos clientes e da comunidade organizacional em geral, incluindo os colaboradores.

Como conclusão principal desta auditoria, podemos afirmar que a rede informática, da Câmara Municipal de Paços de Ferreira apresenta deficiências graves, do ponto de vista de segurança de sistemas de informação.

As deficiências detetadas afetam tanto a rede interna como a rede externa, comprometendo, de forma crítica, a confidencialidade e integridade dos dados corporativos da organização. Relativamente à integridade dos sistemas e capacidade de controlo e monitorização, deverão ser efetuadas melhorias significativas, que minimizem as deficiências detetadas. Devido à inexistência uma plataforma de publicação de serviços externos (DMZ), que possibilite a existência de um nível de separação de tráfego distinto entre o perímetro e a rede interna da organização, assim como uma solução de monitorização/alarmística de controlo da rede interna, que garanta um nível de qualidade de serviço (QoS) e que cumpra as exigências e expectativas de negócio da organização, a integridade dos recursos/informação corporativos é exposta a riscos elevados no decorrer do funcionamento diário da organização.

Perante uma análise de risco efetuada à plataforma existente, concluiu-se que os principais vetores de risco não se encontram mitigados, devendo, para tal, existir um planeamento estruturado de acordo com as necessidades da organização, devidamente associado a uma análise de segurança corretiva e preventiva, para a infraestrutura tecnológica e aplicacional da Câmara Municipal de Paços de Ferreira.

3.1. Análise de Risco

ÁREA	RISCO
Segurança de Perímetro	Elevado
Arquitectura de Rede	Elevado
Segregação de Redes	Elevado
Acessos Remotos	Reduzido
Domínio Corporativo	Crítico
Gestão de Conteúdos	Médio
Backup & Restore	Crítico
Gestão de Actualizações	Elevado
Políticas de Segurança	Elevado
Monitorização e Alarmística	Crítico
Política de Passwords	Crítico
Sistemas Críticos	Elevado
Configurações de Serviços	Elevado
Segurança Física	Elevado
Gestão de Catástrofes	Elevado

Figura 5 – Risco por Área (Fonte: Autor)

Na figura 5, pode ver-se o grau do risco relativamente às diversas áreas como, por exemplo, com risco crítico, Monitorização e alarmística, políticas de passwords, domínio corporativo e backup e restore. Todas estas falhas, muito graves, foram detetadas.

3.2. Política de Segurança da Informação

As decisões tomadas por um administrador/responsável de sistemas de informação irão determinar quão segura ou insegura é a sua rede, quantas funcionalidades ela irá oferecer e qual será a facilidade em utilizá-la. No entanto, não é possível tomar decisões adequadas sobre segurança da informação sem antes determinar quais são as metas de segurança a atingir. Até que estas sejam determinadas, não se poderá fazer uso efetivo de qualquer conjunto de ferramentas de segurança, pois não existirá um conhecimento sobre as áreas a verificar e quais as restrições a impor.

Uma política de segurança adequada define-se como sendo a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.

O principal propósito da existência de uma política de segurança é informar, todos os que constituem a organização, dos deveres e obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados.

A tentativa de utilização de um conjunto de ferramentas de segurança, na ausência de pelo menos uma política de segurança implícita, não faz qualquer sentido.

Para que uma política de segurança seja apropriada e efetiva, deverá ter a aceitação e o suporte de todos dentro da organização. É de especial importância que a administração apoie, por completo e de forma inequívoca, o processo de implementação de uma política de segurança. Caso contrário, a mesma não terá o impacto pretendido.

No instante em que a política for estabelecida, a mesma deverá ser claramente comunicada de uma forma global, devendo ser criado um documento em que os utilizadores assinem, dizendo que a leram, entenderam e concordam. Esta é uma questão de especial importância em todo o processo. Por fim, a política deverá ser revista periodicamente, verificando-se se a mesma está a ter o sucesso desejado perante as necessidades pretendidas, respeitantes à segurança da informação.

No intuito de tornar uma política de segurança viável a longo prazo, é necessário contemplar uma flexibilização de nível elevado, baseada no conceito de segurança da arquitetura da infraestrutura tecnológica.

Verificou-se a ausência de políticas formais de segurança corporativas, implementadas e aplicadas à organização e aos seus sistemas de informação, devidamente acreditadas e aplicadas pela organização, o que impede a clara definição dos objetivos a cumprir, no que respeita à segurança da informação, assuntos ou sistemas específicos.

Não existe um documento formal que expresse as preocupações do Executivo e estabeleça as linhas mestras para a gestão da segurança da informação, aprovado por esse mesmo Executivo, publicado e comunicado de forma adequada a todos os colaboradores da instituição.

Apesar de haver um conjunto de procedimentos que tentam assegurar a segurança da informação, não existe um conjunto de políticas de segurança formais, ligadas aos sistemas de informação, presentes na plataforma tecnológica da organização.

Implicitamente, não existe um gestor que seja exclusivamente responsável pela manutenção e análise crítica da política de segurança da informação, de acordo com um processo de análise crítica definido, e que ocorra como decorrência de qualquer mudança que venha a afetar a avaliação de risco original, tais como incidentes de segurança significativos, novas vulnerabilidades ou mudanças organizacionais.

No entanto, encontram-se implementados procedimentos adequados referentes à componente de análise e filtragem de conteúdos, que são minimamente adequadas para a realidade da organização.

Não se encontra implementado um procedimento formal de realização de *backups* da informação presente na totalidade dos servidores da plataforma tecnológica. Apenas são realizados *backups* diários com uma política de rotatividade semanal, ao servidor aplicacional e ao servidor SIG.

Não existe um registo da descrição de procedimentos para a realização dos referidos *backups,* assim como a implementação de uma política formal para a realização dos mesmos e a respetiva política de rotatividade implementada.

Não existem planos de recuperação da informação referente aos dados corporativos, com a agravante da informação não ser regularmente analisada com o intuito de avaliar a sua integridade.

Não é efetuada a distribuição geográfica das cópias de segurança, por diversos locais, como seria o correto.

Não existe um plano de *Disaster Recovery* corporativo, que abranja a totalidade dos sistemas da plataforma tecnológica da organização, de forma a garantir um nível de conformidade adequado, perante a manutenção do negócio da organização.

Do mesmo modo, não existem planos de contingência formais para casos de desastre ou perda de informação, referente aos dados corporativos, não sendo a informação regularmente analisada com o intuito de avaliar a sua integridade.

Não existe uma política de integração adequada da segurança de perímetro com a segurança interna da organização.

No decorrer da auditoria, não foi detetada a existência e implementação de uma política corporativa específica e adequada para a utilização de passwords dentro da organização, no que concerne aos níveis de segurança desejados.

Através de ferramentas de análise/auditoria adequadas, verificou-se que as passwords, que estão a ser utilizadas no momento pelos utilizadores, têm um nível extremamente fraco, pois não foram necessários mais do que uns escassos minutos para que uma grande percentagem das mesmas fosse descoberta, sendo a totalidade das mesmas revelada nos instantes seguintes.

3.3. Organização da Segurança da Informação da organização

A organização da segurança da informação diferencia as relações ou responsabilidades do nível de segurança da informação, por parte de colaboradores internos e por parte de entidades externas.

A segurança da informação é uma responsabilidade organizacional, partilhada por todos os membros da direção de uma instituição. Como tal, deverá existir uma estrutura de gestão para controlar a implementação de políticas formais de segurança da informação, no interior da organização, garantindo um direcionamento claro para as iniciativas de segurança da informação.

É de extrema importância e utilidade a existência de consultoria especializada em segurança da informação no interior das organizações. Em condições ideais, deverá existir nas mesmas um consultor de segurança da informação especializado, com vasta experiência na área. A qualidade das suas ações determinará a eficiência da segurança da informação da organização.

Na atualidade, as organizações recorrem cada vez mais a prestação de serviços por entidades externas, em que as mesmas têm acesso a sistemas e informação corporativa classificada como crítica e de extrema importância.

Como tal, convém que o acesso destas entidades aos sistemas de informação corporativa seja corretamente controlado, sendo necessário efetuar previamente uma análise e avaliação dos riscos envolvidos para que sejam determinadas as possíveis implicações na segurança e controlos necessários a serem implementados.

A avaliação do tipo de acesso facultado aos prestadores de serviços externos é de especial importância. Por exemplo, os riscos associados ao acesso através de uma ligação à rede corporativa são diferentes dos riscos associados a um acesso físico à organização. Como tal, diferentes medidas e análises deverão ser consideradas.

Com o decorrer da auditoria de segurança da informação, realizada na Câmara Municipal de Paços de Ferreira, verificou-se que, apesar de estarem estabelecidos procedimentos que visam a segurança da informação e dos mesmos serem geridos pelos membros da unidade de informática, não existe uma equipa dedicada, por membros da unidade de informática, que implemente e dirija as políticas formais de segurança, aplicadas à informação e sistemas corporativos da organização.

A não existência do referido fórum impede a análise crítica e a aprovação de uma política formal de segurança da informação para a organização, assim como as responsabilidades envolvidas.

Não é realizada a monitorização exclusiva e dedicada das principais mudanças na exposição dos recursos da informação, às principais ameaças que estão constantemente a surgir, assim como dos incidentes de segurança da informação que ocorram.

Não existe a aprovação formal das principais iniciativas para o incremento do nível de segurança da informação corporativa, por um órgão interno com análise crítica e ligado diretamente ao executivo.

Não está a ser efetuada a avaliação crítica e formal dos incidentes de segurança que surgem no dia a dia e não existe, na organização, um consultor interno especializado na área da segurança da informação. No entanto, existem colaboradores específicos que coordenam

o conhecimento, assim como as experiências internas, de forma a garantirem a consistência e o auxílio nas tomadas de decisão sobre o tema da segurança.

Não são mantidos contactos formais com autoridades legais e organismos reguladores, (prestadores de serviços de informação e operadores de telecomunicações) de forma a garantir que ações adequadas e apoio especializado possam ser rapidamente acionados, no caso de ocorrerem incidentes relacionados com a segurança da informação.

O acesso de prestadores de serviços aos recursos de processamento da informação está a ser minimamente controlado, através de controlos de segurança implementados (acesso físico e lógico). No entanto, não é efetuada, de forma regular, uma avaliação dos riscos envolvidos, para que sejam determinadas as possíveis implicações na segurança e os controlos necessários a implementar.

Não existem acordos que envolvam o acesso de prestadores de serviços aos recursos de processamento da informação da organização, baseados em contratos formais que deverão fazer referência aos requisitos de segurança, de forma a garantir a conformidade com as normas e políticas de segurança em vigor na organização.

Na organização, não existem recursos humanos, dedicados especificamente à análise e controlo dos sistemas de segurança da informação.

Não existe uma separação, dentro da organização, entre funções de auditoria/conformidade de segurança da informação e funções de implementação de tecnologia.

Tal facto implica que não exista uma organização da segurança da informação mais independente dentro da instituição, que resulta da necessidade de uma abordagem holística de segurança, que combina um pensamento estratégico com as capacidades operacionais que operam sobre esse conhecimento. Abordagem essa que pretende unir pessoas, processos e tecnologias, de forma a que as necessidades de segurança estejam alinhadas com as necessidades da organização.

3.4. Classificação e Controlo dos Recursos de Informação

Uma organização deve proceder à identificação dos recursos de informação, assim como à documentação da importância desses mesmos recursos. A classificação e controlo

da mesma deverá incluir toda a informação necessária para o caso de haver necessidade de se efetuar uma possível recuperação de um desastre que possa ocorrer, como a identificação do tipo de recurso, seu formato, localização, cópia de segurança, informação do licenciamento e o seu valor para o negócio da organização.

Baseado na importância do bem em questão, e do seu valor para o negócio, deverão ser implementados níveis de segurança de acordo com a sua importância.

Um conjunto apropriado de procedimentos de segurança deverão ser definidos para classificar e tratar a informação de acordo com o esquema de classificação adotado pela organização. Estes procedimentos precisam de abranger todos os recursos de informação.

A realização do inventário dos recursos de informação permite assegurar que as proteções adequadas estão a ser realizadas de forma correta, podendo também ser requerido para outras finalidades de negócio, como saúde e segurança no trabalho, seguros ou área financeira (gestão patrimonial).

O processo de compilação de um inventário dos recursos de informação é um aspeto extremamente importante na gestão de risco. Uma organização deve ser capaz de identificar os seus recursos de informação e respetivos valores e importância. Baseada nesta informação, uma organização pode, então, fornecer níveis de proteção proporcionais ao valor e importância desses mesmos recursos.

Convém que um inventário dos principais recursos associados a cada sistema de informação seja estruturado e mantido. Convém que cada recurso e seu respetivo proprietário sejam claramente identificados e a respetiva classificação de segurança seja acordada e documentada, juntamente com a sua localização atual.

3.5. Controlo e Classificação dos Recursos de Informação

Não se verificou a existência da realização de um inventário dos principais ativos associados a cada sistema de informação, devendo o mesmo ser estruturado e atualizado de forma regular.

Verificou-se que cada recurso e o seu respetivo proprietário não estão claramente identificados, assim como não é efetuada a classificação de segurança, relativa ao nível de criticidade para a organização.

Verificou-se a existência de proteções adequadas nos principais recursos de informação, presentes na organização, que asseguram um nível mínimo de proteção.

Existe um conjunto de procedimentos, embora não estejam formalmente definidos na política de segurança da informação da organização, que tratam da classificação e tratamento da informação, de acordo com o esquema de classificação adotado pela organização. Os procedimentos verificados abrangem os diversos recursos da informação, nos diversos formatos (físico e lógico).

Os controlos de segurança implementados têm em consideração as necessidades do negócio para a partilha ou restrição de informações (embora não reflitam o impacto na organização) e de acessos não autorizados ou perda de informação.

Não é efetuada a classificação formal da informação e respetivos recursos, em termos de criticidade para a organização, de acordo com o seu valor e sensibilidade para a mesma.

Não é efetuada a avaliação formal de cada um dos recursos identificados, quanto ao potencial impacto negativo causado sobre o negócio face a uma eventual situação de indisponibilidade ou concretização de ameaça sobre esse mesmo recurso.

3.6. Segurança da Informação vs. Recursos Humanos

Muitas vezes, a segurança da informação é quebrada por elementos internos, devido a diversos fatores, como são, por exemplo, as questões e crises económicas. Como tal, cada recurso humano só deverá conhecer e ter acesso à informação estritamente necessária ao desempenho da sua função, conseguida através da implementação de diversos níveis de acesso de segurança, relativos à informação corporativa.

Deverão ser desenvolvidas ações de formação e sensibilização para a problemática da insegurança da informação, contemplando todos os recursos humanos da organização. Deverão ser distribuídas responsabilidades e papéis a desempenhar por cada um dos elementos, face a uma situação de quebra de segurança ou catástrofe. Regras e responsabilidades de segurança deverão ser documentadas onde for apropriado, de acordo com a política de segurança da informação implementada e em vigor na organização. Convém que elas incluam quaisquer responsabilidades gerais pela implementação ou manutenção da política de segurança, assim como quaisquer responsabilidades específicas para a proteção

de determinados recursos, ou pela execução de determinados processos ou atividades de segurança.

Todos os recursos humanos de uma organização e prestadores de serviço externos deverão estar conscientes dos procedimentos para notificação dos diversos tipos de incidentes (violação da segurança, ameaças, fragilidades ou mau funcionamento) que possam ter impacto na segurança dos recursos organizacionais. Convém que eles sejam solicitados a notificar quaisquer incidentes ocorridos ou suspeitos, o mais rapidamente possível, ao ponto de contacto designado. Convém que a organização estabeleça um processo disciplinar formal para tratar com os funcionários que cometam violações na segurança.

Para ser capaz de lidar com os incidentes de forma apropriada, deverão ser recolhidas evidências, o mais rapidamente possível, após a sua ocorrência.

Processos disciplinares formais deverão existir para os colaboradores que tenham violado as políticas e procedimentos de segurança organizacional. Este tipo de processo pode dissuadir os colaboradores que, de outra forma, seriam inclinados a desrespeitar os procedimentos de segurança. Adicionalmente, convém que se assegure um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança, sérias ou persistentes.

Não estão documentadas regras e responsabilidades relacionadas com a segurança da informação, de acordo com a política formal de segurança de informação da organização que deveria existir.

Inerentemente, não estão formalmente definidas quaisquer responsabilidades gerais pela implementação ou manutenção da política de segurança da organização, assim como quaisquer responsabilidades específicas para a proteção de determinados recursos de informação, ou pela execução de determinados procedimentos ou atividades relacionadas com a segurança da informação.

No caso dos colaboradores temporários e prestadores de serviços, que não estão abrangidos pela existência de um contracto de trabalho ou prestação de serviço, não é exigida a assinatura de um acordo de confidencialidade, antes do acesso às instalações de processamento de informação.

No entanto, existe um processo de avaliação e supervisão das atividades destes colaboradores, com autorização de acesso a sistemas críticos.

Formalmente, não está definido e registado no documento da política de segurança da organização a distribuição das diferentes responsabilidades e funções a desempenhar por cada um dos elementos ligados aos sistemas presentes na plataforma tecnológica da organização, face a uma situação de quebra de segurança ou catástrofe.

Não é realizado o desenvolvimento de ações de formação e sensibilização para a problemática da insegurança da informação, a todos os colaboradores da organização e prestadores de serviços (sempre onde e quando se justificar), embora existam procedimentos informais e a consciencialização das pessoas, que visam assegurar a proteção dos recursos e informação considerados críticos para a organização.

3.7. Segurança Física e Ambiental

Um dos aspetos de segurança mais básico e importante a ser considerado numa organização diz respeito à segurança física das instalações e dos sistemas de informação. Na maioria dos casos, por mais seguro que seja um sistema, um acesso indevido pode comprometer toda a informação. A segurança física de instalações, apesar de constituir uma questão de vital importância para o seu normal funcionamento, é, muitas vezes, subalternizada, senão mesmo marginalizada pela maioria, com particular incidência nas instalações onde se encontra a plataforma tecnológica das organizações.

As ameaças internas podem ser consideradas como o risco número um à segurança dos recursos tecnológicos. Uma estrutura de segurança física apropriada é o passo inicial para a proteção da organização, no sentido de salvaguardar a informação contra acessos indevidos.

Neste aspeto, existem três princípios simples e básicos:

- ✓ Manter as pessoas afastadas;
- ✓ Restringir o acesso;
- ✓ Proteger a rede.

Convém que os recursos e instalações de processamento de informações críticas ou sensíveis do negócio estejam localizadas em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e respetivo controlo de acesso (físico e lógico). Convém que estas áreas sejam protegidas, do ponto de vista físico, de acessos não autorizados, de deterioração ou interferência. Convém que a proteção estabelecida seja proporcional aos riscos identificados, através da avaliação e análise de risco realizada.

A proteção física pode ser conseguida através da criação de diversas barreiras físicas em torno da propriedade física da organização e das instalações dos recursos de sistemas e tecnologias da informação.

Cada barreira estabelece um perímetro de segurança, contribuindo para o aumento da proteção total fornecida. Um perímetro de segurança define-se como sendo algo que estabeleça uma barreira ou limite, por exemplo, uma parede, uma porta com controlo de entrada através de um cartão, ou mesmo um balcão de controlo de acesso com registo manual. A localização e a resistência de cada barreira dependem dos resultados de uma avaliação de risco.

O acesso às instalações da Câmara Municipal de Paços de Ferreira é realizado através de uma portaria, onde é efetuada a identificação das pessoas e posterior encaminhamento das mesmas para os locais pretendidos, sendo registadas a data e a hora da sua entrada e saída.

Verificou-se que os recursos e instalações de processamento de informação crítica ou sensível ao negócio, pertencentes à plataforma tecnológica da organização, estão localizados em áreas minimamente seguras, embora não exista um perímetro de segurança claramente definido.

Apesar de existirem diversas barreiras físicas de acesso, não existe um sistema lógico de controlo de acessos no interior das instalações que impeça as pessoas, que se encontrem no interior da mesma, de acederem, fisicamente, às áreas de maior criticidade da organização.

Não existe uma forma de identificação visível por parte de todos os colaboradores, como, por exemplo, cartões identificativos que sejam utilizados para autorizar e validar qualquer acesso às diversas áreas, com a respetiva permissão, de forma a facilitar a identificação de

qualquer pessoa estranha à organização que não esteja devidamente autorizada e acompanhada.

Parte dos sistemas pertencentes à plataforma tecnológica da organização está fisicamente protegida contra ameaças à sua segurança e perigos ambientais.

No entanto, a totalidade dos mesmos não está instalada de forma a reduzir o risco de ameaças ambientais, perigos e oportunidades de acesso não autorizado.

A porta que dá acesso às instalações onde se encontra a plataforma tecnológica da organização não possui um dispositivo básico de fecho automático (mola), assim como não apresenta características de corta-fogo e sensores de alarme.

Não estão protegidos contra falhas de energia e outras anomalias na alimentação elétrica todos os equipamentos (quando justificável) assentes na plataforma tecnológica da organização. Nestes casos, o fornecimento de energia apropriado não ocorre de forma automática e apropriada, em conformidade com as especificações dos fabricantes dos equipamentos.

No entanto, este tipo de equipamentos não é verificado de forma periódica, de forma a garantir que o mesmo esteja com a capacidade adequada, nem é testado de acordo com as recomendações do fabricante.

Não foi detetada a existência de um sistema eletrónico de vigilância nas instalações, incluindo a sala onde se encontram localizados os sistemas pertencentes à plataforma tecnológica da organização.

Verificou-se a existência de um sistema de ventilação adequado, no local onde se encontra a plataforma de sistemas e comunicações.

No entanto, verificou-se a existência de um sistema adequado de deteção de incêndio, no interior das instalações, incluindo o local onde se encontra a plataforma de sistemas de informação.

Não existe, no local onde se encontra a plataforma de sistemas e comunicações, um sistema automático de incêndios que seja específico e adequado a esse local. Contudo,

existem alguns extintores manuais distribuídos pelo edifício (existindo um nas imediações da sala de sistemas).

Verificou-se que a cablagem elétrica e de comunicações, que transmite dados ou suporta os serviços de informação, se encontra protegida contra interceção ou deterioração, através de proteção adequada disponibilizada pela presença de calha técnica, evitando a sua exposição através de locais de acesso público.

Os cabos elétricos não se encontram separados dos cabos de comunicações, através de dispositivos apropriados (calha técnica), de forma a que sejam prevenidas interferências eletromagnéticas.

Verificou-se que os equipamentos pertencentes à plataforma tecnológica da organização não estão sujeitos a uma manutenção correta e apropriada, de forma a que seja garantida a continuidade da disponibilidade e integridade dos mesmos.

Informação e recursos tecnológicos não estão adequadamente protegidos de divulgação, modificação ou roubo por pessoas não autorizadas, através da implementação correta de controlos de segurança adequados que minimizem a sua perda;

Verificou-se a existência de armários (rack's) apropriados para a localização dos equipamentos da plataforma tecnológica dos sistemas de informação

Não se verificou a presença de políticas formais aplicadas à organização para que equipamentos, informações ou *software* não sejam retirados da organização sem a devida autorização.

De igual forma, não são efetuados controlos de segurança que permitam detetar a remoção não autorizada de propriedade, assim como a entrada de novos equipamentos

3.8. Controlo de Acessos

O controlo de acessos caracteriza-se como sendo o processo de autorização de acesso a informação e objetos de rede a utilizadores, grupos de utilizadores e postos de trabalho. Os conceitos-chave que o constituem são: permissões, direitos de utilizador, credenciais de acesso e auditoria de objetos.

Um dos principais problemas, que envolve a segurança do ambiente corporativo, prende-se com o fator humano. A forma como os utilizadores interagem com os diversos ambientes e sistemas da empresa representa a maioria dos incidentes relacionados com a segurança da informação.

Pode-se mesmo dizer que os problemas relacionados com a interação dos colaboradores da empresa estão diretamente ligados a controlos de acesso lógico.

Uma política de acesso na rede adequada especifica quais os sites e conteúdos que podem ser acedidos por cada um, se um protocolo concreto está acessível para comunicações de entrada e saída e se as comunicações entre endereços IP especificados, utilizando protocolos e portas específicos, devem ser permitidas ou negadas.

A segurança de perímetro e a segurança física são fatores essenciais para elaborar uma política de controlo de acessos correta. Adicionalmente, serviços de autenticação e autorização de fácil utilização asseguram que apenas os utilizadores autorizados conseguem aceder à rede.

O recurso a VPNs fornece o controlo de acessos e a encriptação de dados entre diferentes recursos de uma rede. Isto permite que os utilizadores se liguem remotamente à rede corporativa sem o risco de um *hacker* intercetar a informação.

A utilização de redes WLANs dentro de redes empresariais é já muito comum. Os empregados apreciam a liberdade e mobilidade proporcionada pelas redes *wireless* e as empresas beneficiam do aumento de produtividade que estas implicam. Mas os Gestores IT consideram que existem riscos de acesso ilegítimo a alguns APs, por dispositivos de utilizadores não autorizados. Para diminuir os ataques e manter a rede segura, as WLANs empresariais necessitam de ser instaladas com capacidades de autenticação e encriptação robustas.

O acesso à informação e respetivos processos de negócio não estão totalmente protegidos e controlados com base nos requisitos de segurança e do próprio negócio.

O sistema de controlo de acessos (*firewall*) responsável pela segurança de perímetro está corretamente configurado, apresentando um nível reduzido de exposição para o exterior, embora exista um circuito de acesso à Internet, por onde o acesso é realizado de forma não controlada, onde é exposta a informação corporativa a riscos extremamente elevados.

Existe um circuito de acesso remoto a um posto de trabalho, com uma aplicação específica, através do qual é disponibilizado um acesso livre e não controlado à totalidade dos recursos da organização.

As regras de controlo de acessos e privilégios de cada utilizador ou grupo de utilizadores não estão claramente definidas, nem estão refletidas no documento da política de segurança referente ao controlo de acessos que deveria existir.

Não existe um procedimento de registo e cancelamento de utilizadores, para obtenção/cancelamento de acessos aos sistemas de informação, através de um processo formal, presente no documento da política de segurança de informação que deveria existir.

No momento da avaliação, não foi detetada a existência de uma política corporativa formal de utilização de *passwords,* adequada às necessidades da organização, de forma a prevenir acessos não autorizados.

O mecanismo de controlo de acesso básico a cada sistema (login e password), para além de não estar baseado num domínio corporativo, não apresenta a configuração que permita sustentar um nível de segurança adequado. Tendo sido possível o acesso à lista de credenciais dos utilizadores (usernames / passwords) de alguns sistemas, foi conduzida uma auditoria à resistência destas. Os resultados permitiram revelar, num curto período de tempo, as credenciais da maioria dos utilizadores.

A maioria das passwords dos utilizadores foram descobertas nos primeiros minutos de auditoria, tendo como base a utilização de dicionários (listas de palavras comuns em português, inglês e francês), e encontram-se inalteradas há um longo período de tempo.

Foi detetado um conjunto de credenciais de administradores (locais) sem qualquer password. Do mesmo modo, detetou-se que uma grande maioria de utilizadores, com privilégios de administração, se encontrava com as credenciais de acesso (passwords) inalteradas há um longo período de tempo.

Verificou-se a ausência da realização de um controlo efetivo sobre o acesso aos dados e serviços de informação por parte dos utilizadores, através de um processo formal de análise crítica realizado periodicamente.

Os acessos remotos à informação corporativa são realizados através de uma solução de mobilidade adequada à realidade da organização, através da qual são efetuadas ligações seguras (VPNs) entre a organização e o local remoto, em que o utilizador está sujeito a processos de autenticação e a informação é encriptada.

Existem e estão implementados controlos de segurança de rede, através da divisão da mesma em vários domínios lógicos de redes (interno e externo), protegidos por um perímetro de segurança definido, embora exista um circuito de acesso à Internet alternativo que quebra estes mesmos controlos de segurança, expondo a informação corporativa a riscos extremamente elevados.

Verificou-se a inexistência de procedimentos e sistemas para a monitorização do uso dos recursos de informação, de forma que seja possível detetar divergências entre a política de controlo de acessos e o registo de eventos que ocorram, de modo a serem fornecidas evidências no caso da ocorrência de incidentes de segurança.

Não são efetuadas análises dos resultados dos incidentes de segurança que ocorrem, através de um processo formal de análise crítica efetuado regularmente e de forma que seja possível compreender as ameaças detetadas nos sistemas e a razão das mesmas estarem a acontecer.

A comunicação com os routers e firewall, no interior da organização, é permitida através da rede dos postos de trabalho, o que aumenta o risco de intrusão.

Não foi detetada a existência de processos de monitorização ou controlo da qualidade de serviço (QoS) nos circuitos de acesso à Internet.

Verificou-se a existência de uma análise informal aos registos logs dos sistemas, realizada sob a plataforma de servidores da organização, embora não esteja definida uma periodicidade regular com que deveriam ser realizadas.

Não foram detetados mecanismos de controlo de fluxo de tráfego interno, mas existe um sistema de controlo de acessos Web, que faz o armazenamento de informação, analisa e controla os conteúdos.

Apesar de existir um sistema de controlo de acessos Web, que faz o armazenamento de informação (proxy – Squid), o modelo de controlo de acessos revelou ser altamente

permissivo. Não existe qualquer tipo de classificação de nível confidencialidade ou modelo que permita manter a integridade da informação. Através do acesso incondicional (livre) aos *routers*, é permitido um acesso descontrolado à Internet.

Não existem restrições relativas ao acesso à rede via endereço MAC e verificou-se a inexistência de uma plataforma de publicação de serviços externos (DMZ), o que impossibilita a existência de um nível de separação de tráfego distinto entre o perímetro e a rede interna da organização, o que, por si só, expõe a informação corporativa da organização a riscos extremamente elevados.

3.9. Desenvolvimento e Manutenção da Segurança de Sistemas

Projetos de tecnologias de informação e atividades de suporte deverão ser conduzidos desde o seu início, tendo em conta as normas de segurança de informação e respeitando as políticas em vigor na organização.

A verificação dos requisitos adequados a implementar, para os sistemas de informação, garante que a segurança da informação seja parte integrante dos mesmos. Isto incluirá a própria infraestrutura tecnológica, aplicações do negócio e aplicações desenvolvidas pelo próprio utilizador.

O projeto e a implementação dos processos do negócio, que dão suporte às aplicações e aos serviços, podem ser cruciais para as questões ligadas com a segurança da informação. Convém que requisitos de segurança sejam identificados e acordados antes do desenvolvimento de sistemas de informação. Todos os requisitos de segurança, incluindo a necessidade de estabelecer acordos de contingência, deverão ser identificados na fase de levantamento de requisitos de um projeto, acordados e documentados como parte do estudo de caso de um negócio para um sistema de informação.

Para o desenvolvimento de um projeto específico, deverá ser contabilizada a integração de sistemas criptográficos, para que a informação, considerada de risco, seja devidamente protegida e para os quais outros controlos de segurança já implementados não forneçam a proteção adequada.

Todos os projetos de tecnologias de informação deverão ser conduzidos de forma segura. Para tal, o acesso a toda a informação, contida nos diversos arquivos de informação, deverá ser devidamente controlada. A manutenção da integridade dos sistemas de informação deverá ser da responsabilidade da função desempenhada pelo utilizador ao qual pertence a aplicação ou sistema.

Todos os ambientes de desenvolvimento e suporte deverão ser controlados de uma forma rígida. A segurança destes ambientes deverá ser da responsabilidade dos que têm a seu cargo os sistemas de informação. Deverão garantir que todas as modificações dos sistemas que forem propostas sejam analisadas de forma crítica, com a finalidade de assegurar que as mesmas não comprometem a segurança dos sistemas ou o ambiente em que estão inseridos.

A arquitetura de rede provou ser inadequada, atendendo às exigências e aos requisitos mínimos de segurança a serem impostos perante a dimensão da infraestrutura tecnológica da organização.

Não existe uma solução de domínio corporativo, implementado na Câmara Municipal de Paços de Ferreira, não sendo utilizada a totalidade das funcionalidades e potencialidades do conceito de sistemas de diretórios da AD. Este tipo de solução garante capacidades acrescidas ao nível da gestão, flexibilidade e segurança dos elementos inerentes a qualquer organização que baseie o seu negócio numa infraestrutura organizacional SI/TI.

A confidencialidade da informação encontra-se comprometida, devido à falta de segregação de tráfego entre postos de trabalho que são confiáveis e postos de trabalho de acesso livre. Não estão definidos níveis de segurança ou de acesso na rede, atribuindo uma exigência de segurança idêntica entre todas as plataformas de sistemas (servidores, postos de trabalhos, acessos livres, etc.).

Consequentemente, a rede de comunicações interna é vulnerável a ataques provenientes do interior da organização, sendo simples a alguém com algum conhecimento e com um motivo, que tenha acesso local a um posto de trabalho ou a um ponto de rede, aceder a outros locais de rede para conseguir informação considerada classificada.

Não existe qualquer mecanismo de controlo de fluxos de tráfego entre LAN e WAN e não foram detetados quaisquer mecanismos de controlo e/ou compressão de fluxo de tráfego interno (internamente ou através do ISP em vigor).

Não está implementado um processo de alarmística sobre os conceitos de quebra/qualidade de serviço sobre a plataforma crítica da organização.

Está implementado um processo regular de auditoria sobre as permissões a nível do servidor de ficheiros e respetivas ACL's, embora não esteja formalizado como política de segurança.

Não está assegurado, na organização, que os projetos relacionados com tecnologias de informação e atividades de suporte sejam conduzidos desde o seu início, de forma adequada, tendo em conta os aspetos formais relacionados com a segurança da informação.

Verificou-se o controlo de segurança do ambiente de funcionamento onde está presente a plataforma tecnológica da organização, de forma a garantir níveis aceitáveis de exposição ao risco.

Contudo, não estão estabelecidos processos formais que controlem as restrições de segurança no acesso a sistemas e serviços corporativos, segundo a política de segurança da organização.

Propostas de modificações de sistemas não são analisadas desde o seu início, de forma crítica, com o intuito de se verificar se as mesmas não comprometem a integridade da segurança do sistema ou do ambiente de produção.

Não estão a ser utilizados métodos de autenticação de mensagens transmitidas, eletronicamente, para aplicações onde existe a necessidade de requisitos de segurança para a proteção do conteúdo da referida mensagem (assinaturas digitais).

Não existe uma análise de risco de segurança para determinar e identificar o método mais apropriado de implementação de autenticação de mensagens.

A plataforma de postos de trabalho não está abrangida por políticas de segurança (GP). Do mesmo modo, a plataforma de sistemas críticos (servidores corporativos e produtivos) não está integrada em políticas corporativas de segurança.

Verificou-se não estarem implementadas políticas de auditoria formais na organização. Não existe um procedimento formal implementado, para servidores e postos de trabalho, a nível de configurações de segurança e auditoria aos mesmos.

Verificou-se que a plataforma de sistemas, na sua maioria, não se encontra devidamente atualizada. Inclusive, foram detetadas várias vulnerabilidades graves de segurança em vários sistemas da plataforma de servidores.

Nos sistemas que apresentam algum nível de atualização, o processo é efetuado através do recurso à ferramenta do Windows Update, o que pressupõe um acesso Web contínuo e repetido, que origina um aumento do tráfego Web, diminuindo a performance da rede e aumentando os riscos em termos de segurança (exposição ao exterior).

Verificou-se a inexistência de uma solução corporativa, que permita a distribuição de atualizações (*Patch Management*) de forma centralizada e autónoma.

Da mesma forma, não estão definidas nem implementadas políticas globais que representem o processo de atualização da plataforma de sistemas.

Paralelamente, não existe um registo atualizado das “atualizações” que são efetuadas, não sendo mantido um controlo das versões (histórico) para todas as atualizações/intervenções realizadas.

Quando há a necessidade de serem realizadas modificações nos sistemas operativos dos servidores presentes na plataforma tecnológica da organização, como a instalação de *patchs* de segurança, as mesmas não são analisadas e testadas de forma crítica, a fim de garantir que não ocorra nenhum impacto adverso no seu funcionamento ou na segurança do sistema.

Não existe um processo uniformizado nem um modelo standard corporativo que defina e estabeleça um procedimento de instalação formal de sistema operativo e aplicações sobre a plataforma de postos de trabalho.

Não se encontra documentado um registo da topologia de rede minimamente atualizado, de forma a permitir uma rápida identificação dos componentes da mesma.

Em diversas máquinas, não está implementado o sistema de bloqueio automático, através de *screen savers*, quando o utilizador não está presente, ficando desprotegidas e acessíveis a qualquer um.

A maioria dos serviços ativos sobre a plataforma tecnológica apresenta uma grave lacuna na implementação de restrições de segurança.

A parametrização e configuração de segurança dos diversos sistemas operativos não foram efetuadas na maioria dos postos de trabalho, originando alguns vetores de ataque.

Foram detetados, como ativos, alguns serviços desnecessários em diversos postos de trabalho, incluindo alguns sistemas pertencentes à plataforma de servidores da organização.

Caso um atacante consiga ter o nível de acesso básico fornecido a qualquer posto de trabalho ligado à rede, será extremamente difícil perceber o tipo de ataque executado, como também ter a perceção de que existe um intruso na rede.

Os sistemas responsáveis pela componente de sistemas de informação na organização apresentam, na sua generalidade, um conjunto excessivo de serviços ativos. O risco de intrusão, baseado na exploração deste conjunto alargado de serviços “secundários”, é considerado como relevante, podendo dar origem a vários vetores de ataque com alto grau de probabilidade de sucesso. Ou seja, para além da sobrecarga de processamento nos servidores de domínio, ainda existe um acréscimo de exposição de segurança.

Os serviços mais críticos não são auditados de uma forma regular e periódica, nem adequadamente documentados após a sua verificação.

3.10. Gestão de Incidentes de Segurança da Informação

Muitas empresas despertam para a necessidade de implementação de um sistema de resposta e gestão de incidentes, apenas após a ocorrência de um evento de segurança da informação. O "*post hoc*" (depois disto) é um momento crítico, em que somos pressionados a tomar decisões que, na maioria das vezes, não são as mais indicadas, como, por exemplo: bloquear, corrigir, desligar? A resposta deverá ser previamente estudada, ou uma situação, que até então era crítica, pode tornar-se irremediável.

Uma organização moderna deverá ser capaz de lidar com incidentes de segurança da informação. A deteção e gestão precoce de tais eventos evita que os mesmos assumam grandes proporções e, como consequência, resultem, da ocorrência dos mesmos, prejuízos elevados que poderiam ser evitados.

Um sistema que reporte e gira os incidentes de forma sistemática fará com que os mesmos diminuam e sejam evitados, à medida que forem implementados controlos de segurança pró-ativos que evitem a sua ocorrência.

Uma política adequada e técnicas de prevenção contra intrusões são instrumentos tão ou mais efetivos do que as diversas ferramentas de deteção existentes, mas, se ambas falharem, deve haver um eficaz sistema de gestão de incidentes.

Deverá ser estabelecido um procedimento formal de informação da ocorrência de incidentes de segurança relacionados com a informação, assim como o respetivo procedimento de resposta ao incidente de segurança ocorrido, que estabeleça a forma correta de atuação.

Canais de informação de incidentes de segurança deverão existir numa organização, utilizando recursos que sejam de fácil acesso, com uma Intranet existente, telefones específicos, formulários e procedimentos. Desta forma, cria-se um mecanismo que atue, de forma precisa e eficaz, na resposta a incidentes de segurança, sejam eles eventos previstos ou inesperados, e que auxilie na sua prevenção.

Para uma avaliação permanente, deverão ser estabelecidas métricas de segurança com base na gestão de incidências, garantindo o direcionamento dos esforços para um mesmo sentido.

Não se detetou a existência de um processo/procedimento formal de comunicação dos incidentes de segurança, realizado de forma rápida e apropriada aos membros da direção responsáveis pelos sistemas presentes na plataforma tecnológica da organização.

Verificou-se a inexistência de um processo formal de registo e notificação da ocorrência de fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços.

Não existe um sistema adequado em que os utilizadores reportam ao gestor dos sistemas da informação o funcionamento incorreto e problemas relacionados com os sistemas.

Não existem mecanismos que permitam avaliar as quantidades e custos dos incidentes e do mau funcionamento dos sistemas.

Não estão definidos procedimentos, nem a classificação de incidentes de segurança, para que seja garantida uma resposta rápida, efetiva e ordenada.

Não são efetuados registos formais de auditoria e evidências similares para a ocorrência de incidentes de segurança que contemplem a análise e identificação das causas do incidente, planeamento e implementação de medidas para prevenir novamente a sua ocorrência.

3.11. Gestão da Continuidade do Negócio

Tem como objetivo não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.

A prevenção é a melhor forma de superar uma ameaça de desastre e o melhor desastre é aquele que for evitado.

Deverão ser desenvolvidos processos que permitam a gestão e melhoria contínuas de planos de contingência que protejam os processos críticos de negócio dos riscos existentes.

É de extrema importância que as consequências de desastres, falhas de segurança e perda de serviços ocorridos sejam devidamente analisadas. Planos de contingência deverão ser desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados dentro de um período de tempo considerado como aceitável. Tais planos deverão ser mantidos, assim como regularmente testados, de forma a se tornarem parte integrante de todos os outros processos de gestão da segurança.

A continuidade do negócio deverá ter como ponto de partida a identificação dos eventos que podem causar interrupções nos processos do negócio, como, por exemplo, falha de equipamentos, inundações e incêndios. Em seguida, convém que seja feita uma avaliação de risco para a determinação do impacto destas interrupções (tanto em termos de escala de impacto, quanto em relação ao período de recuperação).

Convém que estas atividades sejam executadas com o total envolvimento dos responsáveis pelos processos e recursos do negócio. A avaliação deve considerar todos os

processos do negócio e não deve estar limitada aos recursos e instalações de processamento da informação.

É de extrema importância que os planos de continuidade do negócio sejam mantidos por meio de análises críticas regulares e atualizações, de forma a assegurar a sua integridade. Os procedimentos deverão ser incluídos no programa de gestão de mudanças da organização, presente na política de segurança, de forma a garantir que as questões relativas à continuidade de negócios sejam devidamente tratadas.

Não existe, na organização, uma identificação clara dos sistemas críticos da empresa, reproduzidos e formalizados sobre a forma de uma política corporativa formal, apenas existindo uma perceção de que todos os elementos ligados com a operação são os mais críticos.

Nos sistemas críticos identificados, não se encontra assegurada a disponibilidade imediata dos repositórios dos servidores da plataforma tecnológica corporativa, embora alguns estejam protegidos através de sistemas redundantes de tolerância a falha.

Não existem procedimentos formais, reproduzidos sobre a forma de uma política corporativa de segurança para a reposição de hardware em sistemas críticos.

Não existem contratos de assistência que asseguram a reposição de hardware num curto período de tempo.

Não existem soluções de deteção de *quebra de serviço* para a plataforma de sistemas críticos, assim como não existe um processo de alarmística (geração de alarmes) na sua deteção.

Não existe uma política formal de salvaguarda dos registos de eventos do sistema, por um período de tempo estabelecido pela organização.

Não são efetuadas manutenções e auditorias periódicas aos sistemas críticos, com a regularidade pretendida e adequada, de forma a garantir o bom funcionamento e integridade dos mesmos.

Não existem planos de recuperação das operações de negócio, na escala de tempo requerida, após a ocorrência de interrupções ou falhas de sistemas críticos, mantidos através de análises críticas regulares e respetivas atualizações, de forma a assegurar a sua efetividade contínua.

3.12. Conformidade

A conformidade caracteriza-se como sendo a capacidade de demonstração a todos os elementos humanos da organização, clientes, fornecedores e autoridades externas do compromisso no cumprimento de normativo legais e outras normas, internas ou externas, relacionadas com a informação.

O seu objetivo passa por evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentos ou obrigações contratuais e de quaisquer requisitos de segurança.

O projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários.

Para tal, consultoria em requisitos legais específicos deverá ser procurada em organizações de consultoria jurídica ou em profissionais liberais, adequadamente qualificados. Os requisitos legislativos variam de país para país e também para a informação criada num país e transmitida para outro (isto é, fluxo de dados internacional).

Estatutos, regulamentos ou cláusulas contratuais relevantes deverão ser explicitamente definidos e documentados para cada sistema de informação. Controlos de segurança e responsabilidades específicas para atender a estes requisitos deverão ser, de forma similar, definidos e documentados.

Os recursos de processamento da informação de uma organização são fornecidos para propósitos do negócio. Como tal, deverá existir a autorização do seu uso por parte da direção da instituição. Convém que qualquer uso destes recursos para propósitos não profissionais ou não autorizados, sem a aprovação do executivo, seja considerado como uso impróprio. Se essa atividade for identificada por processo de monitorização ou outros meios, deverá ser do conhecimento do gestor responsável para que sejam aplicadas ações disciplinares.

Por fim, a legalidade do processo de monitorização de utilização varia de país para país e pode requerer que os colaboradores sejam avisados dessa monitorização ou estejam formalmente em concordância com este processo.

Não se verificou a presença de estatutos, regulamentos ou cláusulas contratuais relevantes, explicitamente definidos e documentados para cada sistema de informação.

Não se detetou a implementação de procedimentos apropriados para garantir a conformidade com as restrições legais no uso de material, de acordo com as leis de propriedade intelectual.

Os registos de elevada importância da organização encontram-se protegidos em locais adequados, contra perdas, destruição e falsificações.

Não se verificou a presença de políticas de segurança corporativas, que impedem a utilização de *software* não autorizado e a utilização dos recursos corporativos de uma forma indevida e que não respeite as conformidades, aplicadas a toda a organização, conforme a política de segurança da organização.

Não existe a garantia formal de que os procedimentos de segurança, aplicados dentro da organização, estejam a ser executados em conformidade com as normas e políticas de segurança presentes e que nela deveriam existir.

Os sistemas de informação da organização não são periodicamente verificados, com a finalidade de se verificar se os mesmos respeitam e estão em conformidade com as normas de segurança implementadas e aplicadas a essa mesma organização.

Verificou-se a ausência de capacidade de demonstração, a todos os elementos humanos da organização, a clientes, a fornecedores e a parceiros externos, do compromisso no cumprimento de normativos legais e outras normas, internas ou externas, relacionadas com a segurança da informação.

3.13. Cultura e Organização da Instituição

Uma análise serena da cultura de segurança em Portugal evidencia um défice tremendo entre o que é feito e o que é necessário fazer, a bem da proteção das pessoas e das organizações.

Apontando o foco para este tema, ocorre questionar se é diferente a situação no mundo da segurança informática. A resposta é, decididamente, não. O cenário atual, neste domínio, é caracterizado por ameaças crescentes, decorrentes da, cada vez maior, importância dos sistemas de informação e do uso da Internet, com as empresas e as organizações a experimentarem dificuldades, ou mesmo ausência, na colocação em prática de medidas executivas de proteção dos seus negócios, estando a correr riscos que podem ser danosos para o seu futuro.

Estudos recentes indicam que 91% das empresas assumiram ter sido alvo de ataques informáticos, antecipando uma tendência crescente de agravamento do problema. Os números falam por si.

Uma vez mais se pode afirmar que, também, em Portugal se correm riscos ao nível da Segurança Informática, que ameaçam as organizações, a economia e, consequentemente, as pessoas.

O papel da segurança informática no desenvolvimento da sociedade de informação é muito simples de definir: a segurança de sistemas de informação é o pilar mais importante.

Pensar que se pode prescindir da segurança informática é alienar uma elevada probabilidade de sucesso e, mesmo, arriscar o seu fracasso.

É fundamental que as organizações tenham presente estes conceitos e que façam parte de uma cultura intrínseca da organização. Deverá haver a clara noção da importância vital para a salvaguarda da informação e tecnologia corporativa, que é a existência de um plano de segurança formal.

Embora se tenha verificado a ausência da implementação de uma política de segurança corporativa formal, a organização tem a noção da necessidade de confidencialidade e da elaboração de um plano de segurança dos sistemas e informação, tendo consciência de que os sistemas informáticos são um bem precioso para a empresa.

Não existe uma identificação formal dos sistemas de risco, presentes na organização, embora haja a noção dos riscos associados a que os mesmos possam estar expostos.

Não existem, neste momento, normas ou políticas de segurança formais na organização, embora haja diversos procedimentos implementados que zelam para que os requisitos de segurança sejam respeitados;

Será aconselhável a introdução de restrições adicionais, de uma forma formal, refletidos numa política corporativa de segurança, apoiada pela direção da organização, de forma a evitar a utilização desresponsabilizada da totalidade dos recursos corporativos por parte dos utilizadores.

4. Relatório Técnico

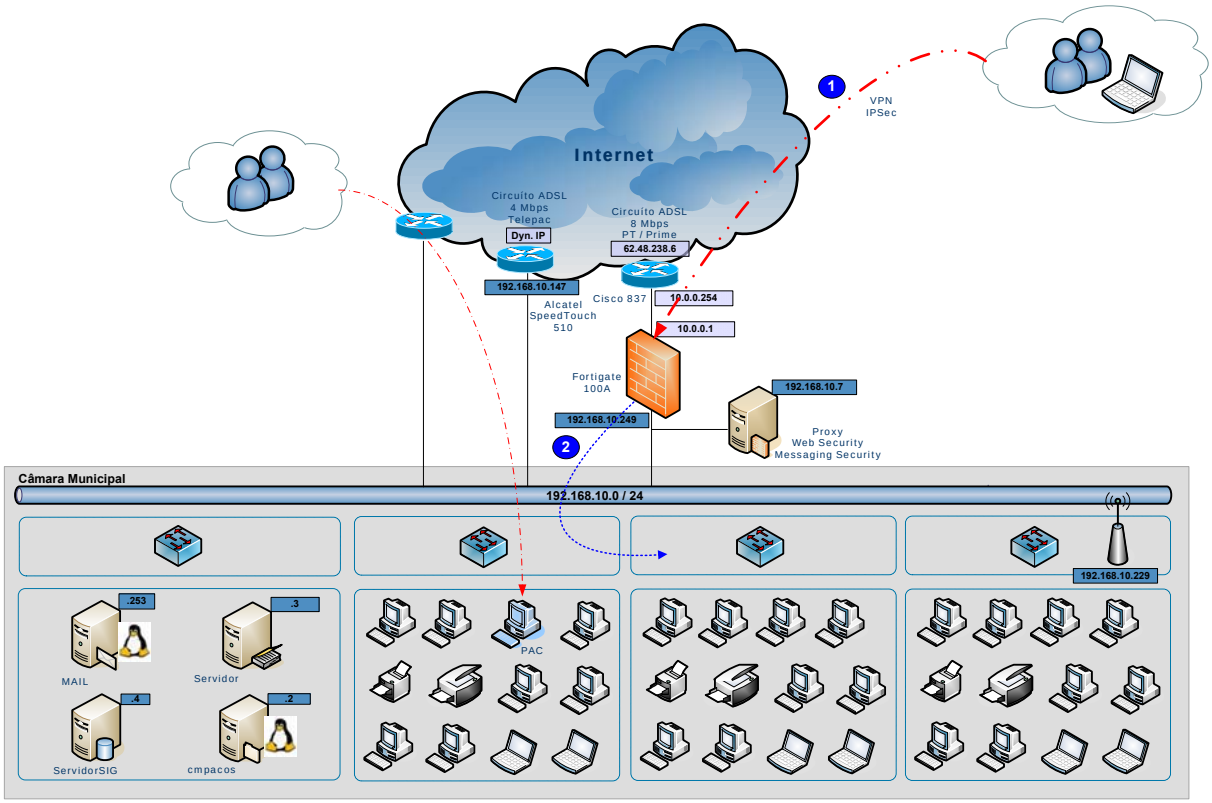

Figura 7 - Topologia de Rede (fonte: desconhecida)

4.1. Relatório de Vulnerabilidades - Servidores

CMPACOS

IP Address	Details	Hostname	Operating System
		cmpacos	Sun Microsystems SunOS (Sun StorEdge T300)

Figura 8 – Servidor de aplicações (Fonte: Autor)

Vulnerabilidades de alta segurança

Overflow de buffer remoto no Sendmail

Versões do Sendmail de 5.79 a 8.12.7 são vulneráveis a esse overflow de buffer.

Várias vulnerabilidades de Squid (versões anteriores do Squid 2-4 STABLE6 são vulneráveis)

Execução remota de código e / ou negação de serviço.

Servidor POP3 pode estar vulnerável a uma exploração de overflow de buffer remoto

Contém um overflow de buffer que pode resultar na sobre gravação da memória de processo, incluindo o endereço de retorno na pilha e a execução de código.

Possível overflow de buffer do snmpXdmid SunOS

Possível ataque de string de formato statd

Algumas versões desse serviço são vulneráveis (execute comandos arbitrários como root)

Vulnerabilidade de serviço RPC.ypasswdd

O serviço RPC.ypasswdd é vulnerável a uma exploração de overflow de buffer remoto.

Vulnerabilidade de overflow de buffer remoto, possível no daemon do protocolo de impressão

Solaris

Permitir que um invasor local ou remoto quebre o daemon (in.lpd) ou execute código arbitrário com privilégio de supervisor.

Vulnerabilidades de segurança médias

O serviço SNMP está ativado neste host

Inúmeras vulnerabilidades foram relatadas em implementações SNMP de vários fornecedores.

Oracle HTTP Server em execução

Servidor HTTP Oracle em execução neste computador

Serviço de dedo correndo

Usando um finger server, um utilizador remoto pode obter uma ampla gama de informações sobre utilizadores na máquina local.

TCP ports - 18 open ports

13[Description: Daytime => Time of the Day / Service: Unknown]
21[Description: FTP => File Transfer Protocol / Service: Unknown]
23[Description: Telnet => Remote Login Protocol / Service: Unknown]
25[Description: SMTP => Simple Mail transfer Protocol / Service: Unknown]
79[Description: Finger / Service: Unknown]
110[Description: Pop3 => Post Office Protocol 3 / Service: Unknown]
111[Description: SunRPC => SUN Remote Procedure Call / Service: Unknown]
512[Description: Exec => Remote process execution / Service: Unknown]
513[Description: Login => Remote login (a la telnet) / Service: Unknown]
514[Description: Shell => cmd / Service: Unknown]
515[Description: printer => Printer Spooler / Service: Unknown]
540[Description: uucp / Service: Unknown]
4045[Description: lockd => NFS File Locking / Service: Unknown]
6000[Description: X server / Service: Unknown]
6112[Description: dtspcd => CDE Subprocess Control Service / Service: Unknown]
7777[Description: Oracle HTTP Server / Service: Unknown]
8080[Description: Http-Proxy / Service: Unknown]
8888[Description: AnswerBook2 / Service: Unknown]

Figura 9 – Portas abertas (servidor de aplicações) (Fonte: Autor)

SERVIDOR

IP Address	Details	Hostname	Operating System
		SERVIDOR	Windows 2000

Figura 10 – Servidor de Ficheiros (Fonte: Autor)

Vulnerabilidades de alta segurança

Servidor POP3 pode estar vulnerável a uma exploração de overflow de buffer remoto. Contém um overflow de buffer que pode resultar na sobre gravação da memória de processo, incluindo o endereço de retorno na pilha e a execução de código.

Vulnerabilidades de segurança médias

Vulnerabilidade DDE (intercâmbio dinâmico de dados de rede) - um utilizador mal-intencionado pode elevar os seus privilégios

Acesso anónimo ao FTP permitido - recomenda-se desabilitar logins anónimos.

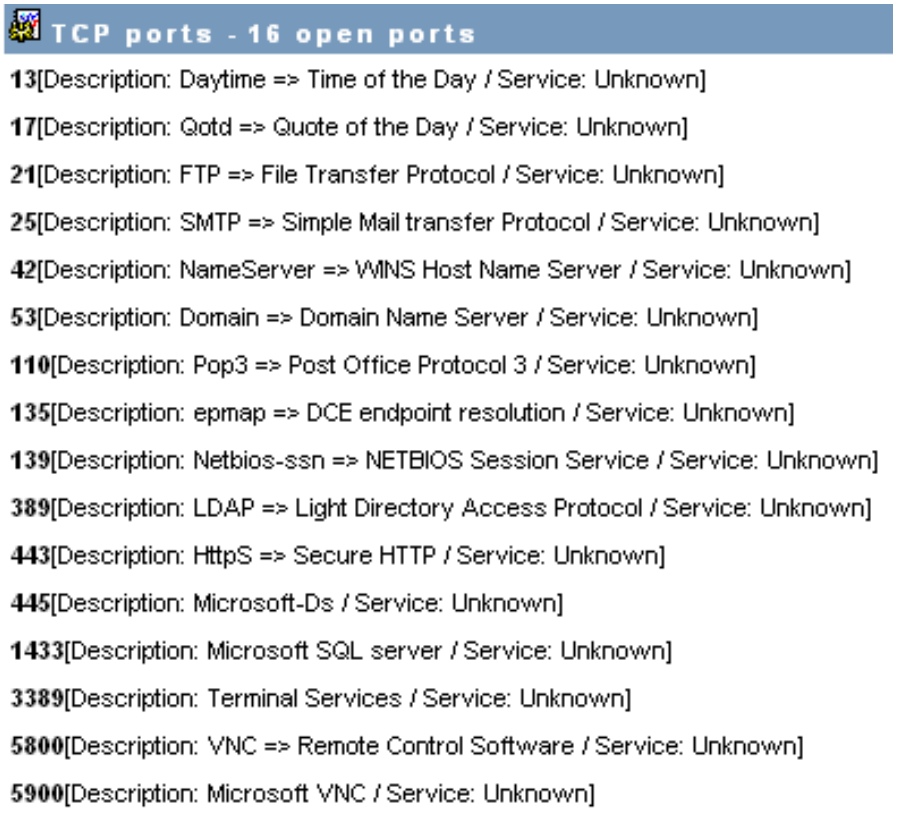

Figura 11 – Portas abertas (servidor de ficheiros) (Fonte: Autor)

SERVIDORSIG

IP Address	Details	Hostname	Operating System
		SERVIDORSIG	Windows Server 2003

Figura 12 – Servidor de SIG (Fonte: Autor)

Vulnerabilidades de alta segurança

Várias vulnerabilidades de Squid (versões anteriores do Squid 2-4 STABLE6 são vulneráveis)

Execução remota de código e / ou negação de serviço
Servidor POP3 pode estar vulnerável a uma exploração de overflow de buffer remoto

Contém um overflow de buffer que pode resultar na sobre gravação da memória de processo, incluindo o endereço de retorno na pilha e a execução de código.

TCP ports - 13 open ports

13[Description: Daytime => Time of the Day / Service: Unknown]
17[Description: Qotd => Quote of the Day / Service: Unknown]
21[Description: FTP => File Transfer Protocol / Service: Unknown]
25[Description: SMTP => Simple Mail transfer Protocol / Service: Unknown]
42[Description: NameServer => WINS Host Name Server / Service: Unknown]
53[Description: Domain => Domain Name Server / Service: Unknown]
110[Description: Pop3 => Post Office Protocol 3 / Service: Unknown]
135[Description: epmap => DCE endpoint resolution / Service: Unknown]
139[Description: Netbios-ssn => NETBIOS Session Service / Service: Unknown]
445[Description: Microsoft-Ds / Service: Unknown]
515[Description: printer => Printer Spooler / Service: Unknown]
548[Description: AFP => Apple File Share / Service: Unknown]
8080[Description: Http-Proxy / Service: Unknown]

Figura 13 – Portas abertas (servidor de SIG) (Fonte: Autor)

IP Address	Details	Hostname	Operating System
			probably Unix

Figura 14 – Servidor de MailRelay (Fonte: Autor)

Vulnerabilidades de alta segurança

Várias vulnerabilidades de Squid (versões anteriores do Squid 2-4 STABLE6 são vulneráveis)

Execução remota de código e / ou negação de serviço

Vulnerabilidade de serviço RPC.ypasswdd

O serviço RPC.ypasswdd é vulnerável a uma exploração de overflow de buffer remoto

Velho openssh

Versões antigas do openssh anteriores a 3.7.1 tinham uma vulnerabilidade que permitia às pessoas executar comandos remotamente

Vulnerabilidades de segurança médias

O servidor SSH aceita conexões da versão 1.x

A versão 1 do protocolo SSH tem várias vulnerabilidades. Isso deve ser desativado e somente os clientes da versão 2 devem ter permissão para se conectar

Alguns banners do servidor POP3 que fornecem informações ao invasor

O script exibe as informações fornecidas pelo servidor POP3. Essas informações podem ajudar um atacante a escolher o melhor vetor de ataque para o servidor.

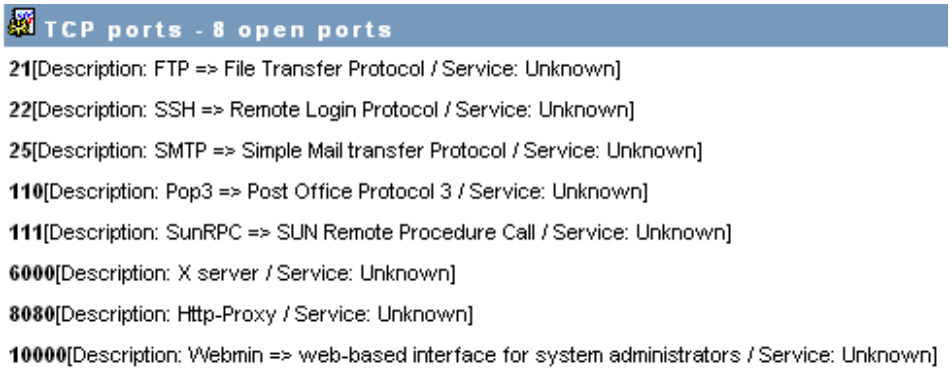

Figura 15 – Portas abertas (servidor de MailRelay) (Fonte: Autor)

MAIL

Figura 16 – Servidor de Mail (Fonte: Autor)

Vulnerabilidades de alta segurança

Várias vulnerabilidades de Squid (versões anteriores do Squid 2-4 STABLE6 são vulneráveis)

Execução remota de código e / ou negação de serviço

Possível overflow de buffer do snmpXdmid SunOS

Possível ataque de string de formato statd

Algumas versões desse serviço são vulneráveis (execute comandos arbitrários como root)

Vulnerabilidade de serviço RPC.ypasswdd

O serviço RPC.ypasswdd é vulnerável a uma exploração de overflow de buffer remoto

Vulnerabilidade de serviço RPC.ypasswdd

O serviço RPC.ypasswdd é vulnerável a uma exploração de overflow de buffer remoto

Vulnerabilidades de segurança médias

O serviço SNMP está ativado neste host

Inúmeras vulnerabilidades foram relatadas em implementações SNMP de vários fornecedores. Deve-se verificar se o sistema está vulnerável.

Servidor IMAP4 (bufferoverflow wu-imapd)

O Wu-imapd é vulnerável a uma condição de overflow de buffer. Isso foi relatado para ocorrer quando um utilizador válido solicita atributos de caixa de correio parcial. A exploração pode resultar na execução de código arbitrário.

Vulnerabilidades de segurança médias

Revelação do caminho do servidor da Web 404

Alguns servidores da Web divulgam o caminho da webroot, quando solicitados por uma página inexistente. Isso não deve ser permitido em servidores de produção.

Serviço de dedo correndo

Usando um finger server, um utilizador remoto pode obter uma ampla gama de informações sobre utilizadores, na máquina local.

O banner do servidor IMAP4 fornece informações ao invasor

O banner do servidor IMAP4 fornece informações que podem ajudar um invasor.

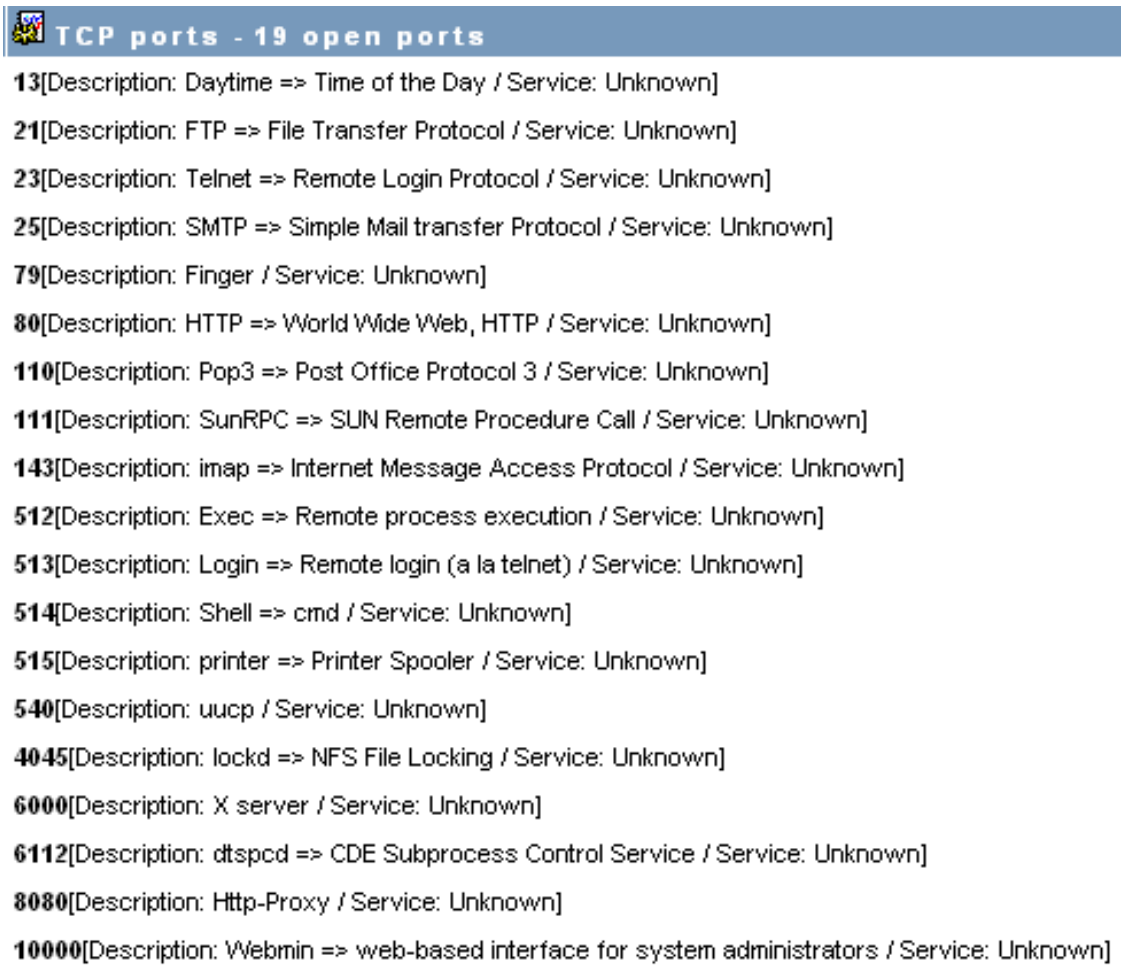

Figura 17 – Portas abertas (servidor de Mail) (Fonte: Autor)

4.2. Relatório de Vulnerabilidades – *Passwords*

Figura 18 – Passwords (vulnerabilidades) (Fonte: Autor)

Domain	User Name	LM Password	<8	Password	Password Age (days)	Audit Time
CMPF					701	0d 0h 0m 0s
CMPF					0	0d 0h 0m 0s
CMPF			x		234	0d 0h 7m 40s
CMPF					154	0d 1h 16m 10s
CMPF					782	
CMPF					782	
CMPF					782	
CMPF					782	
CMPF			x		659	
CMPF			x		647	
CMPF			x		647	
CMPF			x		647	
CMPF			x		647	
CMPF			x		642	
CMPF			x		642	
CMPF			x		638	
CMPF					740	
CMPF			x		615	
CMPF			x		609	
CMPF			x		609	
CMPF			x		609	
CMPF			x		609	
CMPF			x		609	
CMPF			x		609	
CMPF			x		609	
CMPF			x		0	
CMPF			x		537	
CMPF			x		526	
CMPF			x		523	
CMPF			x		490	
CMPF			x		490	
CMPF			x		428	
CMPF			x		321	
CMPF			x		321	
CMPF			x		321	
CMPF			x		321	
CMPF			x		321	
CMPF			x		321	
CMPF			x		295	
CMPF			x		295	
CMPF			x		295	
CMPF			x		295	

Figura 19 – N.º de dias de cada password (Fonte: Autor)

4.3. Relatório de Vulnerabilidades – IP´s Públicos

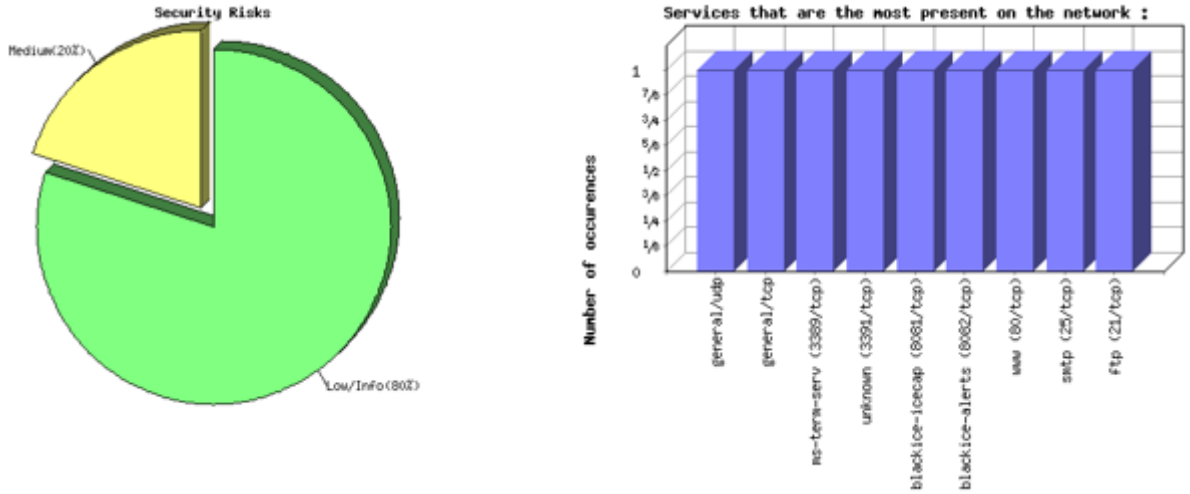

Figura 20 – Resumo das falhas no IP público (Fonte: Autor)

IP externo

Aviso encontrado na porta blackice-icecap (8081 / tcp). O servidor remoto está a executar com o WebDAV ativado. O WebDAV é uma extensão padrão da indústria para a especificação HTTP. Ele adiciona um recurso para utilizadores autorizados para adicionar e gerenciar remotamente o conteúdo de um servidor da web.

O servidor de frontpage remoto pode vazar informações sobre o utilizador anónimo, sabendo o seu nome. Ataques mais sofisticados podem ser iniciados.

Aviso encontrado na porta ms-term-serv (3389 / tcp). Os Serviços de Terminal estão habilitados no host remoto. Os serviços de terminal permitem que um utilizador do Windows obtenha remotamente um login gráfico (e, portanto, atue como um utilizador local no host remoto).

Se um invasor obtiver um login e uma senha válidos, ele poderá usar esse serviço para obter mais acesso ao host remoto. Um invasor também pode usar esse serviço para montar um ataque de dicionário contra o host remoto e, assim, tentar efetuar o login remotamente.

Observe que o RDP (Protocolo de Área de Trabalho Remota) é vulnerável a ataques Man-in-

the-middle, facilitando aos invasores o roubo das credenciais de legitimados utilizadores, personificando o servidor Windows.

O host remoto não descarta os pacotes TCP SYN que possuem o sinalizador FIN definido. Dependendo do tipo de firewall que se está a usar, o atacante pode aproveitar-se dessa falha para ignorar as suas regras.

Portas abertas

FTP (21/TCP)

SMTP (25/TCP)

WWW (80/TCP)

BLACKICE-ICECAP (8081/TCP)

BLACKICE-ALERTS (8082/TCP)

MS-TERM-SERV (3389/TCP)

(3391/TCP)

General/TCP

General/UDP

5. Recomendações

Uma vez identificados os requisitos de segurança, convém que os controlos de segurança sejam selecionados e implementados para assegurar que os riscos são reduzidos a um nível aceitável.

Pretende-se, com este documento, fornecer recomendações para a gestão da segurança da informação, aos responsáveis pela introdução, implementação ou manutenção da segurança na Câmara Municipal de Paços de Ferreira. Tem como propósito disponibilizar uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança da informação, reforçando a confiança nos relacionamentos entre as organizações.

Devem as recomendações descritas neste documento ser selecionadas e usadas de acordo com a legislação e as regulamentações vigentes.

Este documento deverá ser encarado como o ponto de partida para o desenvolvimento de recomendações específicas para a organização, que deverão contemplar o planeamento da estratégia de evolução a curto, médio e longo prazo.

Serão propostas ações de melhoria de segurança com uma indicação de criticidade e relações de interdependência entre as ações propostas.

As ações de melhoria incluirão alterações a nível organizacional, alterações de sistemas ou equipamentos e a implementação de processos de segurança, entre outros.

Deve ainda ser criado um regulamento de utilização das tecnologias de informação.

5.1. Políticas de Segurança da Informação

Disponibilizar, ao executivo, uma orientação e apoio para a segurança da informação.

Estabelecer uma política clara que demonstre apoio e compromisso com a segurança da informação, através da emissão e manutenção de uma política de segurança da informação para toda a organização.

Aprovar um documento da política de segurança, pelo executivo, publicado e comunicado, de forma adequada, a todos os colaboradores. Este deve expressar as preocupações do executivo e estabelecer os principais objetivos para a gestão da segurança da informação. No mínimo, deve incluir as seguintes orientações:

1. Definição de políticas de segurança de informação, a importância das mesmas como mecanismo que habilita a utilização e partilha de informação;

2. Declaração de compromisso do executivo, dando total apoio nos objetivos e princípios da segurança da informação;

3. Breve explanação das políticas, princípios, padrões e requisitos da conformidade de importância específica para a organização, como sendo a conformidade com a legislação e cláusulas contratuais, requisitos na educação da segurança, prevenção e deteção de vírus e *softwares* maliciosos, gestão da continuidade do negócio, e as respetivas consequências das violações na política de segurança da informação;

4. Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registo dos incidentes de segurança;

5. Referência a documentação que possa apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os utilizadores usem;

6. Comunicar esta política, através de toda a organização, a todos os colaboradores, de forma que seja relevante, acessível e compreensível para o leitor em foco.

A política de segurança da organização deverá ter um gestor específico, responsável pela sua manutenção e análise crítica, de acordo com um processo de análise crítica definida.

Este processo deverá garantir que a análise crítica ocorrerá na existência de qualquer alteração que afete a avaliação de risco original, tais como incidentes de segurança significativos, existência de novas vulnerabilidades identificadas, ou existência de alterações na infraestrutura tecnológica da organização.

Especificamente, deverão ser efetuadas periodicamente as seguintes análises críticas:

1. Qualidade da política, manifestada através do número, tipo e impacto dos incidentes de segurança registados;

2. Custo e impacto da implementação de controlos de segurança na eficiência da organização;

3. Possíveis efeitos das alterações, que poderão ser efetuadas na plataforma tecnológica da organização, na ocorrência de incidentes de segurança.

5.2. Organização da Segurança

Estabelecer uma estrutura de gestão para iniciar e controlar a implementação da segurança da informação dentro da organização.

A segurança da informação deverá ser uma responsabilidade organizacional, partilhada por todos os membros do executivo. Criar um fórum de gestão para garantir um direcionamento claro e um suporte de gestão visível dos envolvidos para as iniciativas de segurança. Deve, este fórum, promover a segurança dentro da organização através do comprometimento apropriado e dos recursos adequados. O fórum pode ser parte de um corpo diretivo existente.

Tipicamente, tal fórum é responsável pelo seguinte:

1. Análise crítica e aprovação da política da segurança da informação e das responsabilidades envolvidas;

2. Análise crítica e monitorização de incidentes de segurança da informação;

3. Aprovação das principais iniciativas para aumentar o nível da segurança da informação.

A política de segurança da informação deve fornecer um guia geral sobre a atribuição de regras e responsabilidades de segurança na organização. Deve complementar, onde for necessário, com orientações mais detalhadas para locais, sistemas ou serviços específicos. Devem ser claramente definidas as responsabilidades, em cada loca,l para os ativos físicos e de informação, bem como dos processos de segurança, como, por exemplo, o plano de continuidade de negócios.

Em muitas organizações, um gestor de segurança da informação terá toda a responsabilidade pelo desenvolvimento e implementação da segurança e pelo suporte à identificação dos controles. Contudo, a responsabilidade pela alocação de recursos e pela implementação dos controlos permanece, geralmente, com os gestores. Uma prática comum é indicar um proprietário para cada ativo de informação, tornando-o responsável pela sua segurança no dia a dia.

Consultoria especializada em segurança é normalmente requerida em diversas organizações. Em condições ideais, deverá existir um consultor de segurança da informação, interno e com um nível de experiência elevado. No entanto, nem todas as organizações podem ter nos seus quadros um consultor especialista de segurança.

Nestes casos, é recomendável que seja identificado um colaborador específico para coordenar o conhecimento interno, de forma a garantir a consistência necessária, fornecendo auxílio nas decisões a tomar sobre questões de segurança da informação.

Nestes casos, deverá haver a requisição periódica de consultores externos, com a finalidade de ser realizada uma consultoria de segurança especializada, através de pessoas com vasta experiência na área.

Os mesmos estão incumbidos de fornecer apoio em todos os aspetos relacionados com a segurança da informação, assim como a passagem de conhecimentos obtidos da experiência das auditorias de segurança realizadas diariamente por este tipo de especialistas.

As qualidades das suas avaliações, das ameaças à segurança e os trabalhos de consultoria no aconselhamento da implementação de controlos de segurança determinarão a eficiência da segurança da informação da organização.

A informação considerada como crítica para a organização pode ser colocada em risco, através do acesso de prestadores de serviços (externos), através de uma gestão adequada de segurança.

Quando é considerada a necessidade de ligações de prestadores de serviços à plataforma tecnológica corporativa, deverá ser realizada uma avaliação de risco, para, através dela, serem identificadas quaisquer necessidades de implementação de controlos de segurança a fim de garantir a salvaguarda da informação corporativa.

Para tal, deverão ser tidos em conta fatores como o tipo de acesso requerido, o valor da informação, os controlos de segurança implementados, a forma como os prestadores de serviços realizam o referido acesso e as implicações deste acesso na segurança da informação da organização.

Estes acessos à informação e aos recursos da informação corporativa não devem ser autorizados até que os controlos apropriados sejam implementados, assim como a definição de um contrato entre ambas as partes, que defina os termos do acesso, referentes à segurança da informação.

5.3. Classificação e Controlo dos Recursos de Informação

Manter a proteção adequada aos ativos da organização e assegurar que recebem um nível de proteção adequado.

Controlar todos os recursos da informação da organização, devendo ter um utilizador responsável.

A realização do inventariado dos recursos assegura que a proteção está a ser realizada de forma adequada. Identificar os utilizadores e que a estes seja atribuída a responsabilidade pela manutenção apropriada.

Exemplos de recursos associados aos sistemas de informação que deverão ser identificados:

Recursos de informação: arquivos e bases de dados, documentação dos sistemas, manuais de utilizador, procedimentos de suporte e operação, planos de contingência, informações armazenadas;

Recursos de *Software*: aplicações, sistemas, ferramentas de desenvolvimento e utilitários;

Recursos físicos: computadores, monitores, equipamentos de comunicações (router, fax, switch, etc), dispositivos magnéticos de *backup,* outros equipamentos técnicos, mobília;

A informação possui diversos níveis de criticidade e sensibilidade. Alguns itens poderão necessitar de um nível adicional de proteção ou de um tratamento especial.

A classificação da informação deve ter em consideração as necessidades do negócio, para partilha ou restrição da informação, e os respetivos impactos, como, por exemplo, o acesso não autorizado e a perda de informação. Geralmente, a classificação que é dada à

informação é o método mais rápido para determinar a forma como a mesma é tratada e protegida.

Tomar cuidados adequados à quantidade de categorias da classificação e aos benefícios obtidos com o seu uso. Esquemas excessivamente complexos podem tornar a sua utilização incómoda, complexa e economicamente inviável.

É importante que um conjunto apropriado de procedimentos seja definido para classificar e tratar a informação, de acordo com o esquema de classificação adotado pela organização.

5.4. Segurança da Informação vs. Recursos Humanos

Reduzir os riscos relacionados com o erro humano, roubo, burla ou uso indevido das instalações.

As regras e responsabilidades de segurança devem ser documentadas onde for apropriado, de acordo com a política de segurança da informação da organização. As mesmas devem incluir quaisquer responsabilidades gerais pela implementação ou manutenção da política de segurança da organização, assim como qualquer responsabilidade específica para a proteção de determinados recursos da informação, ou pela execução de determinados processos ou atividades relacionadas com a segurança da informação.

Quando o trabalho envolver pessoas externas, sejam elas abrangidas por um contrato de trabalho ou qualquer outro tipo de acordo, e as mesmas tenham acesso às instalações de processamento da informação, em particular aquelas que tratam de informações consideradas como críticas para a organização (tais como, informações financeiras ou informações altamente confidenciais), a organização deve fazer uma verificação da idoneidade de crédito. Em particular, para funcionários que estão em posições com níveis consideráveis de autoridade, este procedimento deve ser realizado periodicamente.

Geralmente, a utilização de acordos de confidencialidade ou de não divulgação alerta que a informação é confidencial ou secreta. Normalmente, os funcionários deveriam assinar tais acordos como parte dos termos e condições iniciais de contratação.

Para colaboradores temporários e prestadores de serviços que não estejam cobertos pela existência de um contrato de trabalho (que contenha o acordo de confidencialidade), há que exigir a assinatura do acordo de confidencialidade antes do mesmo ter acesso às instalações da plataforma tecnológica da informação da organização.

Este acordo de confidencialidade tem que ser revisto quando existirem modificações nos termos de contratação, em particular quando existe a saída de funcionários da organização ou quando termina o contrato de trabalho existente.

Os termos e condições de trabalho determinam as responsabilidades dos funcionários pela segurança da informação. Sempre que se justificar e for apropriado, estas responsabilidades devem continuar por um período de tempo definido, após o término do

contrato de trabalho. De igual forma, é conveniente que possíveis ações, que possam ser tomadas nos casos de desrespeito ao acordo, também sejam incluídas no contrato.

Formação contínua dos utilizadores

Todos os funcionários e colaboradores da organização e, quando se justificar e for relevante, prestadores de serviços receberão formação apropriada, sendo regularmente informados sobre as políticas e procedimentos de segurança da organização. Isto incluirá requisitos de segurança, responsabilidades legais e controlos do negócio, assim como formação sobre o uso correto das instalações onde se localiza a plataforma tecnológica da organização, como, por exemplo, procedimentos de acesso ou utilização correta dos sistemas e aplicações, antes que seja fornecido qualquer acesso aos serviços ou informação corporativos.

5.5. Segurança Física e Ambiental

Prevenir acessos não autorizados, deterioração e interferências nas informações e instalações físicas da organização.

Perímetro de segurança física

Devem as seguintes diretrizes e controlos ser consideradas e implementadas em locais apropriados da organização.

1. O perímetro de segurança seja claramente definido, e fisicamente consistente;

2. A utilização correta e adequada de barreiras físicas, ou outro meio de controlo de acesso físico e lógico, em todas as áreas das instalações, que previnam o acesso não autorizado, ou contaminações do ambiente, como as causadas pelo fogo e inundações;

3. A utilização de portas com características de corta-fogo no perímetro de segurança das instalações onde se localizam os sistemas da plataforma tecnológica da organização, e que as mesmas possuam sensores de alarme, e dispositivos de encerramento automático, de forma a garantir a proibição dos acessos não autorizados e a integridade da segurança das instalações.

Controlo de entrada física

As áreas de segurança da organização devem estar protegidas por controlos de entrada apropriados, para se assegurar que apenas pessoas autorizadas tenham acesso às instalações. Para tal, recomenda-se que os seguintes controles sejam considerados:

1. Devem ser confirmadas as permissões de acesso dos visitantes às áreas de segurança da organização, assim como o registo da hora de entrada e saída do mesmo nas instalações;

2. O acesso às informações restritas, às instalações e aos recursos da plataforma tecnológica deve ser controlado, registado e restrito apenas a pessoal autorizado;

3. Recomenda-se a todos os colaboradores o uso de identificação visível, como, por exemplo, cartões identificativos (badges), e que sejam utilizados para autorizar e validar qualquer tipo de acesso físico às instalações;

4. Os direitos de acesso às áreas de segurança têm que ser periodicamente revistos e atualizados;

5. Deverão ser implementadas medidas e processos formais de auditoria ao controlo de acessos.

Instalação e proteção de sistemas críticos

1. As instalações da plataforma tecnológica de servidores devem estar localizadas adequadamente, de modo a reduzir riscos de intrusão e espionagem durante o seu uso;

2. Devem ser adotados diversos procedimentos de forma a minimizar potenciais ameaças, como roubo, incêndios, inundações, radiação eletromagnética ou interferência no fornecimento de energia elétrica;

3. Monitorizar e avaliar os aspetos relacionados com o ambiente das instalações para sejam evitadas condições que possam afetar, de forma adversa, as instalações de processamento da informação.

4. Devem ser considerados os impactos de um desastre, caso ocorra nas proximidades das instalações, como, por exemplo, incêndios, inundações ou explosões nas imediações;

Fornecimento de energia elétrica

A continuação da utilização de sistemas de fornecimento de energia contínuos, em sistemas críticos para a organização, é de todo recomendada. Desta forma, consegue-se garantir a continuidade dos serviços e, caso seja necessário, o encerramento correto dos sistemas presentes na totalidade da plataforma tecnológica da organização.

Os planos de contingência deverão contemplar os procedimentos a serem realizados, no caso de falhas neste tipo de sistemas de fornecimento de energia elétrica. Da mesma forma, este tipo de equipamento deverá continuar a ser verificado periodicamente para que seja garantida a capacidade adequada e testada, de acordo com as recomendações do fabricante.

Adicionalmente, deverão estar instalados interruptores elétricos de emergência, localizados próximo das saídas de emergência das salas de equipamentos. A iluminação de emergência deverá estar disponível para a eventualidade de uma falha da energia elétrica primária. Finalmente, deverão estar implementadas, no edifício, proteções contradescargas elétricas atmosféricas.

Segurança da cablagem de comunicações

A cablagem elétrica e de comunicações, que transmite dados ou suporta os serviços de informação, tem que ser protegida contra interceção ou deterioração. Assim, recomenda-se o seguinte:

1. Os cabos elétricos e de comunicações das instalações devem ser subterrâneos, onde for possível, ou devem ser submetidos a proteções alternativas adequadas, como se verificou existirem nas instalações;
2. Os cabos de rede devem estar protegidos contra interceções não autorizadas ou fatores que causem desgaste, através do uso de calhas adequadas e evitando a sua passagem através de áreas públicas;

3. Os cabos elétricos deverão estar separados dos cabos de comunicações para que sejam prevenidas interferências eletromagnéticas;

4. Para os sistemas críticos, deverão ser implementados alguns procedimentos adicionais, como uso de cabos de fibra ótica, identificação de dispositivos não autorizados ligados à cablagem e uso de meios de transmissão alternativos.

Manutenção de Sistemas Críticos

Considerar a manutenção correta dos sistemas críticos, que garanta a disponibilidade, a continuidade e a integridade dos mesmos. Para isso, devem ter-se em conta os seguintes pontos:

1. Realização de manutenções e auditorias aos sistemas, com uma periodicidade e especificações recomendadas pelo fabricante;

2. Apenas pessoal autorizado e habilitado deve executar a manutenção, as reparações e os serviços nos equipamentos;

3. Registação de todas as falhas suspeitas ocorridas e de toda a manutenção preventiva;

4. Execução de procedimentos formais de controlos apropriados, quando os equipamentos forem enviados para manutenção ou reparação, fora das instalações físicas da organização;

A informação dos sistemas críticos pode ser exposta pelo descuido na alienação de equipamentos. Convém que os dispositivos de armazenamento de informação sensível sejam avaliados para se assegurar que toda a informação foi removida ou sobreposta de uma forma segura.

5.6. Gestão de Operações e Comunicações

Garantir a utilização segura e correta dos recursos da informação.

Procedimentos e responsabilidades operacionais

Os procedimentos de utilização identificados pela política de segurança devem ser documentados e mantidos atualizados. Estes procedimentos deverão ser tratados como documentos formais e as possíveis alterações devem ser autorizadas pelo executivo.

As alterações efetuadas nos sistemas e recursos de informação têm que ser corretamente controladas. O controlo inadequado das referidas alterações é a principal causa de falha de segurança nos sistemas. Deste modo, deverá existir uma formalização dos procedimentos e responsabilidades a implementar, de forma a garantir um controlo satisfatório de todas as alterações de equipamentos, aplicações, sistemas e dos próprios procedimentos.

Planeamento e aceitação dos sistemas

As exigências relacionadas com a capacidade dos sistemas deverão ser monitorizadas, assim como as exigências futuras, de forma a garantir a disponibilidade da capacidade adequada de processamento e armazenamento.

Estas repercussões deverão ter em consideração os requisitos de novas aplicações e sistemas e as tendências atuais e futuras do processamento de informação da organização.

Convém que os responsáveis utilizem estas informações para identificar e evitar potenciais restrições que possam representar ameaças à segurança do sistema ou aos serviços dos utilizadores, devendo planear uma ação apropriada para que tal seja evitado.

Deverão ser estabelecidos critérios de aceitação de novos sistemas, atualizações e novas versões de aplicações e sistemas, assim como deverão ser efetuados os testes apropriados dos sistemas antes da sua aceitação. Convém que os responsáveis garantam que os requisitos e critérios para aceitação de novos sistemas estejam claramente definidos, acordados, documentados e testados, de acordo com a política de segurança da organização.

Proteção contra software malicioso

Deverão ser implementados controlos de segurança contra software malicioso, como, de resto, se verifica na organização, assim como procedimentos para a devida consciencialização dos utilizadores. Esta proteção deverá ser baseada na consciencialização da segurança na organização, num adequado controlo de acessos, assim como nos mecanismos de gestão de alterações efetuadas.

Deverão ser implementados os seguintes controlos de segurança:

1. Implementação de uma política formal, exigindo conformidade com as licenças de utilização do software e proibindo o uso de software não autorizado na organização;

2. Implementação de uma política formal para proteção contra os riscos associados com a importação de arquivos e software, seja de redes externas ou de qualquer outro meio, indicando quais as medidas preventivas que devem ser adotadas;

3. Realização de análises críticas periódicas de aplicações e dos dados dos sistemas que suportam processos críticos do negócio. A presença de qualquer arquivo ou atualização não autorizada deverá ser alvo de uma investigação formal;

4. Verificação, antes da sua utilização, da existência de vírus em qualquer arquivo de origem desconhecida ou não autorizada e em qualquer arquivo recebido a partir de redes não confiáveis;

5. Existência de planos de contingência adequados para a recuperação de sistemas, em caso de ataques de vírus, incluindo os procedimentos necessários para salvaguardar e recuperar os dados considerados críticos;

6. Implementação de procedimentos para a verificação de toda a informação relacionada com software malicioso, assim como a garantia de que os alertas sejam precisos e informativos.

Cópias de segurança

Cópias de segurança dos dados e de software essenciais ao negócio deverão continuar a ser feitos regularmente. Deverão, também, ser disponibilizados recursos e instalações alternativos, de forma a garantir que todos os dados e sistemas aplicativos essenciais ao negócio possam ser recuperados após um desastre ou problemas em dispositivos de *backup*. Os mesmos deverão ser testados regularmente, de forma integral, de maneira a garantir a satisfação dos requisitos dos planos da continuidade do negócio.

Registo de Operações

Deverá ser mantido um registo atualizado das atividades do pessoal das operações. Esse registo deverá incluir, conforme se justifique e seja apropriado, os seguintes pontos:

1. Horário de início e fim das intervenções;

2. Erros e ações de correção adotadas;

3. Confirmação do uso correto das bases de dados e dos resultados gerados na intervenção;

4. Identificação da pessoa que realiza a intervenção;

Qualquer tipo de falha que seja detetada deverá ser reportado aos responsáveis pelos sistemas, a fim de serem implementadas medidas de correção.

Deverão existir regras claras para o tratamento das falhas de informação, como:

1. Análise crítica sobre os registos de falhas para que seja assegurado que estas foram satisfatoriamente resolvidas;

2. Análise crítica sobre as medidas de correção aplicadas para assegurar que as mesmas não tenham comprometido os controlos de segurança e que as ações adotadas tenham sido devidamente autorizadas.

Gestão da rede corporativa

É necessária a utilização de um conjunto de controlos, de forma a obter e a preservar a segurança na rede corporativa da organização. Daí a necessidade de implementar controlos para garantir a segurança de dados nas redes, assim como a proteção dos serviços disponibilizados contra acessos não autorizados.

Correio Eletrónico

O correio eletrónico surge nas comunicações comerciais, substituindo os meios tradicionais, como faxes e cartas. Recorrendo a este meio de comunicação, foi incrementada a velocidade de comunicações, alterada a estrutura das mensagens, o grau de formalidade e as ações não autorizadas. Atendendo a este fator, é de todo necessário que sejam considerados certos cuidados e controlos para se reduzirem os riscos associados com a utilização deste meio de comunicação, que incluem:

1. Vulnerabilidades de acessos não autorizados, modificação ou negação do serviço *(denial of service);*

2. Vulnerabilidades associados à falta e confiabilidade e disponibilidade do serviço;

3. Considerações legais relacionadas com a necessidade potencial de prova de origem, envio, entrega e aceitação;
4. Implicações da divulgação externa de listas de colaboradores.

É necessário criar uma regra formal e clara, de acordo com a política de segurança presente na organização, para a utilização do correio eletrónico, incluindo:

1. Proteção adequada para se evitarem ataques de vírus e interceção da mensagem;

2. Proteção de anexos enviados por correio eletrónico;

3. Orientação e instrução relativamente às situações em que se deve, ou não, utilizar o correio eletrónico;

4. Responsabilização das pessoas, de modo que não sejam enviadas mensagens difamatórias de forma a comprometer a organização, ou a utilizar o correio eletrónico corporativo para fazerem compras não autorizadas, ou outro tipo de serviço;

5. Uso de técnicas de encriptação das mensagens para que seja salvaguardada a confidencialidade e a integridade das mensagens;

6. Uso de assinaturas e certificados digitais;

7. Retenção de mensagens enviadas e recebidas.

5.7. Controlo de Acessos

Controlar o acesso à informação e prevenir acessos não autorizados aos sistemas de informação.

Controlar o acesso à informação e processos organizacionais, na base de requisitos de segurança e do negócio. Ter em consideração as políticas de autorização e dispersão da informação.

Requisitos de negócio e política

Os requisitos do negócio, para controlo de acessos, devem ser definidos e documentados. De igual modo, as regras de controlo de acessos e direitos para cada utilizador ou grupo de utilizadores devem estar claramente estabelecidas no documento de controlo de acessos, presente na política de segurança corporativa. Deve, também, ser dado, aos utilizadores e prestadores de serviços, um documento contendo claramente os controlos de acessos que satisfaçam os requisitos do negócio.

Recomenda-se que a política tenha em consideração os seguintes fatores:

1. Requisitos de segurança de aplicações específicas de negócio;

2. Identificação de toda a informação referente às aplicações do negócio;

3. Políticas de autorização e distribuição de informação, como é o caso da necessidade de conhecer os princípios e níveis de segurança, bem como a classificação da informação;

4. Compatibilidade entre o controlo de acessos e as políticas de classificação da informação dos diferentes sistemas e redes;

5. Legislação vigente e qualquer obrigação contratual considerando a proteção do acesso a dados ou serviços;

6. Perfil de acesso de utilizador padrão para categorias de trabalho comuns;

7. Gestão dos direitos de acesso em todos os tipos de ligações disponíveis num ambiente distribuído e ligado numa rede corporativa;

Regras de controlo de Acessos

Alguns cuidados na especificação de regras de controlo de acessos:

1. Diferenciação entre as regras que sempre devem ser cumpridas das regras opcionais ou condicionais;

2. Estabelecimento de regras baseadas na premissa “Tudo deve ser proibido a menos que expressamente permitido “, ao invés da regra “Tudo é permitido a menos que expressamente proibido”;
3. Modificações nos rótulos de informação que são atribuídos automaticamente pelos recursos de processamento de dados e dos atribuídos a critério de um utilizador;

4. Modificações nas permissões dos utilizadores que são atribuídas automaticamente por um sistema de informação daquelas atribuídas por um administrador;

Diferenciação entre regras que requerem aprovação.

Gestão de acessos do utilizador

Estabelecer procedimentos para controlar a concessão de permissões de acesso aos sistemas de informação e serviços. Estes procedimentos devem cobrir todas as etapas do ciclo de vida de acesso de um utilizador, desde o registo inicial de novos utilizadores até ao registo final de exclusão dos utilizadores que deixem de ter necessidade de ter acesso aos sistemas de informação e serviços. Dar especial atenção, quando apropriado, à necessidade de controlar a concessão de permissões de acesso privilegiado, os quais permitem aos utilizadores sobrepor os controlos do sistema.

Controlar o acesso aos serviços de informação através de um processo formal de registo de utilizador, com os seguintes requisitos:

1. Utilização de identificador de utilizador (ID) único, de forma a que cada utilizador possa ser identificado e feito responsável pelas suas ações;

2. Diferenciação entre as regras que sempre devem ser cumpridas das regras opcionais ou condicionais;

3. Verificação da adequação do nível de acesso concedido aos propósitos do negócio e a sua consistência com a política de segurança da organização;

4. Entrega de um documento escrito aos utilizadores sobre os seus direitos de acesso;

5. Solicitação da assinatura dos utilizadores no anterior documento, indicando que eles entenderam as condições de seus direitos de acesso;

6. Manutenção de um registo formal de todas as pessoas registadas que usem o serviço;

7. Remoção imediata dos direitos de acesso dos utilizadores que tenham mudado de função ou saído da organização;

8. Verificação periódica para remoção de utilizadores e contas redundantes.

5.8. Gestão de privilégios

Deve ser restrita e controlada a concessão e a utilização de privilégios. O uso inadequado de privilégios em sistemas é frequentemente apontado como o maior fator de vulnerabilidade de sistemas.

Os sistemas com mais de um utilizador, que necessitam de proteção contra acesso não autorizado, devem ter a concessão de privilégios controlada através de um processo de autorização formal. Devem ser seguidos os seguintes passos:

1. Conceder privilégios a indivíduos conforme a necessidade de uso ou determinação por eventos. Por exemplo, os requisitos mínimos para a sua função somente quando necessário;

2. Um processo de autorização e um registo de todos os privilégios concedidos devem ser mantidos;

3. Não fornecer os privilégios até que todo o processo de autorização esteja finalizado;

Gestão de palavras-passe dos utilizadores

As palavras-passe são um meio comum de validação da identidade de um utilizador para obtenção de acessos a um sistema de informação ou serviço. A concessão de palavras-passe tem que ser controlada através de um processo de gestão formal, tendo em considerção o seguinte:

1. Solicitar aos utilizadores a assinatura de uma declaração, a fim de manter a confidencialidade de sua palavra-passe e de grupos de trabalho;

2. Garantir que os utilizadores mantêm as suas próprias palavras-passe, sendo inicialmente fornecidas com cariz seguro e temporário, o que os obriga a alterá-las imediatamente. O fornecimento de palavras-passe temporárias, no caso dos utilizadores se esquecerem da sua, deve ser efetuado unicamente após a sua identificação positiva;

3. Requerer que palavras-passe temporárias sejam dadas aos utilizadores de forma segura. O uso de mensagens de correio eletrónico desprotegidas deve ser evitado. Os utilizadores têm que confirmar a receção das mesmas.

Não devem ser guardadas as palavras-passe no computador de forma desprotegida. Há outras tecnologias para a identificação e autenticação de utilizadores, tais como reconhecimento biométrico, através da verificação de impressão digital.

Os utilizadores têm que estar alertados para o facto de:

1. Manter a confidencialidade das palavras-passe;

2. Evitar o registo em papel, a menos que possa ser guardado de forma segura;

3. Alterar a palavra-passe sempre que existir qualquer indicação de possível comprometimento do sistema;

4. Selecionar palavras-passe de qualidade, com um mínimo de 6 a 8 caracteres, que sejam fáceis de lembrar, não baseadas em algo que outras pessoas possam facilmente adivinhar ou obter a partir de informações pessoais, isentas de caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos;

5. Alterar a palavra-passe em intervalos regulares.

5.9. Desenvolvimento e Manutenção da Segurança de Sistemas

Requisitos de segurança de sistemas

Na especificação dos requisitos do negócio para novos sistemas, ou melhoria nos sistemas já existentes, especificar os requisitos de controlo de segurança. Nestas especificações, considerar os controlos automatizados a serem incorporados no sistema e a necessidade de suporte a controlos manuais.

Refletir o valor para o negócio, dos requisitos e controlos de segurança, dos recursos de informação envolvidos e o potencial impacto que pode resultar da falha ou ausência de segurança. A estrutura para analisar os requisitos e segurança e identificar os controlos que os satisfazem está presente na avaliação e gestão de riscos de segurança.

Controlos de segurança adicionais podem ser necessários para sistemas que processam ou têm impacto em recursos organizacionais considerados críticos, valiosos ou sensíveis para a organização. Estes controlos devem ser determinados na base dos requisitos de segurança e na avaliação de riscos.

Controlos de criptografia

A codificação é uma técnica criptográfica que pode ser usada para proteger a confidencialidade da informação.

Técnicas e sistemas criptográficos deverão ser implementados para a proteção das informações que são consideradas de risco e para as quais outros controlos de segurança não fornecem a proteção adequada.

É necessário desenvolver uma política formal para a utilização de controlos de criptografia a fim de proteger a informação corporativa. Tal política é necessária para maximizar os benefícios e minimizar os riscos da utilização das técnicas criptográficas, assim como evitar o uso impróprio ou incorreto.

As assinaturas digitais fornecem os meios para proteção da autenticidade e integridade de documentos eletrónicos.

A sua utilização é aconselhada em casos em que existe a necessidade de verificação de quem assinou o documento eletrónico, averiguando se o seu conteúdo foi modificado.

5.10. Gestão de Incidentes de Segurança da Informação

Minimizar danos originados pelos incidentes de segurança e pelo mau funcionamento, assim como monitorizar e aprender com os mesmos.

Notificação dos incidentes de segurança

Deve a organização estabelecer um procedimento de notificação formal, assim como um procedimento de resposta ao referido incidente de segurança, estabelecendo a ação correta a ser tomada ao se receber uma notificação do incidente.

Todos os colaboradores internos e prestadores de serviço têm que estar conscientes dos procedimentos para notificação de incidentes de segurança e devem ser instruídos para comunicar tais incidentes, da forma mais rápida.

É necessário implementar os processos de retorno (*feedback*) adequados para assegurar que os incidentes estão notificados com os resultados obtidos após ser tratado e fechado. Estes incidentes podem ser utilizados na formação de consciencialização dos utilizadores, como exemplos do que pode acontecer, como reagir a tais incidentes e como evitá-los no futuro.

Notificação de falhas de segurança

Todos os utilizadores devem registar e notificar qualquer fragilidade ou ameaça que tenha ocorrido, ou que seja suspeita, na segurança de sistemas ou serviços.

Devem efetuar essas notificações, o mais rapidamente possível, para os seus superiores ou então, diretamente, para os responsáveis dos sistemas de informação. Todos os utilizadores deverão ser informados de que não podem, em nenhuma circunstância, tentar indagar uma fragilidade suspeita. Isto acontece para a sua própria proteção, pois a

investigação de uma fragilidade pode ser interpretada como potencial uso impróprio do sistema.

Deverão estar implementados mecanismos que permitam que tipos, quantidades e custos dos incidentes e do funcionamento incorreto sejam quantificados e monitorizados. Esta informação deverá ser utilizada para se identificarem os incidentes ou funcionamentos incorretos de alto impacto.

Isto pode indicar a necessidade da implementação de melhorias ou de controlos de segurança adicionais para limitar a sua ocorrência, assim como os custos relacionados com futuras ocorrências.

Processos disciplinares

Deverão ser instituídos processos disciplinares formais para os funcionários que tenham violado as políticas e procedimentos de segurança em vigor na organização.

A existência de tais processos poderá dissuadir os colaboradores que, de outra forma, seriam inclinados a desrespeitar os procedimentos de segurança.

Adicionalmente, deve ser assegurado um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança, sérias ou persistentes.

É necessário definir as responsabilidades e procedimentos de gestão de incidentes para garantir uma resposta rápida, efetiva e ordenada aos incidentes de segurança.

5.11. Gestão da continuidade de negócio

Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra falhas ou desastres.

Implementar um processo de gestão da continuidade de negócio para reduzir, para um nível aceitável, a interrupção causada por desastres ou falhas de segurança, através de ações de prevenção e recuperação.

Embora a possibilidade de ocorrência de catástrofes seja diminuta, deverá existir um planeamento para possíveis eventualidades.

É de extrema importância que as consequências resultantes de desastres, falhas de segurança e perdas de serviços sejam analisadas detalhadamente. Para tal, recomenda-se que os planos de contingência sejam desenvolvidos e implementados, para garantir que os processos de negócio possam ser recuperados num período útil de tempo requerido.

É importante que tais planos sejam mantidos e testados, de forma a se tornarem parte integrante de todos os processos organizacionais. É de igual importância que a gestão da continuidade de negócio inclua controlos para identificar a redução de riscos, a limitação das consequências dos estragos do incidente e a garantia de recuperação oportuna dos recursos vitais.

A continuidade do negócio deve ter como ponto de partida a identificação dos eventos que possam causar interrupções nos seus processos, por exemplo, falha de equipamentos, inundações e incêndios.

De seguida, deve-se efetuar uma avaliação de risco para a determinação do impacto destas interrupções (tanto em termos de escala de estragos como em relação ao período de restauro).

Estas atividades devem ser executadas com o total envolvimento dos responsáveis pelos processos e recursos do negócio. A avaliação deve considerar todos os processos do negócio e não deve estar limitada aos recursos e instalações da plataforma tecnológica dos serviços de informação. Em função dos resultados da avaliação de risco, deve-se desenvolver um plano estratégico para se determinar a abordagem mais abrangente a ser adotada para a continuidade do negócio. Uma vez criado, o plano deverá ser validado pelo executivo.

6. Situação atual

Após uma análise ao sistema existente na Câmara de Paços de Ferreira, verificou-se, conforme descrito anteriormente, que havia bastantes falhas ao nível da segurança interna e externa.

Foram, então, colmatadas todas as falhas verificadas, ou seja, todos os servidores foram migrados para o DataCenter do Vale do Sousa Digital, ao qual nós pertencemos, tendo uma parte nossa nesse DataCenter,

Foi criado um domínio corporativo e foram implementadas regras de segurança e de acessos, nomeadamente à Internet. Cada utilizador apenas tem acesso aos seus dados. Existe um servidor de dados onde todos armazenam os seus ficheiros. Nesse mesmo servidor existe uma drive onde estão pastas partilhadas para os diversos serviços.

Nas máquinas dos utilizadores, instalou-se o antivírus Panda, que permite uma maior segurança dos dados e emails, principalmente vindos do exterior.

E para dar cumprimento legal ao Regime Jurídico da Segurança do Ciberespaço, no que concerne aos requisitos exigidos pelo DL 65/2021 de 30 de julho, implementaram-se várias alterações, que se descrevem a seguir.

Gestão de identidades, autenticação e controlo de acessos:

O ciclo de vida de gestão de identidades está definido:

- Sistema de informação para a gestão de identidades e acessos;
- Diretório central de utilizadores e grupos;
- Serviços de autenticação.

Existem os seguintes controlos de acesso físico às redes e sistemas de informação:

- Barreiras de acesso através da utilização de torniquetes e/ou portas de segurança, restringindo assim as áreas reservadas;
- Registo de entradas e saídas.

Existem controlos aos acessos remotos através de:

- Gestão de identidades e acessos;

- Diretório de utilizadores e grupos;
- Serviços de autenticação;
- Solução tecnológica para acesso remoto.

Aplicação dos princípios do menor privilégio e da segregação de funções:

- Gestão do Ciclo de Vida de Identidades e Acessos.

Agora, existe proteção da integridade das redes de comunicação:

- Utilização de *Firewalls* (*cluster*) em Alta disponibilidade, com políticas de segurança e funcionalidades que permitem a segurança desde *layer* 4 a *layer* 8.
- Configuradas redes de comunicação reservadas com perfis específicos (gestão, DMZ, Internet, Intranet, entre outras).

A identificação dos colaboradores é verificada e revista e as suas credenciais são confirmadas interactivamente, quando necessário:

- Gestão de Identidades e Acessos.

São definidos os devidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação, através:

- da Gestão de Identidades e Acessos;
- do Diretório de Utilizadores e grupos;
- de Serviços de Autenticação;

Formação e sensibilização

Foram ministradas várias formações, ao longo do ano de 2022, no que respeita à segurança da informação, nas quais os colaboradores, com acessos privilegiados às redes e sistemas de informação da organização, são devidamente consciencializados sobre as suas funções. Tal também se aplica à gestão de topo. Foram, também, realizadas formações a partes interessadas externas, por forma a que as mesmas também compreendam quais os seus papéis e responsabilidades na organização. Além disso, são divulgados comunicados por email de informação de segurança, de forma a alertar os colaboradores de novos vetores de ataque e precauções a ter na utilização dos serviços da organização, como o email, internet, *cloud*.

Segurança de dados

É dever das redes e sistemas de informação proteger a confidencialidade e integridade da informação armazenada na organização. Para cumprimento desse dever, contribuem:

- A tecnologia e as funcionalidades para encriptação de ficheiros, bases de dados e cópias de segurança;
- A validação criptográfica dos dados que são armazenados.

Procede-se, ainda, à proteção da integridade e confidencialidade da informação transmitida (aplicável quer a redes de comunicações internas, quer externas), através de:

- ✓ Serviços de cifra de comunicações.

A organização garante a existência de procedimentos de autorização, monitorização, registo e controlo dos dados de redes e sistemas de informação, bem como dos componentes que entram e saem das suas instalações.

A organização monitoriza a capacidade das redes e dos sistemas de informação, em que são efetuadas previsões sobre as necessidades de capacidades futuras, por forma a garantir que a performance dos sistemas está alinhada com os requisitos de prestação de serviços críticos, bem como com novas funcionalidades de que a organização vai necessitando ao longo do tempo.

Para tal, procede-se à:

- ✓ Monitorização de métricas e histórico de capacidade dos recursos informáticos;
- ✓ Implementação de redundância nas redes e sistemas de informação que suportam os serviços críticos da organização.

A organização utiliza os mecanismos de verificação necessários para confirmar a integridade de *software*, *firmware* e dados. Para isso, efetua a separação dos ambientes das suas redes e dos seus sistemas de informação, de forma física e/ou lógica, de acordo com as suas funções. Para isso, tem:

- ✓ Zonas de segurança de redes de comunicações;
- ✓ Segregação física ou lógica de ambientes;

A organização implementa os devidos mecanismos de validação e verificação de integridade do hardware, promovendo as devidas validações periódicas pelo fabricante ou pelo devido fornecedor certificado.

Princípios e procedimentos de proteção da informação

A organização tem a configuração base necessária para as suas redes e sistemas de informação, para os seus componentes e para as suas comunicações e conetividades.

Para esclarecer em que consiste a base necessária da organização, possuímos:

- Programas informáticos instalados em estações de trabalho;

- Equipamentos pessoais (computadores portáteis, impressoras e outros dispositivos móveis);

- Servidores e elementos de rede;

- Versões e atualizações aplicadas a sistemas operativos e aplicações, configurações e parâmetros por omissão, topologia de redes e composição lógica das arquiteturas das redes e sistemas de informação.

Por forma a que esta base esteja implementada corretamente, possuímos:

- ✓ Sistema de gestão de atualizações de segurança.

São aplicados, na organização, os princípios de engenharia de segurança da informação na especificação, desenho, desenvolvimento, implementação e modificação das suas redes e sistemas de informação. Estes princípios, nos sistemas legados que a organização detém, são aplicados, na medida do possível, tendo em conta o estado atual do hardware, software e *firmware* desses sistemas.

A organização realiza as suas cópias de segurança, sendo as mesmas testadas e validadas regularmente, através da execução de planos de testes de restauro, podendo as mesmas ser utilizadas, caso seja necessário efetuar-se o restauro das mesmas. Para tal, a organização utiliza:

- Ferramenta de cópias de segurança.

Na Câmara Municipal de Paços de Ferreira, são seguidas as políticas e regulamentação existentes, relativas à proteção de redes e sistemas de informação contra desastres naturais, falhas de energia, incêndios e inundações.

Existe, na organização, o seguinte:

- Proteção contra picos de corrente elétrica;
- Dispositivos físicos para simplificar e tornar seguro o controlo de energia;
- Gerador de eletricidade de emergência;
- Sensores de fumo, humidade, inundação e temperatura.

A organização, quando necessário, procede à destruição dos dados, de acordo com a política instituída, procedendo-se à:

- Higienização de ficheiros e sistemas de ficheiros, com destruidor de ficheiros;
- Utilização do destruidor de papel, quando necessário.

Com o objetivo de melhorar a segurança dos sistemas de informação, são atualizados regularmente (mês a mês) os processos de proteção, de forma a que as possíveis fragilidades existentes sejam identificadas e alvo de plano de correção.

A Câmara Municipal de Paços de Ferreira tem, neste momento, medidas e controlos para a monitorização efetiva da sua infraestrutura de rede, para a posterior recolha de estatísticas relacionada com incidentes de segurança, em colaboração com a empresa Hardsecure.

Foi implementado Multifator Autentication, com a colaboração da Whatchguard, e existem também os seguintes documentos (carecem de aprovação do executivo e respetiva publicação):

- Plano Tratamento Risco
- Política de Segurança da Informação
- Política Uso Aceitável Internet
- Política Equipamentos Moveis
- Política Teletrabalho
- Política Uso Aceitável Ativos
- Política Controlo de Acessos

- Política Segurança Física
- Política Anti-Malware
- Política Backups
- Política Software
- Política Gestão Vulnerabilidades Técnicas
- Política Segurança Rede
- Política Segurança Relação Fornecedores
- Procedimento Classificação Informação
- Procedimento Acesso Datacenter
- Procedimento Gestão Acessos Utilizador
- Procedimento Avaliação Eventos Segurança Informação
- Procedimento Resposta Incidentes Segurança Informação
- Processo Avaliação Tratamento Risco
- Formulário Avaliação Risco

A infraestrutura está protegida pela firewall, Paloalto. A VPN de acessos do exterior aos serviços é feita com o GlobalProtect da Paloalto. O MFA está aplicado na VPN, como no Office 365, que foi instalado no município, com o plano E3.

Em conclusão, a Câmara Municipal de Paços de Ferreira não está totalmente livre de um potencial ciber ataque. Contudo, está minimamente protegida.

7. Conclusões finais

De uma forma resumida, no intuito de focar os aspetos de maior criticidade, relacionados com a vertente de segurança da informação presente na plataforma tecnológica da Câmara Municipal de Paços de Ferreira, concluiu-se que os aspetos que se destacam como sendo críticos e, consequentemente, com maior urgência e necessidade de intervenção são os seguintes:

Políticas de Segurança de Informação – A ausência de um conjunto de políticas corporativas formais, direcionadas para a Segurança da Informação, implica uma falha na componente organizacional. Deve ser desenvolvido e implantado um conjunto de documentação corporativa que reflita as normas de segurança a aplicar à informação crítica existente na organização. Essa documentação deverá ser devidamente formalizada perante o executivo, através de um documento formal que expresse as preocupações da organização e estabeleça as linhas mestras para a gestão da segurança da informação, aprovado pelo executivo, publicado e comunicado, de forma adequada, a todos os funcionários;

Arquitetura de Rede – Verificou-se a ausência de uma arquitetura de rede adequada, que garanta a integridade da rede corporativa, reduzindo ao mínimo a sua exposição a riscos de intrusão externos e proteja a rede corporativa de conteúdos maliciosos oriundos do exterior. Deve ser implementada uma plataforma de publicação de serviços externos (DMZ), que possibilite a existência de um nível de separação de tráfego distinto entre o perímetro e a rede interna da organização, o que, por si só, mitiga a exposição da informação corporativa da organização a riscos extremamente elevados;

Domínio Corporativo - As funcionalidades e potencialidades disponibilizadas pelo conceito de domínio corporativo não estão a ser devidamente utilizadas. Deve ser criado um domínio corporativo baseado em tecnologia Microsoft – *Active Directory* – que respeite as normas e exigências de segurança da organização. A ausência de políticas de segurança, referentes a um domínio corporativo e à plataforma de postos de trabalho da organização, pode ser considerada como uma falha grave de segurança e organizacional na operação e gestão das diversas plataformas tecnológicas e aplicacionais em vigor na organização;

Gestão de Atualizações – A plataforma de sistemas, na sua maioria, não está a ser devidamente atualizada. Torna-se necessário corrigir a ausência de um conjunto de políticas e procedimentos, que garantam o correto funcionamento dos sistemas de informação de um ponto de vista de segurança, nomeadamente ao nível das atualizações de segurança nos sistemas, através da implementação imediata de um sistema adequado ao ambiente tecnológico presente na organização;

Controlo de acessos à Internet – Notou-se, também, a ausência de um sistema de controlo de acessos à Internet (Proxy), implementado de uma forma correta, que acelere as comunicações e que proteja a rede de conteúdos não desejados;

Backup & Restore - Não se encontra implementado, na organização, um procedimento para a realização de backups da informação corporativa, presente nos servidores da sua plataforma tecnológica. Atualmente, apenas estão a ser efetuadas cópias de segurança (backups) ao servidor aplicacional e ao servidor SIG, o que representa uma falha grave de segurança, na preservação da informação, e põe em risco o bom funcionamento dos serviços. Deverá ser definido um planeamento adequado, de modo que sejam realizadas, com uma periodicidade pré-estabelecida, cópias de segurança aos dados e sistemas críticos para a organização;

Monitorização/Alarmística - Da mesma forma, a falta de um sistema de monitorização e alarmística de eventuais anomalias dos sistemas críticos, devidamente associado a um modelo de suporte reativo, apresenta-se como uma referência a ter em conta, de forma preponderante.

Auditorias periódicas – Verificou-se a necessidade de manutenção e auditoria periódica aos sistemas de informação, garantindo um conjunto de políticas e procedimentos que garantam o correto funcionamento dos sistemas de informação, de um ponto de vista de segurança;

Suporte Preventivo e Reativo – Constatou-se, ainda, a ausência de um modelo funcional e abrangente de suporte (preventivo e reativo) na organização que garanta um acompanhamento regular no processo de evolução e estratégia das Tecnologias e Sistemas de Informação da Câmara Municipal de Paços de Ferreira.

Após a analise descrita neste trabalho, procedeu-se à mitigação das falhas identificadas. Desde logo, se implementou o domínio corporativo, que impede que os utilizadores possam, por exemplo, instalar software que se venha a verificar como sendo maligno. Também, ao nível de passwords, com o domínio pode-se parametrizar determinada complexidade e tempo de expiração. Foi instalada a firewall Fortinet e segmentada a rede, com a compra de switchs de layer 2. A firewall incorpora um proxy, o que permitiu bloquear determinados sites, como, por exemplo, o Facebook.

Mais tarde, a Fortinet foi substituída pela firewall ISA da Microsoft e, posteriormente, substituiu-se pelo PFSense. Atualmente, a que está a funcionar, no município, é a Paloalto.

Todos os servidores foram migrados para o DataCenter do Vale do Sousa Digital, o que permitiu resolver os problemas de segurança física e backups. Foram, também, implementadas todas as políticas que foram descritas no capítulo anterior.

Posto isto, pode-se concluir que, neste momento, a Câmara Municipal de Paços de Ferreira está menos vulnerável a ataques cibernéticos.

Bibliografia

Carneiro, Alberto (2002), **Introdução à Segurança dos Sistemas de Informação**, FCA.

Stallings, W. (2006), **Cryptography and Network Security,** Prentice Hall.

Davis, C.; Schiller, M.; Wheeler, K. (2007), **IT Auditing - using controls to protect information assets**, McGraw Hill.

Correia M., Sousa P. (2010), **Proteção em Sistemas Operativos**, in FCA. Segurança em Software, Lisboa, FCA.

Ferreira, F.; Araújo, M, **Política de Segurança de Informação** - Guia Prático para Elaboração e Implementação, 2.ª edição, Rio de Janeiro: Ciência Moderna, 2008.

Natário R, **"O Ciberespaço E A Vulnerabilidade Das Infraestruturas Críticas: Contributos para um Modelo Nacional de Análise e Gestão do Risco Social"**, Academia Militar, Tese de mestrado, Lisboa, 2014.

Information security, Article in Business Information Review · June 2016.

Information Systems Security Governance Research: A Behavioral Perspective Article, January 2006.

Howard,). Reduce Security Risks this Decade. Indianapolis, Wiley Publishing, Inc., Security 2020. D. and K. Prince (2011