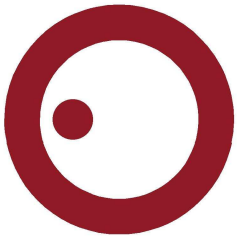


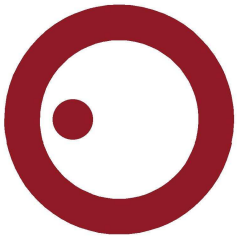
escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

PLANO DE IMPLEMENTAÇÃO DE UM SGSI, BASEADO NO QNRCS, EM MUNICÍPIOS DE PEQUENA E MÉDIA DIMENSÃO

ESTUDANTE PEDRO MIGUEL GONÇALVES MARQUES

Leiria, Setembro de 2024



escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

PLANO DE IMPLEMENTAÇÃO DE UM SGSI, BASEADO NO QNRCS, EM MUNICÍPIOS DE PEQUENA E MÉDIA DIMENSÃO

ESTUDANTE PEDRO MIGUEL GONÇALVES MARQUES
Número: 2220289

Dissertação realizada sob orientação do Professor Doutor Leonel Filipe Simões Santos (leonel.santos@ipleiria.pt) e coorientação do Professor Especialista Carlos Manuel Gonçalves Antunes (carlos.antunes@ipleiria.pt).

Leiria, Setembro de 2024

AGRADECIMENTOS

Gostaria de expressar os meus sinceros agradecimentos a todos aqueles que contribuíram para a realização desta dissertação. A conclusão deste trabalho só foi possível graças ao apoio, orientação e incentivo de várias pessoas especiais.

Em primeiro lugar, quero expressar a minha mais sincera gratidão à minha família. À minha esposa, agradeço profundamente por todo o apoio e dedicação incansável na elaboração deste trabalho. A tua paciência e compreensão foram fundamentais para que eu pudesse prosseguir, mesmo nos momentos mais desafiadores. À minha filha Camila, agradeço pelas várias ajudas, que também foram importantes para o desenvolvimento deste documento. E ao meu filho António, agradeço pela compreensão e pelo apoio na execução de algumas tarefas do meu dia a dia, permitindo-me ter o tempo necessário para me dedicar a este projeto.

Agradeço também aos meus orientadores, Prof. Doutor Leonel Santos e Prof. Especialista Carlos Antunes, pelo seu envolvimento, apoio constante e disponibilidade durante todas as fases deste projeto. Foi um privilégio trabalhar sob a vossa supervisão, e estou imensamente grato por todo o tempo, paciência e dedicação que empenharam na minha dissertação. Os vossos conselhos e contributos foram essenciais para a superação dos vários desafios.

Obrigado a todos por fazerem parte deste percurso e por tornarem esta experiência gratificante.

A todos, deixo o meu mais sincero muito obrigado!

RESUMO

Os municípios de pequena e média dimensão, bem como grande parte das organizações de menor dimensão, enfrentam desafios significativos na proteção dos respetivos ativos de informação devido a diversos fatores, como veremos ao longo desta dissertação.

Esta dissertação propõe, para esses municípios, um plano de implementação de um Sistema de Gestão da Segurança da Informação (SGSI), baseado no Quadro Nacional de Referência para a Cibersegurança (QNRCS), estruturado em várias linhas de ação, que abordam temas essenciais para a execução do plano.

Inicialmente, é efetuada a caraterização dos municípios de pequena e média dimensão, onde se incluem referências às suas particularidades. Em seguida, discute-se a norma ISO/IEC 27001 e o QNRCS e ferramentas associadas, com referência a conceitos essenciais relacionados com a Segurança da Informação, bem como a temática de Gestão de Ativos de Informação, processo de definição do Contexto e o processo de Análise de Riscos. São também revistas as normas, regulamentos e legislação aplicável à realidade específica dos municípios.

Deste estudo resultou a criação de um roadmap detalhado e personalizado para a implementação do SGSI nos municípios de pequena e média dimensão, descrevendo-se processos como, Estratégia para gestão do SGSI, Gestão dos Ativos de Informação, Análise de Risco, Políticas, Procedimentos e Controlos de Segurança de Informação e, por fim, a estrutura documental para o SGSI.

A adoção da proposta de estrutura documental apresentada, que inclui, Política Geral de Segurança da Informação, Política de Uso Aceitável (PUA) para os recursos de TI, Plano de Resposta a Incidentes, Playbook para incidente de Phishing, entre outros documentos, representa um passo importante para os municípios de pequena e média dimensão assegurarem a conformidade com os padrões de cibersegurança.

Palavras-chave: Sistema de gestão de segurança da informação, Gestão dos Riscos, Políticas e Procedimentos, Cibersegurança, Quadro Nacional de Referência para a Cibersegurança

ABSTRACT

Small and medium-sized municipalities, as well as a large portion of smaller organizations, face significant challenges in protecting their information assets due to various factors, as will be discussed throughout this dissertation.

This dissertation proposes, for these municipalities, an implementation plan for an Information Security Management System (ISMS), based on the portuguese cybersecurity reference framework (QNRCS - Quadro Nacional de Referência para a Cibersegurança), structured around several action lines that address essential topics for the execution of the plan.

Initially, the characterization of small and medium-sized municipalities is provided, including references to their particularities. Then, the ISO/IEC 27001 standard, the QNRCS, and associated tools are discussed, with reference to essential concepts related to Information Security, as well as the themes of Information Asset Management, the process of defining the Context, and the Risk Analysis process. Additionally, standards, regulations, and legislation applicable to the specific reality of municipalities are reviewed.

This study resulted in the creation of a detailed and customized roadmap for the implementation of an ISMS (Information Security Management System) in small and medium-sized municipalities. The roadmap outlines key processes such as the ISMS management strategy, information asset management, risk analysis, information security policies, procedures, controls, and, finally, the documentation framework for the ISMS.

The adoption of the proposed documentation framework, which includes the General Information Security Policy, Acceptable Use Policy (AUP) for IT resources, Incident Response Plan, Phishing Incident Playbook, among other documents, represents an important step for small and medium-sized municipalities to ensure compliance with cybersecurity standards.

Palavras-chave: Information Security Management System, Risk Management, Policies and Procedures, Cybersecurity, National Cybersecurity Reference Framework

ÍNDICE

Apêndices

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

BCP	Business Continuity Plan.
BT	Baixa Tensão.
BYOD	Bring Your Own Device.
CAF	Cyber Assessment Framework.
CERT	Computer Emergency Response Team.
CIA	Confidentiality, Integrity e Availability.
CISO	Chief Information Security Officer.
CNCS	Centro Nacional de Cibersegurança.
CSIRT	Computer Security Incident Response Team.
DPO	Data Protection Officer.
DRP	Disaster Recovery Plan.
ENISA	European Union Agency for Cybersecurity.
GLPI	Gestionnaire Libre de Parc Informatique.
HIDS	Host-based Intrusion Detection Systems.
IAAS	Infrastructure as a Service.
IEC	International Electrotechnical Commission.
INEM	Instituto Nacional de Emergência Médica.
IoT	Internet of Things.
ISACA	Information Systems Audit and Control Association.
ISO	International Organization for Standardization.
NCI	Norma de Controlo Interno.

NCSC	National Cyber Security Center.
NIS	Network and Information Systems.
NIST SP 800-61	National Institute of Standards and Technology Special Publication 800-61.
NLI	Núcleo Local de Inserção.
OES	Operadores de Serviços Essenciais.
PAAS	Platform as a Service.
PGRCIC	Plano de Gestão de Riscos de Corrupção e Infrações Conexas.
PRI	Plano de Resposta a Incidentes.
PSI	Política de Segurança da Informação.
PUA	Política de Uso Aceitável.
QACC	Quadro de Avaliação de Capacidades de Cibersegurança.
QNRCS	Quadro Nacional de Referência para a Cibersegurança.
RGPD	Regulamento Geral sobre a Proteção de Dados.
RSI	Rendimento Social de Inserção.
SAAS	Software as a Service.
SANS	SysAdmin, Audit, Network, and Security Institute.
SGSI	Sistema de Gestão de Segurança da Informação.
SI	Segurança da Informação.
SIEM	Security Information and Event Management.
SIR	Security Incident Response.
SOA	Statement of Applicability.
SOC	Security Operations Center.
TI	Tecnologias de Informação.
TICE	Tecnologias da Informação, Comunicação e Eletrónica.

VPN Virtual Private Network.

1

INTRODUÇÃO

Os municípios enfrentam diversos desafios em matéria de cibersegurança, influenciados por diversos fatores, nomeadamente, a ampla gama de áreas de atuação e responsabilidades, a crescente complexidade das ameaças de cibersegurança e a limitação de recursos.

Alguns destes desafios surgem relacionados com a complexidade da infraestrutura de TI que os municípios gerem, que abrange diversas áreas, tais como, urbanismo e ordenamento do território, trânsito e mobilidade, habitação, educação, saúde, cultura, desporto, ambiente, ação social, segurança e proteção civil. Estas áreas, na maioria dos casos, tem sistemas de informação diferentes, o que aumenta a complexidade de proteger todos os ativos de informação.

Em particular, municípios de pequena e média dimensão enfrentam dificuldades na adoção de um SGSI, devido à complexidade do processo de implementação. O QNRCS pode ser parte da solução para esses desafios, pois fornece diretrizes e melhores práticas que irão auxiliar na mitigação dos riscos e na implementação de medidas de segurança mais eficazes.

Um desafio, igualmente importante, surge no âmbito da proteção de dados pessoais. Os municípios tratam dados pessoais de cidadãos em várias áreas, como os guardados em sistemas de informação relacionados com o funcionamento das escolas, os relacionados com pedidos de licenciamento ou outro tipo de requerimentos, registos de serviços sociais e culturais, entre outros. A proteção destes dados é de extrema importância, principalmente no que concerne ao cumprimento da legislação relacionada com a proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD).

Um outro desafio cada vez mais atual nos municípios, são as diversas ameaças de cibersegurança de que tem sido alvo. Os municípios estão sujeitos a uma grande variedade de ameaças de cibersegurança, incluindo ataques de ransomware, phishing, malware e outras formas de exploração, e cada departamento e área pode ser alvo de um tipo dessas ameaças. No caso dos municípios responsáveis pela gestão de infraestrutura crítica de serviços essenciais, tais como, sistemas de água, energia e trânsito, este desafio aumenta, sendo crítico proteger estes sistemas contra ameaças de cibersegurança.

Os desafios apresentados anteriormente, são apenas uma amostra das dificuldades com que os municípios se deparam. A estes, acrescem ainda, as regulamentações específicas de segurança de informação, o que exige um esforço contínuo de conformidade. Na atualidade, é importante destacar a influência do novo quadro regulamentar da União Europeia, a NIS2, publicado em 14 de dezembro de 2022 e que irá a curto prazo entrar em vigor no nosso país. A data limite para a transposição desta Diretiva para a legislação nacional é 17 de outubro de 2024.

Com a NIS2, um maior número de entidades, incluindo todas as autarquias, passam a estar obrigadas a adotar as normas regulatórias europeias de cibersegurança.

A referida Diretiva estabelece sanções elevadas, com coimas que podem chegar a dez milhões de euros ou 2% do volume de negócios anual, além de exigir medidas mais apertadas para a gestão dos riscos.

A NIS2 tem enfoque na prevenção e mitigação de riscos e nesse contexto, a implementação de um SGSI, conforme se irá propor neste trabalho, permitirá uma abordagem proativa para identificar e gerir as ameaças de cibersegurança.

Para enfrentar estes desafios, os municípios tem de adotar uma abordagem estratégica para a cibersegurança. Esta abordagem, para além de outras medidas, inclui o desenvolvimento de um programa de segurança de informação.

Um programa de segurança da informação consiste na definição de um conjunto de ações estruturantes, consequentes de um estudo prévio de avaliação de riscos, definição de objetivos e de medidas de segurança, que serão assim a base do SGSI de uma organização.

Neste estudo, subordinado ao tema Plano de Implementação de um SGSI, baseado no Quadro Nacional de Referência para a Cibersegurança (QNRCS), nos municípios de pequena e média dimensão, será utilizado o QNRCS e ferramentas relacionadas, como instrumentos de apoio à elaboração de um plano de implementação de um SGSI. Pretende-se apresentar uma metodologia de trabalho de criação de um SGSI para os municípios de pequena e média dimensão, seguindo as diretrizes do QNRCS e alinhada com as competências legais próprias e objetivos estratégicos deste tipo de organização. O QNRCS foi criado no âmbito da missão do Centro Nacional de Cibersegurança (CNCS), sendo o CNCS instituído com a entrada em vigor da Lei n.º 46/2018, a qual define um conjunto de medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (regime jurídico de segurança no ciberespaço). O QNRCS é um documento complementar à referida lei, já que esta, não refere métodos a seguir para implementar um programa de segurança de informação. Visto ser um documento guia, que está de acordo com os padrões internacionais de gestão da

segurança de informação, contribuirá de forma relevante para a elaboração de um SGSI.

1.1 OBJETIVOS

O objetivo deste trabalho consiste na elaboração de uma proposta de metodologia de implementação de um SGSI, para os municípios de pequena e média dimensão, e garantir que estas autarquias tenham um conjunto de políticas, procedimentos e controlos eficazes para aumentar a proteção das suas informações contra ameaças de cibersegurança. Com este trabalho pretende-se definir um conjunto de ações concretas a adotar para cada uma das áreas do SGSI, determinará e direcionará ações no âmbito da gestão dos riscos de segurança da informação, classificação e avaliação dos ativos relacionados com os sistemas de informação, indicação de controlos necessários, a sua aplicabilidade e forma de operacionalizar.

Pretende-se também apresentar protótipos das seguintes Políticas e Planos: Política Geral de Segurança da Informação, Política de Uso Aceitável para os Recursos de TI, Plano de Resposta a Incidentes, Plano de Comunicação de Incidentes, Plano de Testes ao PRI, Plano de Divulgação Interna e Formação do PRI, Playbook para Incidente de Phishing, Playbook para Incidente de Acesso Não Autorizado e Playbook para Incidente de Ransomware.

Com este trabalho pretende-se obter os seguintes resultados e contributos:

- Apresentação de uma proposta de procedimento para Avaliação dos Riscos de cibersegurança, em relação aos ativos que garantem a continuidade de funcionamento das redes e dos sistemas de informação em produção e ainda dos ativos que garantem a prestação de serviços;
- Indicação de ações que poderão ser adotadas no campo da gestão de ativos de informação;
- Indicação de um conjunto de procedimentos operacionais de implementação, repartidos nas seguintes cinco linhas de ação: Estratégia para gestão do SGSI, Gestão de Infraestrutura Física e Ambiental, Gestão da Tecnologia, Gestão dos Ativos Humanos no âmbito da SI e Compliance;
- Produção de um conjunto de documentos, que propõem os controlos de prevenção, deteção e investigação necessários, a sua aplicabilidade e forma de operacionalizar;
- Produção de um protótipo de Política Geral de Segurança da Informação;
- Produção de um protótipo de Política de Uso Aceitável (PUA) para os recursos de TI;
- Produção de uma proposta de Plano de Resposta a Incidentes e respetivos documentos acessórios, tais como: Plano de comunicação de incidentes, Plano de testes ao PRI, Plano de divulgação interna e formação do PRI, Playbook

para incidente de Phishing, Playbook para incidente de Acesso Não Autorizado e Playbook para incidente de Ransomware.

É importante destacar que o roadmap a apresentar neste trabalho efetuará referência a todas as etapas da estrutura do plano de implementação do SGSI, no entanto, não serão abordadas ou detalhadas, as etapas finais, referentes a Operação e Desenvolvimento do SGSI, pois estas estão fora do âmbito deste estudo.

1.2 METODOLOGIA E CRONOLOGIA

Para a execução da proposta de Plano de Implementação de um SGSI, conforme objeto deste estudo, será necessário efetuar recolha de informação acerca das funções, competências, domínios de intervenção dos municípios de pequena e média dimensão, e também dos processos internos que decorrem habitualmente numa autarquia de pequena e média dimensão. Esse levantamento será efetuado através de análise de documentos disponibilizados pelos municípios nos vários tipos de fontes abertas e através de consulta a normas, regulamentos, resoluções e legislação aplicável ao setor.

Numa fase inicial, serão propostos procedimentos para identificação de recursos e definição de responsabilidades para a implementação e continuidade de um SGSI, definindo-se a ligação com os sistemas e tecnologias de informação e com todo o contexto deste tipo de entidade.

Posteriormente, definir-se-á uma abordagem estruturada e sistemática, para planear e executar as etapas necessárias, de definição de um plano de implementação de um SGSI eficaz para um município.

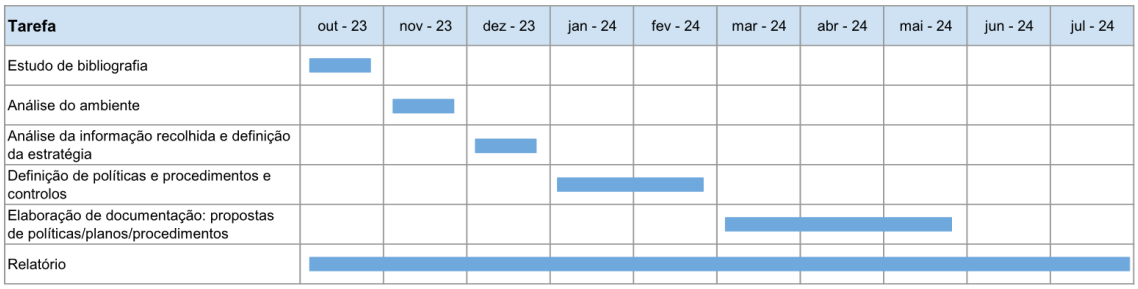
O plano de implementação de um SGSI baseado no QNRCS, seguirá as seguintes etapas:

- Análise do ambiente: definição de procedimentos para avaliar os ativos de informação de uma autarquia, definição de procedimentos para identificar as possíveis ameaças e vulnerabilidades existentes e avaliar o impacto que essas ameaças podem ter numa autarquia;
- Definição da estratégia: com base na análise do ambiente hipotético de uma autarquia, definir uma estratégia de segurança da informação, que inclua objetivos e metas claras, bem como uma estratégia de gestão de riscos;
- Criação de políticas e procedimentos de segurança da informação e definição de controlos para mitigar os riscos identificados na análise do ambiente;
- Gestão de incidentes: sugestão de processos para identificar, responder e gerir incidentes de segurança da informação;
- Monitorização, avaliação e melhoria contínua: efetuar referência à necessidade de existirem procedimentos para monitorizar regularmente o SGSI e assim garantir que os controlos funcionam corretamente e que os objetivos e metas de segurança da informação são atingidos, atuando sempre que necessário com ações corretivas e preventivas para melhorar o SGSI.

O diagrama de Gantt, conforme figura n.º 1, ilustra o desenvolvimento das diferentes etapas do trabalho:

Plano de implementação de um SGSI, baseado no QNRCS, em municípios de pequena e média dimensão

Visão geral do trabalho



Tarefa	out - 23	nov - 23	dez - 23	jan - 24	fev - 24	mar - 24	abr - 24	mai - 24	jun - 24	jul - 24
Estudo de bibliografia										
Análise do ambiente										
Análise da informação recolhida e definição da estratégia										
Definição de políticas e procedimentos e controlos										
Elaboração de documentação: propostas de políticas/planos/procedimentos										
Relatório										

Figura 1: Diagrama de Gantt - etapas do trabalho

1.3 ESTRUTURA DO DOCUMENTO

Este documento está organizado em cinco capítulos, nos quais, nos primeiros três capítulos, são apresentados os objetivos definidos, metodologia e cronologia adotada, caraterização dos municípios portugueses, revisão de literatura e de conceitos relacionados, apresentada uma breve caraterização da norma ISO/IEC 27001 e do QNRCS e ferramentas associadas. São ainda descritos alguns dos regulamentos e legislação aplicável às autarquias locais, no âmbito da segurança da informação, e efetuada uma referência a trabalhos relacionados.

No quarto capítulo, é desenvolvida a proposta de Plano de Implementação do SGSI e apresenta-se a respetiva estrutura. Esta inclui um roadmap detalhado e personalizado, para adoção nos municípios de pequena e média dimensão, cobrindo as várias etapas necessárias para uma implementação bem-sucedida, em áreas como, estratégia para gestão do SGSI, Gestão dos Ativos de Informação, Análise de Risco, Políticas, Procedimentos e Controlos de Segurança de Informação e, por fim, a Estrutura Documental para o SGSI.

Encerra, no capítulo quinto, com a Conclusão.

2

CARATERIZAÇÃO DOS MUNICÍPIOS PORTUGUESES

A definição de autarquia local está prevista na Constituição da República Portuguesa, no artigo 235.º (República, 2023), o qual estabelece que: "A organização democrática do Estado compreende a existência de autarquias locais, as quais são pessoas coletivas territoriais dotadas de órgãos representativos e que visam a prossecução de interesses próprios das populações respetivas."

O artigo 236.º da Constituição da República Portuguesa, estabelece que "O município é a autarquia local que tem por circunscrição o concelho."

A Lei n.º 75/2013, de 12 de setembro (República, 2013b), que estabelece o regime jurídico das autarquias locais, também define autarquia local como "a pessoa coletiva territorial dotada de órgãos representativos eleitos diretamente pelos cidadãos que residem no seu território e que visa a prossecução de interesses próprios das populações respetivas".

Assim, os municípios são legalmente definidos como autarquias locais. Um município é equivalente a um concelho. Cada município ou concelho é uma unidade administrativa local com seu próprio governo local, conhecido como câmara municipal.

As autarquias locais tem o objetivo de visar a prossecução de interesses próprios da população residente no concelho, mediante órgãos representativos eleitos.

Atualmente, os municípios possuem atribuições nos seguintes domínios (art.º 23.º do Anexo I da Lei n.º 75/2013, de 12 de setembro (República, 2013a)):

- Equipamento rural e urbano;
- Energia;
- Transportes e comunicações;
- Educação;
- Património, cultura e ciência;
- Tempos livres e desporto;
- Saúde;
- Ação social;
- Habitação;

- Proteção civil;
- Ambiente e saneamento básico;
- Defesa do consumidor;
- Promoção do desenvolvimento;
- Ordenamento do território e urbanismo;
- Polícia municipal;
- Cooperação externa

A definição destas atribuições tem subjacente a prossecução das funções de interesse local pelo nível de governo mais próximo da população que, naturalmente, conhece melhor os seus problemas e necessidades, o qual sustenta a crescente transferência de atribuições e competências da Administração Central para os municípios.

Em 2018, com a aprovação da Lei n.º 50/2018 (República, 2018), referente à Transferência de Competências para as Autarquias Locais e para as Entidades Intermunicipais, foi iniciado um processo de descentralização administrativa da administração central para os municípios, que pode ainda não estar concluído em alguns municípios. As novas competências transferidas para os municípios abrangem uma ampla gama de áreas, destacando-se as seguintes:

- Educação - gestão dos estabelecimentos públicos de educação e de ensino integrados na rede pública dos 2.º e 3.º ciclos do ensino básico e do ensino secundário, incluindo o profissional, nomeadamente na sua construção, equipamento e manutenção;
- Saúde - gestão e realização de investimentos relativos a novas unidades de prestação de cuidados de saúde primários, nomeadamente na sua construção, equipamento e manutenção.
- Cultura - de entre outras competências, gerir, valorizar e conservar património cultural que, sendo classificado, se considere de âmbito local e gerir, valorizar e conservar os museus que não sejam museus nacionais.
- Segurança e proteção civil - destaque para a competência de intervenção na gestão dos sistemas de videovigilância e de vigilância móvel no âmbito da defesa da floresta contra incêndios e assegurar o funcionamento do centro de coordenação operacional municipal.
- Património - responsabilidade na gestão do património imobiliário público sem utilização e afeto à administração direta e indireta do Estado, incluindo partes de edifícios.

- Habitação - no âmbito desta competência, destaque para a transferência para os municípios, da titularidade e gestão dos bens imóveis destinados a habitação social que integram o parque habitacional da administração direta e indireta do Estado.
- Estruturas de atendimento ao cidadão - competência para instalar novas lojas de cidadão, cabendo-lhes posteriormente a sua gestão, em articulação com a rede nacional de lojas de cidadão e ainda, instalar e gerir os espaços cidadão, em articulação com a rede de lojas de cidadão e instituir e gerir os centros locais de apoio à integração de migrantes.

No seguimento da verificação das competências legalmente previstas, destacam-se algumas das funções mais relevantes para o objeto deste estudo, e que são desenvolvidas pelos municípios que já tenham concluído o processo de descentralização administrativa:

- Educação: os municípios que tenham aceite a delegação de competências nesta matéria, são responsáveis pela gestão das escolas públicas do seu concelho, desde a educação pré-escolar ao ensino secundário. Significa assim que são responsáveis por dotar as escolas do seu concelho com condições necessárias para que os alunos possam usufruir de um ensino de qualidade. As atividades escolares nas diversas vertentes da sua responsabilidade, incluem, a organização e gestão da rede educativa, construção, conservação, manutenção e apetrechamento dos estabelecimentos de ensino pré-escolar, do ensino básico e secundário, organização e coordenação do fornecimento de refeições escolares nos vários estabelecimentos de ensino, no apoio às crianças no domínio da Ação Social Escolar, gestão do pessoal não docente, afetos aos estabelecimentos de ensino, colaboração nos projetos educativos, entre outras.
- Saúde: os municípios cujo processo de descentralização administrativa neste âmbito já tenha sido concluído, gerem os centros de saúde, nomeadamente, através da beneficiação de edifícios e equipamentos, contratação de pessoal e de serviços para o funcionamento destas infraestruturas.
- Cultura: os municípios promovem atividades culturais, dinamizam museus, bibliotecas, teatros e eventos culturais. Efetuam a produção de conteúdos diversos, em alguns casos com divulgação dinâmica nas redes sociais. Ainda no âmbito da cultura, efetuam a gestão de arquivos históricos e bibliotecas.
- Desporto: os municípios promovem atividades desportivas, disponibilizam campos desportivos, pavilhões gimnodesportivos, piscinas entre outros equipamentos desportivos.

- Ambiente: os municípios são responsáveis pela gestão dos resíduos sólidos, limpeza urbana, manutenção de jardins e espaços verdes, gestão dos sistemas de rega e proteção do ambiente.
- Ação social: os municípios prestam serviços de ação social, como apoio a idosos, pessoas com deficiência e famílias em situação de vulnerabilidade. Promovem o acesso a uma habitação adequada às pessoas que vivem em situações habitacionais indignas e que não dispõem de capacidade financeira para encontrar uma solução habitacional condigna. No caso dos municípios que tenham aceite a transferência de competências no âmbito da Ação Social, os municípios asseguram o Serviço de Atendimento e Acompanhamento Social, a coordenação do Núcleo Local de Inserção (NLI) e os Contratos de Inserção dos beneficiários do Rendimento Social de Inserção (RSI).
- Segurança e proteção civil: os municípios são responsáveis pela gestão da proteção civil, nomeadamente, através da organização de exercícios e da sensibilização da população para os riscos naturais e pelo combate a catástrofes e situações de emergência. Os municípios de média dimensão dispõe de um Centro Municipal de Proteção Civil, que consiste numa estrutura permanente de direção que pretende garantir a coordenação e a articulação com todos os agentes de proteção civil municipal integrantes do sistema de proteção e socorro, assegurando a coordenação e o controlo das situações de âmbito municipal que, pela sua natureza, gravidade, extensão e meios envolvidos ou a envolver, requeiram a sua intervenção, acompanhando em permanência a situação operacional no domínio das entidades integrantes ao Sistema Integrado de Operações de Proteção e Socorro.

  Para além as funções acima referenciadas, asseguram a limpeza e manutenção de florestas e caminhos florestais, articulam a atuação dos organismos com competências em matérias de defesa da floresta, no âmbito da sua área geográfica e preparam planos de defesa da floresta contra incêndios.
- Planeamento e gestão do território: os municípios são responsáveis pelo planeamento do território do seu concelho, nomeadamente através da elaboração de planos diretores municipais.
- Obras públicas: os municípios são responsáveis pela execução de obras públicas, como a construção de estradas, pontes e edifícios públicos.
- Turismo: os municípios promovem o turismo no seu concelho, nomeadamente através da criação de infraestruturas turísticas e da organização de eventos culturais e desportivos.

- Planeamento Urbanístico e Planos de Pormenor: neste âmbito os municípios dispõe de gabinetes com técnicos de Sistemas de Informação Geográfica, onde são efetuados trabalhos técnicos de ortofotocartografia e cartografia.
- Urbanização: os municípios são responsáveis pelas intervenções de urbanização dos espaços urbano, tais como, cidades.
- Edifícios Municipais de domínio público: os municípios asseguram a manutenção de edifícios municipais de domínio público, tais como, castelos e outros edifícios históricos.
- Saneamento: neste âmbito os municípios efetuam a gestão das rede de infraestruturas de saneamento, com o intuito de aumentar a qualidade ambiental dos recursos hídricos existentes.
- Cemitérios: os municípios, em alguns casos, asseguram a gestão deste tipo de infraestruturas.
- Água: os municípios são os responsáveis das redes e sistemas de abastecimento de água.
- Energia: os municípios são responsáveis pela gestão da Iluminação Pública. Ainda neste âmbito, a atividade de distribuição de energia elétrica em baixa tensão (BT) é um direito exclusivo dos municípios. Estes, ao longo dos anos, tem optado pela concessão da exploração desta atividade.
- Turismo: neste âmbito verifica-se a disponibilização pela maioria do municípios de cobertura wifi em pontos turísticos e a disponibilização informação ao turista pela via digital. Os municípios consideram que estas ferramentas tecnológicas tornam-se também num verdadeiro aliado no desenvolvimento e promoção dos destinos turísticos, tanto para utilização dos visitantes como da população residente.
- Feiras e mercados: os municípios dinamizam feiras tradicionais ou temáticas.
- Apoio ao tecido empresarial: os municípios disponibilizam infraestruturas de localização empresarial, tais como zonas industriais entre outras.
- Edifícios para congressos/eventos: os municípios efetuam a gestão das infraestruturas e equipamento associado e requerido à realização destes eventos.
- Freguesias: os municípios efetuam a gestão das infraestruturas relacionadas com a instalação de delegações/balcões dos municípios nestas entidades.
- Instalações e Serviços Municipais: os municípios asseguram a manutenção e beneficiação de edifícios municipais, e respetivos equipamentos, administrativos, informáticos, entre outros.

2.1 CARATERIZAÇÃO EM TERMOS DE DIMENSÃO POPULACIONAL

Em Portugal, verificamos atualmente, um total de 308 municípios, dos quais 278 estão no Continente e 30 estão nas Regiões Autónomas (sendo 19 nos Açores e 11 na Madeira).

Um método predominante para classificar os municípios em termos de dimensão é baseado na consideração do número de residentes. Assim, com base na informação disponibilizada pelo INE quanto ao número total de população residente, podemos organizar os municípios em três categorias diferentes:

- Municípios Pequenos – com população inferior ou igual a 20 000 habitantes;
- Municípios Médios – com população superior a 20 000 habitantes e inferior ou igual a 100 000 habitantes;
- Municípios Grandes – com população superior a 100 000 habitantes.

Assim, de acordo com informação disponibilizada pelo Anuário Financeiros dos Municípios Portugueses relativa ao ano de 2022 (Cávado e do Ave e Universidade do Minho, 2022), que tem por base o nº de habitantes publicado pelo Instituto Nacional de Estatística (INE), obtemos o quadro apresentado na figura n.º 2, que nos apresenta o número de municípios portugueses considerados Pequenos, Médios e Grandes.

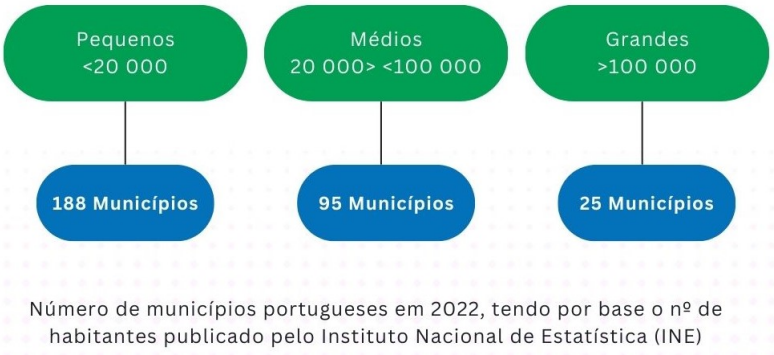


Figura 2: Categorização dos Municípios Portugueses quanto à dimensão

Conforme informação disponibilizada pelo INE e também pelo nuário Financeiros dos Municípios Portugueses relativa ao ano de 2022 (Cávado e do Ave e Universidade do Minho, 2022), no que concerne à caraterização dos municípios por regiões e de acordo com a sua dimensão, apresenta-se o quadro da figura n.º 3, que nos indica o peso percentual dos municípios Pequenos, Médios e Grandes, em cada uma das regiões de Portugal.

Fazendo a análise conjunta dos dados apresentados na figura n.º 2 e na figura n.º 3, revela que os municípios pequenos têm uma presença mais significativa no Alentejo, no Centro e nas regiões insulares.

Percentagem	Norte	Centro	Lisboa	Alentejo	Algarve	Açores	Madeira
Pequenos	53 %	65%	6%	78%	44%	84%	73%
Médios	35%	32%	33%	22%	56%	16%	18%
Grandes	12%	3%	61%	0%	0%	0%	9%

Figura 3: Categorização por regiões, considerando a dimensão dos municípios

Em contraste, na Região de Lisboa, apenas 6% dos municípios são considerados pequenos, com mais de 60% dos municípios, que se situam nessa região, a serem de grande dimensão.

2.2 CARATERIZAÇÃO QUANTO À DIMENSÃO DO VOLUME DE NEGÓCIOS

Consultando a informação disponibilizada pelo Anuário Financeiros dos Municípios Portugueses relativo ao ano de 2022 (Cávado e do Ave e Universidade do Minho, 2022), verifica-se que os municípios que arrecadam a maior quantidade de receita financeira, ou seja, maior volume de negócios, são principalmente aqueles de grande dimensão, e em menor quantidade, alguns de média dimensão.

Esta observação é baseada na figura n.º 4, obtida a partir do Mapa do Anuário Financeiro dos Municípios Portugueses de 2022, em particular na análise da receita cobrada.

	Município	Dimensão	2022
1	Lisboa	G	944 470 135
2	Cascais	G	290 783 343
3	Porto	G	268 711 476
4	Sintra	G	240 041 502
5	VN Gala	G	201 095 896
6	Oeiras	G	190 791 876
7	Loures	M	165 055 967
8	Loulé	G	161 774 360
9	Almada	G	144 360 350
10	Matosinhos	G	141 489 131
11	Seixal	G	139 820 294
12	Braga	G	131 035 020
13	Setúbal	G	120 605 433
14	Coimbra	G	118 210 635
15	Funchal	G	116 539 148
16	VN Famalicão	G	113 263 687
17	Odivelas	G	107 685 531
18	Guimarães	G	107 302 103
19	Amadora	G	103 557 983
20	Gondomar	G	101 784 202
21	VF Xira	G	99 798 942
22	Albufeira	M	97 472 689
23	Leiria	G	96 932 125
24	Mala	G	96 551 214
25	Mafra	M	92 180 017
26	SM Feira	G	91 452 022
27	Aveiro	M	85 321 122
28	Barcelos	G	82 487 545
29	V. Castelo	M	80804 845
30	Paredes	M	79 192 638
31	Portimão	M	78 349 167
32	Lagos	M	77 231 574
33	Viseu	G	74667 688
34	F. Foz	M	69 217 237
35	Palmela	M	68 027 409

Figura 4: Volume de negócios em euros, municípios de grande e média dimensão

Pela análise da figura n.º 5, verificamos que os municípios que têm uma receita financeira mais modesta são os de menor dimensão.

	Município	Dimensão	2022
1	Corvo	P	1 982 773
2	Sta. Cruz das Flores	P	3 274 403
3	Lajes das Flores	P	3 826 642
4	Sta. Cruz Graciosa	P	4 735 257
5	Calheta (R.A.A)	P	5 063 877
6	Porto Santo	P	5 399 470
7	Alvito	P	5 641 390
8	Castanheira Pera	P	5 725 939
9	São Roque do Pico	P	5 778 295
10	Barrancos	P	5 957 939
11	Nordeste	P	6 526 452
12	Arronches	P	6 549 006
13	Mourão	P	6 581 998
14	Fronteira	P	6 842 294
15	Mesão Frio	P	6 864 600
16	Pedrógão Grande	P	7 110 071
17	Vila do Porto	P	7 157 704
18	Lajes do Pico	P	7 202 080
19	Porto Moniz	P	7 260 075
20	SM Penaguião	P	7 463 879
21	Góis	P	7 558 627
22	V. Nova Barquinha	P	7 618 350
23	Alter do Chão	P	7 686 043
24	Castelo de VAIDE	P	7 697 004
25	Manteigas	P	7 702 393
26	Penedono	P	7 728 966
27	Constância	P	7 737 230
28	Golegã	P	7 777 906
29	Fornos de Algodres	P	7 780 115
30	Cuba	P	7 814 782
31	Santana	P	7 990 880
32	F.Espada à Cinta	P	8 008 222
33	Madalena	P	8 029 925
34	Penela	P	8 069 154
35	Mora	P	8 105 376

Figura 5: Volume de negócios em euros, municípios de pequena dimensão

2.3 ESTRUTURA ORGÂNICA TIPO, DE UM MUNICÍPIO DE PEQUENA E MÉDIA DIMENSÃO

No âmbito da preparação de um programa de segurança de informação, é relevante perceber a estrutura orgânica da entidade, dado que esta tem um papel relevante na implementação de um SGSI.

De acordo com a minha experiência e observação das práticas comuns em autarquias locais, a estrutura orgânica típica de um município de pequena e média dimensão, derivado das suas competência legais, em regra, é a seguinte:

- ✓ Assembleia Municipal
  - 🏢 Presidente da Assembleia Municipal
  - 🏢 Deputados Municipais
- ✓ Câmara Municipal
  - 🏢 Presidente da Câmara Municipal
  - 🏢 Vereadores
- ✓ Unidades Orgânicas Municipais:
  - 🏢 Unidade Orgânica de Administração Geral
  - 🏢 Unidade Orgânica de Educação
  - 🏢 Unidade Orgânica de Saúde
  - 🏢 Unidade Orgânica de Ambiente
  - 🏢 Unidade Orgânica de Obras Públicas
  - 🏢 Unidade Orgânica de Cultura
  - 🏢 Unidade Orgânica de Desporto
  - 🏢 Unidade Orgânica de Turismo
  - 🏢 Unidade Orgânica de Informática

Analisando a estrutura acima identificada, verificamos que é composta essencialmente por três níveis:

- Assembleia Municipal: órgão deliberativo do município, composto por representantes eleitos pelos cidadãos.
- Câmara Municipal: órgão executivo do município, composto pelo Presidente da Câmara Municipal e pelos Vereadores.
- Unidades Orgânicas Municipais: unidades administrativas responsáveis pela prestação de serviços públicos aos cidadãos.

2.4 PRINCIPAIS DIFERENÇAS ENTRE OS MUNICÍPIOS DE GRANDE DIMENSÃO E OS DE MÉDIA E PEQUENA DIMENSÃO

Algumas das principais diferenças entre os municípios de grande dimensão e os de média e pequena dimensão, são:

- Os municípios de grande dimensão tendem a ser maiores em área e densidade populacional, o que normalmente inclui uma grande cidade.
- Os municípios de média e pequena dimensão são menores em área e têm uma população significativamente menor e ficam localizados em áreas rurais ou semi-rurais, com menos densidade populacional.
- Os municípios grandes assumem responsabilidades e competências mais alargadas do que os municípios pequenos e de média dimensão, já que disponibilizam uma grande variedade de serviços urbanos. Estes municípios têm uma infraestrutura urbana mais desenvolvida, como redes de transporte público extensas, e de vários tipos.
- Ao nível da organização interna, os municípios grandes tem uma estrutura maior e mais complexa, bem como um maior número de funcionários.
- No campo da segurança e proteção civil, os municípios de grande dimensão tende a dispor de serviços de segurança e emergência mais robustos e também complexos, incluindo bombeiros e polícias municipais, enquanto, por outro lado, os de pequena e média dimensão, dispõe de serviços de segurança e proteção civil menos centralizados, e que incluem uma grande colaboração comunitária e redes de apoio local, tais como bombeiros voluntários.
- Ao nível orçamental e de financiamento, os municípios grandes tem mais recursos financeiros disponíveis para projetos de grande escala, do que os municípios pequenos e de média dimensão.

2.5 A DIMENSÃO COMO DESAFIO NA IMPLEMENTAÇÃO DE UM SGSI

No âmbito da implementação de um programa de segurança da informação, os desafios para um município de grande dimensão e de pequena e média dimensão são diferentes.

Os municípios de pequena e média dimensão, enfrentam geralmente restrições orçamentais (Nuvem, 2023) para a área de segurança da informação, o que pode dificultar a aquisição de tecnologias de segurança avançadas e a contratação de especialistas em cibersegurança. Muitas vezes, pelas mesmas questão financeiras, estes municípios não têm funcionários dedicados à cibersegurança, o que dificulta em muito o desenvolvimento e a implementação de um sistema de gestão de segurança da informação. Esta falta de recursos humanos especializado em cibersegurança, pode exigir uma atenção adicional na consciencialização dos funcionários e na formação acerca de práticas seguras de segurança da informação.

Os municípios de grande dimensão normalmente dispõe de equipas dedicadas à segurança da informação, sistemas de monitorização avançados e capacidade para implementar medidas alargadas de cibersegurança.

Por outro lado, verifica-se que os municípios de grande dimensão têm uma maior exposição a ameaças, devido à sua dimensão e complexidade, e assim podem ser alvos mais interessantes para ataques de cibersegurança, já que dispõem de uma grande quantidade de informação sensível e sistemas críticos.

2.6 CONCEITO DE CIDADES INTELIGENTES E A SUA APLICAÇÃO NOS MUNICÍPIOS DE PEQUENA E MÉDIA DIMENSÃO

Verificamos, atualmente, uma tendência para os municípios, incluindo os de pequena e média dimensão, aderirem a projetos denominados de Smart City (cidade inteligente) (AlgarData, 2024). Nos locais onde são implementados estes projetos, estes usam tecnologia, inovação e dados para melhorar a qualidade de vida dos residentes, a eficiência operacional e a sustentabilidade ambiental.

No âmbito deste conceito, são criadas várias plataformas digitais que desempenham um papel fundamental na construção e operação de uma Smart City.

No contexto deste trabalho devem ser conhecidos estes tipos de plataformas, já que as mesmas tem a sua importância no processo de implementação do SGSI, pois cada plataforma tem requisitos específicos de segurança e privacidade.

Alguns tipos de plataformas digitais que podemos encontrar atualmente nos municípios de pequena e média dimensão, com projetos do tipo Smart City (Smart Cities Marketplace, 2024), conforme ilustrado na figura n.º 6, são:

- Plataforma de IoT (Internet das Coisas): uma plataforma de IoT é fundamental para ligar sensores e dispositivos em toda a cidade, recolhendo dados em tempo real para monitorizar o tráfego, a qualidade do ar (monitorização ambiental), a utilização de energia, a gestão de resíduos, sistemas de rega, sistemas de saneamento, sistemas de águas, sistemas de iluminação pública, vídeo vigilância, entre outros.
- Plataforma de Mobilidade: uma plataforma de mobilidade digital ajuda a gerir o tráfego, otimizar o transporte público, oferecer informações em tempo real para os cidadãos sobre rotas e congestionamentos, e até mesmo promover soluções de mobilidade sustentável, como partilha de bicicletas e carros.
- Plataforma de Serviços Públicos, mais conhecidos nas autarquias como "Serviços Online": trata-se de uma plataforma digital para serviços públicos, a qual permite que os cidadãos acedam e interajam com os serviços municipais, e efetuem operações de pagamento de serviços, pedidos de licenciamento, solicitação de serviços municipais, etc.
- Plataforma de Energia: a gestão inteligente de energia é uma parte crítica de uma cidade inteligente. Plataformas de energia ajudam a monitorizar os consumos energéticos, promover a eficiência energética e integrar fontes de energia renovável.
- Plataforma de Segurança: para garantir a segurança dos cidadãos e da infraestrutura, as cidades inteligentes podem adotar plataformas de segurança que

incluem vigilância por vídeo, análise dos dados para identificação de anomalias e sistemas de alerta precoce.

- Plataforma de Participação do Cidadão: plataforma que permite a participação ativa dos cidadãos na tomada de decisões (ex.: Orçamento Participativo) e no fornecimento de resposta sobre o território (ex.: participação de incidentes nas vias e espaços públicos), é fundamental para a gestão eficaz dos serviços públicos.

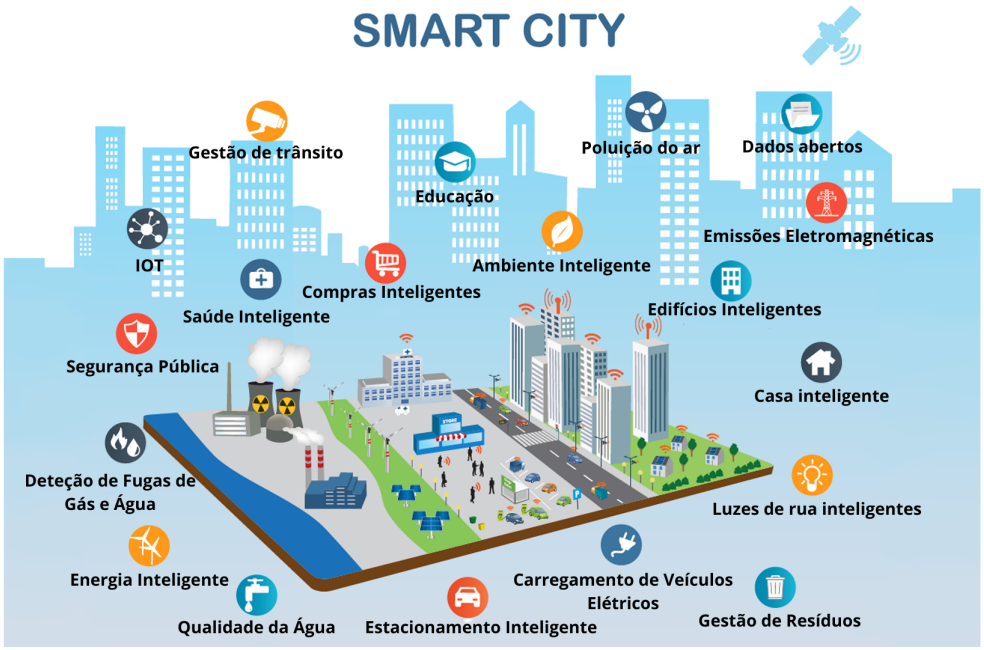


Figura 6: Componentes de uma Smart City. Fonte:DigitalSign, 2024

2.7 CIBERSEGURANÇA NOS MUNICÍPIOS

A cibersegurança abrange a identificação, prevenção, deteção e resposta a eventos cibernéticos, incluindo a recuperação subsequente. Esses eventos podem variar, desde a inadvertida divulgação de informação, até ataques direcionados ao comprometimento de infraestruturas críticas, bem como o roubo de identidades e dados pessoais. A lei relativa à cibersegurança (Segurança do Ciberespaço, 2018), define-a como "as atividades necessárias para proteger a rede e os sistemas de informação, os utilizadores desses sistemas e outras pessoas afetadas pelas ciberameaças".

Assim, a cibersegurança centra-se na segurança da informação, e procura manter a confidencialidade, integridade e a disponibilidade da informação, envolvendo atividades como, identificação, prevenção e resposta e recuperação de incidentes (CNCS, 2023).

A integração crescente da digitalização de processos e o aumento no uso das tecnologias da informação em todas as áreas de atuação dos municípios, criam um novo horizonte de possibilidades, mas, simultaneamente, aumenta o risco dos municípios serem alvos de cibercrime ou ataques cibernéticos, com os impactos, que daí podem advir.

O número de eventos de ciberincidentes está em ascensão, e verifica-se um notável aumento de incidentes significativos que impatam os municípios, representando uma tendência particularmente alarmante.

No último ano, conforme notícia divulgada nos meios de comunicação social em outubro de 2023, pelo menos quatro municípios foram impactadas por incidentes de grande relevância: Gondomar, Lagoa, Oliveira do Hospital e Odemira (Notícias, 2023). Posteriormente a esta notícia, foi conhecido mais um ciberataque ao Município de Alcanena.

O Coordenador do Centro Nacional de Cibersegurança (CNCS), autoridade nacional de cibersegurança, alertou, em outubro de 2023 (Forbes Portugal, 2023), que a transição digital, com mais serviços 'online' nas câmaras, está a aumentar os riscos de ciberataques e defendeu mais recursos e sensibilização das autarquias. Indicou ainda que "Esse movimento de digitalização tem que ser acompanhado com medidas e recursos atribuídos à cibersegurança para ter uma gestão eficaz do risco".

Admite também, que a transição digital, com a introdução de cada vez mais tecnologia, com as cidades inteligentes, na gestão de energia, mobilidade ou gestão de águas, tem exigência, e que este é o momento de fazer "um alerta" para a necessidade de equipar as autarquias de "mecanismos e medidas de cibersegurança desde a fase de conceção de projeto para mitigar estes riscos" (Forbes Portugal, 2023).

Para além de questões de conformidade legal e compliance, dado o aumento significativo no número de ciberataques e ao fato de se entender que a vulnerabilidade de um município pode representar ameaças à segurança de outras entidades e indivíduos, estas entidades têm de implementar mecanismos adequados para se protegerem contra ciberameaças e para isso é crucial a implementação de um SGSI.

2.8 SÍNTESE

Neste capítulo efetuou-se uma breve análise às principais características distintivas dos municípios, abordando as suas competências nas diversas áreas e o panorama nacional quando à dimensão, volume de negócios e estrutura orgânica.

Foram exploradas algumas das diferenças fundamentais entre municípios de grande, média e pequena dimensão, com enfoque nos desafios específicos que enfrentam os de menor dimensão, ao implementar um SGSI. Conclui-se que os desafios para um município de grande dimensão e de pequena e média dimensão são diferentes, e que estes segundos enfrentam, geralmente, restrições orçamentais e de recursos humanos para a área de cibersegurança. No entanto, apesar dessas diferenças, as preocupações com a cibersegurança são comuns a todos os tipos de municípios, e a implementação de um SGSI é essencial, dadas as suas responsabilidades.

Adicionalmente, verificou-se o conceito emergente de cidades inteligentes (smart city) e conclui-se que, pela quantidade de informação sensível e sistemas críticos, incluindo sistemas IoT, os municípios têm uma grande exposição a ameaças.

Por fim, abordou-se a importância crítica da cibersegurança como componente vital para proteger os ativos digitais dos municípios, concluindo com uma referência à atualidade, no que concerne ao número crescente de ciberincidentes nos municípios, e referência a várias recomendações emanadas pelo coordenador do CNCS, enquanto autoridade nacional de cibersegurança.

3

REVISÃO DA LITERATURA E DE CONCEITOS RELACIONADOS

No âmbito do presente capítulo, foi efetuada a revisão de alguns conceitos na área dos sistemas de gestão de segurança de informação e da norma ISO/IEC 27001, bem como, documentação existente acerca do QNRCS, que serão linhas orientadores para o plano de implementação do SGSI.

A temática referente à implementação de Sistemas de Gestão de Segurança de Informação nas organizações, com recurso às varias normas internacionais, nomeadamente, da ISO/IEC 27001 à ISO/IEC 27004, NIST SP 800-12/800-30/800-53/800-37, têm sido objeto de vários trabalhos e artigos académicos nos últimos anos. Este interesse, deve-se ao facto da segurança da informação ser uma preocupação crescente e essencial, para proteger os ativos e garantir o bom funcionamento das organizações nesta era digital.

Com o presente trabalho pretendeu-se enveredar por uma abordagem diferente dos diversos trabalhos académicos, que estudam as normas internacionais referidas no parágrafo anterior, e a sua aplicação a empresas e instituições num contexto mais geral, já que o mesmo será direcionado, para a definição de um plano de implementação, baseado no QNRCS e ferramentas associadas, e direcionado especificamente para o contexto e especificidade dos municípios de pequena e média dimensão.

Deste modo, a revisão da literatura incidiu também sobre as normas, regulamentos e legislação aplicável aos municípios.

Pretendeu-se com esta revisão de literatura obter uma base sólida para compreender, fundamentar e desenvolver de forma bem-sucedida o plano de implementação do SGSI proposto.

3.1 A NORMA ISO/IEC 27001 E A SEGURANÇA DA INFORMAÇÃO

A norma ISO/IEC 27001, é uma norma internacional que estabelece os requisitos para a implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI). Foi publicada pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC) para fornecer uma estrutura abrangente e sistemática para a gestão da segurança da informação em uma organização.

Esta norma estabelece os requisitos gerais para a implementação de um SGSI, e inclui a definição do contexto organizacional, a liderança e o comprometimento da administração das organizações, o envolvimento dos funcionários, a avaliação de riscos, a seleção e implementação de controlos de segurança, a monitorização e análise crítica do desempenho, e a melhoria contínua do sistema.

Ao implementar a norma ISO/IEC 27001, uma organização é capaz de estabelecer um conjunto de controlos de segurança da informação adequados, tendo com base uma prévia avaliação de riscos, para assim proteger os ativos de informação contra ameaças internas e externas. Esta norma pode ser aplicável a qualquer tipo de organização, independentemente da dimensão.

De forma sucinta, os principais benefícios que decorrem da implementação da ISO/IEC 27001 são:

- Aumento da segurança da informação: a norma fornece um conjunto de controlos abrangentes e eficazes para proteger os ativos de informação da organização.
- Conformidade regulamentar: auxilia as organizações a responderem a imposições legais, regulamentares e eventualmente contratuais, relacionados com a segurança da informação.
- Gestão de riscos: como a norma segue uma abordagem baseada em riscos, esta auxilia na identificação e mitigação dos riscos de segurança da informação.
- Melhor reputação: a implementação da norma demonstra o compromisso da organização em proteger as informações confidenciais e sensíveis.

De referir, que a ISO/IEC 27001 é uma norma genérica e não refere medidas de segurança específicas. Terá de ser quem está a operacionalizar, que deverá identificar e implementar os controlos de segurança relevantes, de acordo com as necessidades da organização e respetivo contexto. Segundo a norma ISO 27001, a Segurança da Informação, é a preservação da confidencialidade, integridade e disponibilidade da informação, de modo a garantir que esta esteja protegida contra acessos não autorizados, alterações indevidas, divulgação não autorizada, exclusão acidental

ou intencional, e ainda, garantir que os sistemas de informação estão disponíveis quando necessários.

Esta definição apresentada pela norma, tem como base os seguintes conceitos:

- Confidencialidade: garantia de que as informações são acedias apenas por pessoas autorizadas e que não são divulgadas a terceiros não autorizados.
- Integridade: garantia de que as informações são precisas, completas e protegidas contra alterações não autorizadas ou acidentais.
- Disponibilidade: garantia de que as informações e os sistemas de informação estão disponíveis quando necessários, bem como a capacidade de acedê-los e utilizá-los quando necessário.
- Gestão de Riscos: identificação, avaliação e tratamento dos riscos de segurança da informação, com a implementação de controlos apropriados, de modo a mitigar esses riscos.
- SGSI: estrutura de gestão estabelecida pela organização para gerir de forma abrangente a segurança da informação, incluindo políticas, processos, procedimentos, recursos humanos, tecnologias e controlos de segurança (*ISO/IEC 27001:2013* 2013).

3.2 GESTÃO DE ATIVOS DE INFORMAÇÃO

A Gestão de Ativos de Informação, constitui uma das atividades de um programa de segurança da informação. A gestão de ativos é um processo dinâmico que vai para além da simples inventariação de ativos. Deverá identificar e permitir listar os principais ativos informáticos de suporte às funções críticas, contendo informações relevantes do ponto de vista da cibersegurança e dependências funcionais com outros serviços críticos para a organização (QNRCS Centro Nacional de Cibersegurança, 2023).

Para uma gestão de ativos eficaz, as organizações deverão definir procedimentos, com controlos que garantam a atualização regular dos ativos, com determinada periodicidade ou sempre que ocorram alterações relevantes.

A Gestão de Ativos é importante para a área da cibersegurança porque também permite responder às normas e imposições legais em vigor (RJSE, 2021) e ainda para apoiar na gestão do risco associado aos referidos ativos.

A necessidade de uma Gestão de Ativos também decorre do objetivo de controlar o registo completo do ciclo de vida dos ativos e que agregue em simultâneo a gestão do ciclo de vida dos incidentes (InfoSec, 2023).

O inventário de ativos deve ser mantido atualizado com o registo de todos os ativos essenciais para a prestação dos respetivos serviços (InfoSec, 2023).

Os municípios são entidades abrangidas no âmbito de aplicação do Decreto-Lei n.º 65/2021 (RJSE, 2021), e devem, para além de outras obrigações, elaborar o inventário de ativos e apresentar ao CNCS uma lista de ativos elaborada com base no inventário.

As obrigações de comunicação e informação referentes ao inventário de ativos encontram-se agora previstas no Regulamento n.º 183/2022, de 21 de fevereiro (CNCS, 2022), quanto aos termos da comunicação de informação ao CNCS e formatação aplicável.

Nos termos do n.º 1 do artigo 4.º no Regulamento n.º 183/2022, de 21 de fevereiro, entende -se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.

Para cada ativo identificado, de acordo com o n.º 1 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho (RJSE, 2021), aplica-se o seguinte:

1. A entidade deve efetuar o inventário dos seus equipamentos de acordo com as seguintes regras:

a. Os dispositivos físicos e sistemas devem ser inventariados com a seguinte informação:

i. Número de inventário;

ii. Nome e modelo do equipamento;

iii. Número de série;

iv. Localização.

b. Os dispositivos ligados à rede devem ter a seguinte informação complementar:

i. Endereço IP;

ii. Endereço de hardware.

c. Os responsáveis dos dispositivos e sistemas devem ser identificados com, pelo menos, os seguintes elementos:

i. Nome;

ii. Contacto;

iii. Departamento.

d. Os dispositivos físicos e sistemas devem ser classificados de acordo com a sua criticidade para a entidade.

2. A entidade deve elaborar o inventário de todas as suas aplicações, identificando:

a. Informação necessária ao inventário de uma aplicação, nomeadamente:

i. Nome do software;

ii. Versão;

iii. Fabricante.

b. Os responsáveis pelas aplicações com, pelo menos, os seguintes elementos:

i. Nome;

ii. Contacto;

iii. Departamento.

c. A classificação em função da criticidade da aplicação para a entidade;

d. Quando aplicável, o tipo de contrato de suporte em vigor com o fornecedor da aplicação ou plataforma de software.

3.3 CONCEITOS RELACIONADOS COM SEGURANÇA DA INFORMAÇÃO

Este sub capítulo aborda alguns dos conceitos fundamentais relacionados com a segurança da informação, e que surgem no âmbito da implementação e desenvolvimento de um SGSI.

Riscos de Segurança da Informação e respetiva Avaliação

Relacionado com os Ativos de Informação, surge o conceito de Riscos de Segurança da Informação e Avaliação de Riscos. Os riscos de segurança de informação são ameaças potenciais que podem afetar a confidencialidade, integridade e disponibilidade dos ativos de informação. Os riscos são identificados e avaliados para determinar sua probabilidade e impacto, a fim de tomar medidas adequadas de mitigação. A Avaliação de Riscos, consiste no processo de identificação, análise e avaliação dos riscos de segurança da informação, tendo em consideração a probabilidade de ocorrência e o impacto potencial. Deste modo, conseguimos priorizar os esforços de segurança e determinar as medidas de controlo adequadas (NIST, 2012).

Controlos de Segurança da Informação

O conceito de Controlos de Segurança da Informação está relacionado com as defesas implementadas para mitigar os riscos de segurança da informação. Podem incluir medidas técnicas, organizacionais e procedimentais, como firewalls, criptografia, políticas de acesso, formação de consciencialização em segurança, entre outros (NIST, 2012).

Política de Segurança da Informação

No âmbito da implementação de um SGSI surge a necessidade de dispor de uma Política de Segurança da Informação, que consiste num documento que estabelece a intenção da organização em relação à segurança da informação. Este define as diretrizes gerais, os objetivos e os princípios de segurança que devem ser seguidos por todos os envolvidos na organização (NIST, 2012).

Consciencialização em Segurança da Informação

Um outro termo associado à temática de segurança da informação, é a Consciencialização em Segurança da Informação. Este processo consiste em educar e formar os funcionários no que concerne às práticas de segurança da informação. Isso inclui fornecer orientações sobre a utilização segura de sistemas, proteção de dados sensíveis, proteção de palavras passe, adoção de melhores práticas, detetar phishing e outras ameaças, cumprimento de regulamentação, entre outros aspectos relevantes (Boeira, 2023).

3.4 O QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA

No âmbito da missão do CNCS é criado o QNRCS (QNRCS Centro Nacional de Cibersegurança, 2023), em complemento à referida Lei n.º 46/2018 (regime jurídico de segurança no ciberespaço) (Segurança do Ciberespaço, 2018).

O QNRCS, é um documento guia, que está de acordo com as normas técnicas internacionais, sendo um precioso contributo na elaboração de um programa de segurança da informação.

O QNRCS encontra-se estruturado em objetivos de segurança e medidas de segurança (práticas de segurança de informação, através de um conjunto de medidas).

Em cada objetivo de segurança, define uma ou várias medidas de segurança (bem detalhadas e claras). Cada medida de segurança, tem categorias, divididas também em subcategorias, que tem controlos associados, para implementar a medida. Depois, são elencadas as evidências, para provar a implementação da medida.

As medidas de mitigação de risco referidas no QNRCS, exigem uma análise de risco prévia, que poderá ser auxiliada pela utilização do Guia para Gestão de Riscos, também disponibilizado pelo CNCS. Como resultado desta análise, as medidas a implementar variam de organização para organização, o que significa, que pode não ser necessário implementar todas as medidas indicadas no QNRCS.

3.4.1 *Quadro de Avaliação de Capacidades de Cibersegurança*

Na operacionalização de um programa segurança de informação com recurso ao QNRCS, serão verificados os cinco objetivos da Cibersegurança, conforme figura n.º 7, os quais consistem em identificar, proteger, detetar, responder e recuperar. Para cada objetivo serão descritas medidas de segurança correspondentes, contra ameaças que coloquem em causa a segurança do ciberespaço (QACC Centro Nacional de Cibersegurança, 2023).

Essas medidas definidas pelo QNRCS, na prática são evidências, ferramentas, aplicações ou documentos, que funcionam como prova de implementação das medidas de segurança.

Posteriormente, para verificarmos que evidências serão necessárias implementar, é possível verificar o Quadro de Avaliação de Capacidades de Cibersegurança (QACC) (QACC Centro Nacional de Cibersegurança, 2023), que é um documento complementar ao QNRCS.

No QACC são definidos três níveis de capacidade, para cada medida de Cibersegurança, para que seja possível às organizações o cumprimento dos cinco objetivos

Figura 7: Cinco objetivos da Cibersegurança. Fonte:QNRCS Centro Nacional de Cibersegurança, 2023

do QACC, tendo em conta o seu contexto e dimensão, conforme demonstrado na figura n.º 8:

NÍVEIS DE CAPACIDADE	DESCRIÇÃO	EVIDÊNCIAS
1 – Inicial	Medidas de segurança básicas que poderiam ser implementadas para alcançar o objetivo de segurança, nomeadamente em iniciativas *ad-hoc*, por iniciativas isoladas e pouco formais.	Evidência de implementação das medidas de nível Inicial.
2 – Intermédio	Medidas de segurança que atendem à maioria dos casos e necessidades para atingir os objetivos de segurança da informação. As medidas são atingidas formalmente.	Evidência de implementação das medidas de nível Intermédio.
3 – Avançado	Medidas de segurança avançadas que envolvem a monitorização contínua dos controlos, avaliação e revisão recorrentes, levando em consideração alterações, incidentes, testes e exercícios, para melhoria proativa das mesmas.	Evidência de implementação das medidas de nível Avançado.

Figura 8: Os 3 níveis de capacidade conforme o QACC. Fonte:QACC Centro Nacional de Cibersegurança, 2023

3.4.2 *Roteiro para as Capacidades Mínimas de Cibersegurança*

O CNCS disponibilizou também um documento denominado, Roteiro para as Capacidades Mínimas de Cibersegurança (R. Centro Nacional de Cibersegurança, 2023), complementar ao QNRCS, o qual apresenta um conjunto de ações, passo a passo, que se dividem em cinco fases, que podem ser implementadas por meios internos da organização ou externos.

Na primeira fase define-se a base da cooperação entre o CNCS e a organização e onde são indicados os canais de comunicação entre as duas entidades, bem como a identificação do âmbito dessa colaboração/articulação. Será preparado o quadro de

ameaças a que a organização poderá estar sujeita, calculando o valor relativo dos ativos, definindo áreas de segurança diferentes conforme o valor dos ativos. Também será identificada as dependências funcionais entre os vários sistemas internos, e as dependências entre estes sistemas e os sistemas geridos por terceiros.

Na segunda fase são definidas várias ações necessárias para ir de encontro com o âmbito definido na 1ª fase (definição da arquitetura de segurança e delimitar várias áreas de segurança e respetivas regras de controlo de acessos) e que visem dotar a organização com os principais recursos processuais e técnicas de base para uma defesa eficaz dos seus ativos (perímetro de rede, servidores, postos de trabalho e outros dispositivos). São ainda definidos sistemas processuais internos que garantam a conformidade essencial da organização com requisitos legais e normativos da sua área de atividade.

Na terceira fase, avança-se para a implementação dos desenhos de arquitetura de rede e defesas perimétricas elaborados na fase anterior, através da instalação de firewall, sistemas de deteção de intrusão em dispositivos e aplicações, nomeadamente Host-based Intrusion Detection Systems (HIDS), honeypots e controlo de acessos web (proxy). São implementados mecanismo de alertas de acesso indevidos a bases de dados e outros ativos de valor, alertas de falha de desempenho e disponibilidade de serviços. Nesta fase são efetuadas auditorias de segurança e ou verificações de supervisão, bem como a consolidação de informação de registo e monitorização num Sistema Integrado de Gestão de Eventos (SIEM).

Na quarta fase, procura-se criar procedimentos e políticas que otimizem as capacidades da equipa de cibersegurança, consolidar alguns processos e completar a formação dos recursos humanos (elaborar plano de formação individual), definir as responsabilidades pelas operações de cibersegurança, verificar as proteções a nível tecnológico de equipamentos que contenham ou permitam a circulação em rede de informação da organização. Nesta fase é ainda estabelecido a gestão de processos de mudança. Para muitas organizações de menor dimensão será a última fase deste processo de capacitação interna no domínio da cibersegurança.

A quinta fase, de avaliação conjunta entre a organização e o CNCS, é aplicável apenas a organizações de maior dimensão ou setores críticos, sendo que nesta fase são desenvolvidas ações para implementação de um Centro de Operações de Segurança (Security Operations Center - SOC).

Para além deste roteiro, o CNCS tem disponibilizado um conjunto de manuais de boas práticas no âmbito da Segurança das Redes e Sistemas de Informação, que consistem num conjunto de conceitos, informações e metodologias, que são complementos interessantes à definição dos requisitos técnicos mínimos de uma arquitetura de segurança das redes e sistemas de informação. Os referidos manuais

constituem uma boa base de trabalho para a elaboração dos seguintes planos, que devem incorporar o SGSI:

- Plano de políticas e procedimentos operacionais para operação segura das redes e sistemas de informação;
- Plano para a proteção dos dados e dos recursos de tratamento contra malware;
- Plano de gestão do ciclo de vida dos utilizadores
- Plano de registo e monitorização de atividade (logs);
- Plano para controlo dos sistemas em produção (atualizações);
- Plano para instalação de novo hardware e software;
- Plano para as cópias de segurança;
- Plano para os serviços de computação em nuvem;
- Plano para os suportes de dados (proteção, eliminação);
- Plano para a instalação e proteção dos equipamentos
- Plano de manutenção de equipamentos/sistemas;
- Plano para a subcontratação de serviços;
- Planos de emergência e de continuidade de negócio.

3.5 DEFINIÇÃO DO CONTEXTO E DO PROCESSO DE ANÁLISE DE RISCO

Antes de iniciar o processo de análise de risco tem de ser definido o Contexto, para compreender os critérios, decisões, recursos e matérias internas e externas relevantes para a missão da organização. Deve-se identificar nesta fase os recursos humanos e materiais que os irão garantir a correta execução do processo, tais como, ferramentas de suporte e processos para o tratamento do risco, bem como, o âmbito e fronteiras do processo de gestão de riscos que irá ocorrer, definindo e delimitando todos os pontos fronteira.

Após a definição do Contexto, temos de iniciar o processo de análise de risco. O guia para Gestão de Riscos Segurança da Informação e Cibersegurança (G. G. d. R. Centro Nacional de Cibersegurança, 2023), disponibilizado pelo CNCS, e que está atualmente em fase de recolha de contributos, constitui uma ferramenta interessante de apoio à realização de um processo de gestão dos riscos em matérias de segurança da informação e cibersegurança, permitindo implementar um Plano de Segurança da Informação, indo de encontro com as diretrizes do QNRCS.

Este documento direciona as organizações na escolha das medidas e controlos de segurança a definir e implementar, bem como no processo de análise, avaliação e tratamento periódico dos riscos.

No âmbito deste guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023), entende-se risco como "uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação", sendo identificados os diversos conceitos a ter em conta: ameaça, vulnerabilidade, impato e risco.

Assim, temos de começar por identificar possíveis ameaças que se possam explorar as vulnerabilidades dos ativos, bem como quais os níveis do risco associados, avaliando-se a probabilidade de ocorrência e possíveis impactos.

De referir ainda que a gestão do risco tem de ser efetuada de forma sistematizada e de acordo com um princípio de melhoria contínua, permitindo assim que as organizações identifiquem, quantifiquem e estabeleçam as prioridades em relação ao risco que estão dispostas a aceitar.

3.6 LEGISLAÇÃO E OUTROS NORMATIVOS APLICÁVEIS, NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO

Como referido no início deste capítulo, a revisão da literatura incidiu também sobre as normas, regulamentos e legislação aplicável aos municípios, no âmbito da Segurança da Informação, sendo de referir os seguintes normativos:

- Lei n.º 46/2018, de 13 de Agosto (Segurança do Ciberespaço, 2018) - Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu. Esta lei estabelece o regime jurídico para a segurança do ciberespaço em Portugal e define as obrigações e responsabilidades das entidades públicas e privadas em relação à segurança da informação e à proteção contra ameaças cibernéticas.
- Decreto-Lei n.º 65/2021, de 30 de julho (RJSE, 2021) - Este decreto-lei, transpõe a Diretiva Europeia 2016/1148, também conhecida como Diretiva NIS (Network and Information Systems). Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança. Este regulamento define um quadro legal de obrigações a cumprir no âmbito da Segurança da Informação, sendo de destacar, para o âmbito deste trabalho, a referência à Proteção de infraestruturas críticas, e como verificamos anteriormente, algumas destas poderão ser da responsabilidade dos municípios. O decreto-lei define as infraestruturas críticas e impõe medidas específicas de segurança para proteger essas infraestruturas vitais, como energia, água, saúde e transporte, contra ameaças de cibersegurança.
- Diretiva (UE) 2022/2555 (Diretiva NIS2) - Esta diretiva é uma atualização da Diretiva NIS de 2016, e tem o objetivo de reforçar a segurança das redes e sistemas de informação em toda a União Europeia, com enfoque em medidas de gestão do risco de cibersegurança, no alargamento do âmbito (sendo incluída a Administração Pública), na supervisão e aplicação de sanções mais severas, definição de diretrizes mais claras na comunicação de incidentes e na responsabilização dos órgãos de gestão.

  Esta diretiva surge em resposta ao aumento dos ataques de cibersegurança, e à necessidade de uma proteção mais robusta das infraestruturas críticas e dos serviços essenciais. Neste momento aguarda-se a transposição desta diretiva para a legislação nacional, com prazo limite de 17 de outubro de 2024, e depois, verificar como se concretizará no contexto nacional a referida regulamentação.
- Regulamento n.º 183/2022 (CNCS, 2022) - Regulamento que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança.

- Regulamento Geral sobre a Proteção de Dados 2016/679 (Conselho da União Europeia, 2016) - é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a na União Europeia e Espaço Económico Europeu.
- Lei relativa à Proteção de Dados Pessoais (Lei n.º 58/2019) (República, 2019a) - complementa o RGPD e estabelece regras específicas para o processamento de dados pessoais em Portugal. Regula o tratamento de dados pessoais por parte das entidades públicas e privadas, incluindo as autarquias locais. Embora esta lei tenha como foco principal a proteção dos direitos e privacidade dos titulares de dados pessoais, esta matéria está intrinsecamente ligada à segurança de informação, uma vez que a maioria das violações de dados ocorre devido a falhas no âmbito da cibersegurança. Os municípios no âmbito das suas competências legais tem acesso a um volume muito elevado de dados pessoais, dado que, frequentemente tratam informações pessoais de cidadãos numa variedade de contextos, como requerimentos municipais, pedidos de licenciamentos, serviços sociais e outras operações.

  As autarquias são obrigadas a cumprir as normas rigorosas da proteção de dados pessoais. Para isso, é necessária uma consciencialização sobre a privacidade de dados, na necessidade de conformidade, na implementação de medidas de segurança de informação e adotar uma abordagem transparente para o tratamento de informações pessoais.
- Resolução do Conselho de Ministros n.º 41/2018 (Resolução do Conselho de Ministros n.º 41/2018, 2018) - Diário da República n.º 62/2018. Define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais.

  Em anexo a esta Resolução constam os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado, incluindo assim os municípios.

  Alguns destes requisitos são de implementação obrigatória e outros de implementação facultativa.
- Recomendação nº 2/2022 - Conselho de Prevenção da Corrupção (Conselho Nacional de Cibersegurança, 2022) aprova recomendação sobre cibersegurança para entidades públicas. Este Conselho foi criado pela Lei n.º 54/2008, de 4 de setembro e é uma entidade administrativa independente, que funciona junto do Tribunal de Contas, tendo aprovado e publicado em Diário da Republica, uma recomendação sobre cibersegurança para as entidades públicas, alertando

para a necessidade de proteção contra ataques informáticos que "ponham em causa a confidencialidade, integridade e disponibilidade de informação".

- Lei n.º 59/2019 - Diário da República n.º 151/2019 (República, 2019b). Esta lei aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais. Esta lei poderá ser aplicável aos municípios que disponham de Polícia Municipal, com competências no âmbito da prevenção, investigação, deteção ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.
- Diretriz 2023/1, de 10 de janeiro da Comissão Nacional de Proteção de Dados (CNPD) (Comissão Nacional de Proteção de Dados, 2023). Esta norma é sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais, destinadas aos responsáveis pelos tratamentos e aos subcontratantes, pretendendo sensibilizá-los para as suas obrigações legais no domínio da segurança dos tratamentos e para a necessidade de realizarem um maior investimento nesta área.
- Resolução do Conselho de Ministros n.º 92/2019 - Diário da República n.º 108/2019 (Resolução do Conselho de Ministros n.º 92/2019, 2019). Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Trata-se de um documento orientador que estabelece as políticas, diretrizes e ações a serem implementadas em Portugal para garantir a segurança de informação e a proteção do ciberespaço no país. Esta estratégia foi desenvolvida para enfrentar os desafios crescentes no domínio da cibersegurança, garantindo que Portugal está preparado para lidar com ameaças de cibersegurança e proteger os sistemas de informação, dados e infraestruturas críticas.
- Despacho n.º 1124/2018 - Diário da República n.º 22/2018 (Ministros, 2018). Criação de um grupo de trabalho com o objetivo de estudar e propor um plano para a instalação de uma rede integrada de serviços públicos de comunicações interligando escolas e juntas de freguesia.

3.7 NORMAS E REGULAMENTOS INTERNOS

Os municípios dispõe de normas e regulamentos internos específicos, que são obrigados a cumprir, no exercício das suas responsabilidades e competências.

Alguns exemplos dessas diretrizes internas, que poderão de alguma forma ser relacionadas com a Segurança da Informação e implementação o SGSI, conforme veremos nos capítulos seguintes, são a Norma de Controlo Interno e o Plano de Gestão de Riscos de Corrupção e Infrações Conexas.

3.7.1 *Norma de Controlo Interno*

De acordo com Lei n.º 73/2013, de 3 de setembro, que estabelece a Lei-Quadro das Autarquias Locais, o Decreto-Lei n.º 192/2015, de 11 de setembro, que aprova o Sistema de Normalização Contabilística para as Administrações Públicas e a Lei n.º 75/2013, de 12 de setembro, que estabelece os princípios e objetivos do controlo interno das autarquias locais, uma Norma de Controlo Interno (NCI) é um documento que define os princípios, objetivos, políticas e procedimentos que as autarquias devem adotar para garantir a eficácia, eficiência e transparência da sua gestão.

O conteúdo da NCI reflete as especificidades de uma autarquia e abrange, pelo menos, as seguintes matérias:

- Organização e funcionamento dos serviços: a NCI define as estruturas organizacionais, as funções e responsabilidades das diversas unidades orgânicas da autarquia, bem como os circuitos de informação e comunicação.
- Procedimentos operacionais: a NCI estabelece os procedimentos operacionais a adotar nas diversas áreas de atividade da autarquia, nomeadamente nas áreas da gestão financeira, patrimonial, de recursos humanos e de contratação pública.
- Controlos internos: a NCI defini os mecanismos de controlo interno a implementar, tais como os controlos preventivos, os controlos de deteção e os controlos correctivos.

Com base na análise a várias normas de controlo interno de autarquias locais (Leiria, 2022a)(Soure, 2021) (Mirandela, 2020a), publicadas nos sítios das respetivas autarquias, geralmente, uma Norma de Controlo Interno de uma autarquia, tem a seguinte estrutura:

- Objetivo e âmbito – neste capítulo é definido o propósito geral da norma e específica a área ou processo a que se aplica.
- Princípios Fundamentais – capítulo onde são enumerados os princípios básicos que orientam o controlo interno, como legalidade, eficiência, eficácia, economia e transparência.
- Responsabilidades – neste capítulo são descritas as responsabilidades das diversas unidades orgânicas envolvidas na gestão dos recursos públicos.
- Procedimentos e Controlos – capítulo em que são definidos os procedimentos operacionais e controlos internos, que tem de ser adotados para garantir a conformidade com as normas legais e regulamentares.
- Gestão Financeira e Orçamental – neste capítulo são detalhados os procedimentos relacionados com a elaboração, execução e controlo da execução orçamental. Inclui regras que tem de ser seguidas para realizar aquisições de bens ou serviços, contratações e controlo da execução financeira.
- Contabilidade Pública – inclui um conjunto de normas de contabilidade, relacionadas com registo, controlo e prestação de contas.
- Património e Inventário – capítulo em que são descritas as regras para o controlo e gestão do património público, incluindo inventário, alienação e abate de bens.
- Transparência e Prestação de Contas - inclui regras para a divulgação de informação pública e prestação de contas.
- Auditoria Interna – neste capítulo é definida a estrutura e funcionamento do serviço interno de auditoria, responsável por avaliar a conformidade dos procedimentos e controlos estabelecidos pela norma.
- Sanções e Penalidades – de modo a assegurar o cumprimento da Norma, neste capítulo são definidos as consequências para o incumprimento, incluindo sanções e penalidades aplicáveis.
- Revisão e Atualização – neste capítulo são definidos os procedimentos para revisão e atualização periódica das normas, para que estejam adequadas às alterações legislativas e mudanças internas da autarquia.

A NCI é um documento que tem de ser aprovado pelo órgão executivo da autarquia, sendo objeto de revisão periódica, de modo a garantir a sua adequação às necessidades e aos objetivos da autarquia.

3.7.2 *Plano de Prevenção de Riscos de Gestão, incluindo os de Corrupção e Infrações Conexas*

Por imposição legal, através da Recomendação n.º 1/2009 de 1 de julho, do Conselho para a Prevenção da Corrupção, os municípios tem de dispor de um Plano de Prevenção de Riscos de Gestão, incluindo os de Corrupção e Infrações Conexas.

Um Plano de Prevenção de Riscos de Gestão, incluindo os de Corrupção e Infrações Conexas (PPRGIC) é um documento que define as medidas implementadas por uma autarquia para prevenir, detetar e corrigir riscos de gestão, incluindo os riscos de corrupção e infrações conexas.

O PPRGIC tem como objetivos contribuir para:

- Garantir a legalidade e a regularidade financeira e orçamental da gestão pública: o PPRGIC identifica os riscos de corrupção e infrações conexas, bem como as medidas a serem implementadas para mitigá-los.
- Assegurar a eficiência e a eficácia da gestão pública: o PPRGIC contribui para a racionalização dos recursos públicos e para a obtenção de resultados de acordo com os objetivos definidos.
- Promover a transparência da gestão pública: o PPRGIC contribui para a divulgação das informações relevantes sobre a gestão pública, de modo a permitir o seu controlo e fiscalização pelos cidadãos.

O conteúdo do PPRGIC refere, pelo menos, os seguintes capítulos:

- Âmbito: define o âmbito de aplicação, incluindo as atividades, áreas funcionais e unidades orgânicas abrangidas.
- Riscos: identifica os riscos de corrupção e infrações conexas, bem como a sua probabilidade e impacto.
- Medidas de prevenção: defini as medidas a serem implementadas para prevenir os riscos identificados.
- Medidas de deteção: defini as medidas a serem implementadas para detetar os riscos identificados.
- Medidas de correção: define as medidas a serem implementadas para corrigir os riscos identificados.
- Monitorização e avaliação: define o sistema de monitorização e avaliação das medidas implementadas. De referir que a elaboração do PPRGIC deve ser liderada pelo órgão executivo da autarquia, com a participação de todos as unidades orgânicas da autarquia. O PPRGIC deve ser aprovado pelo órgão

deliberativo da autarquia e deve ser objeto de revisão periódica, de modo a garantir que esteja adequado às necessidades e aos objetivos da autarquia.

Com base na análise a vários PPRGIC de autarquias locais (Leiria, 2022b) (Mirandela, 2020b) (Soure, 2016), publicadas nos sítios das respetivas autarquias, destacam-se algumas das medidas que são incluídas nesse tipo de documento, com interesse para a Segurança da Informação:

- Medidas de prevenção:
  - Formação dos colaboradores sobre os riscos de corrupção e infrações conexas;
  - Implementação de procedimentos de controlo interno, tais como a separação de funções e a auditoria interna;
  - Divulgação das informações relevantes sobre a gestão pública;
- Medidas de deteção:
  - Implementação de um sistema de denúncias;
  - Realização de inquéritos internos;
  - Medidas de correção;
  - Imposição de sanções aos colaboradores responsáveis pelos incumprimentos;
  - Encaminhamento dos casos para as autoridades competentes.

3.8 TRABALHOS RELACIONADOS

No que concerne a trabalhos relacionados com implementação de um SGSI, na pesquisa efetuada surgem muitos trabalhos de investigação, que estudam a adaptação dos padrões das normas da família ISO/IEC 27000 à realidade empresarial e de organizações, distanciado-se do objetivo pretendido com este trabalho.

Com este trabalho de investigação, pretende-se desenvolver uma abordagem mais simplificada e menos complexa do que os standards internacionais, e que vá de encontro com as diferenças e especificidades dos municípios de pequena e média dimensão, para assim conseguir reduzir alguns obstáculos de implementação.

Como referido por alguns autores, como (Smith, 2010), estes standards são demasiado abrangentes, complexos e onerosos, principalmente nas organizações mais pequenas, como poderá ser o caso dos municípios de pequena e média dimensão, deixando de parte as diferenças e especificidades das organizações, bem como os seus requisitos, normas e regulamentos. Neste sentido, este fato, pode levar a que o processo de implementação de um SGSI com estes standards se torne mais suscetível e falível durante a sua implementação. Este autor refere a importância de uma auto-avaliação para conhecer as especificidades da organização, bem como a importância de um âmbito e objetivos bem definidos. Indica a ainda, que deverão ser realizadas auditorias internas para avaliar metas e necessidades no que concerne à implementação do SGSI.

Para os municípios de pequena e média dimensão, será necessário desenvolver uma abordagem mais simplificada, para assim conseguir a redução de alguns obstáculos de implementação.

O trabalho de investigação de (Magalhães, 2023), com o tema Cybersecurity Ecosystem for Critical Infrastructures, tem como objetivo a construção de uma framework de cibersegurança abrangente para ser aplicada em contextos organizacionais que operam infraestruturas críticas, considerando não apenas aspetos técnicos, mas também os processos, políticas e as pessoas envolvidas na segurança da informação.

Este estudo vai de encontro com o pretendido com este trabalho, sendo um contributo muito interessante, dada a adaptabilidade para diferentes organizações, inclusive aos municípios de pequena e média dimensão. O mesmo, pretende resolver o problema da diversidade de frameworks, e do desafio na seleção e implementação dos controlos adequados, procurando criar uma framework eficaz. Inclui ainda informação com os vários passos para implementar um SGSI e referência às melhores práticas de como aplicar os controlos técnicos, indicando a framework Cyber Assessment (CAF), publicada em 2018 pelo National Cyber Security Center (NCSC)

e com foco na Diretiva NIS (Diretiva sobre Segurança das Redes e Sistemas de Informação - infraestrutura crítica da UE e dos serviços digitais essenciais), descrevendo indicadores específicos de boas práticas. Ainda relativamente a este trabalho de investigação, apenas uma nota para a falta de mecanismos para atualização da própria framework, seguindo um princípio de melhoria contínua.

Um outro trabalho de investigação, que também vai de encontro com a problemática deste trabalho, embora com uma visão mais ampla do tema, é a tese de mestrado de (Correia, 2016), a qual prepara a implementação de um SGSI no INEM, tendo como linhas orientadoras as normas da família ISO/IEC 27000. Este trabalho destaca a importância de SGSI num contexto organizacional, efetua a respetiva caraterização teórica, bem como o impato nos sistemas e tecnologias da informação. Define, embora de uma forma genérica, uma estrutura documental no âmbito segurança da informação, incluindo recursos e responsabilidades. Por fim, apresenta a Declaração de Aplicabilidade, organizada em várias áreas de intervenção, nas quais são definidas as medidas a implementar de acordo com os objetivos do INEM e respeitando as normas ISO/IEC 27001 e ISO/IEC 27002.

3.9 SÍNTESE

Com a revisão da literatura e dos conceitos relacionados com a segurança da informação, foram abrangidos diversos tópicos essenciais, proporcionando uma compreensão abrangente sobre o tema.

Verificou-se a norma ISO/IEC 27001, a qual estabelece requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), e fornece diretrizes para identificar, gerir e minimizar os riscos de segurança da informação numa organização.

Apresentou-se a temática da Gestão de Ativos de Informação, como um processo de identificação, classificação e proteção dos ativos de informação de uma organização, a qual dados, sistemas, hardware, software e outros elementos críticos para o funcionamento e segurança de uma organização. Vimos que a gestão eficaz desses ativos contribui para a mitigação de riscos e a preservação da confidencialidade, integridade e disponibilidade da informação. A Gestão de Ativos é importante para a área da Cibersegurança porque também permite responder às normas e imposições legais em vigor (elaborar o inventário de ativos e apresentar ao CNCS uma lista de ativos elaborada com base nesse inventário), para além de apoiar na gestão do risco associado a esses ativos.

Foram ainda descritos alguns conceitos relacionados com Segurança da Informação.

Realizou-se um estudo sobre o QNRCS e as várias políticas, diretrizes e práticas que o compõe, bem como recomendações, para garantir a resiliência contra ameaças de cibersegurança. Foi ainda estudado o Roteiro para as Capacidades Mínimas de Cibersegurança. O QNRCS, que está alinhado com normas técnicas internacionais, é um documento guia essencial para a elaboração de um programa de segurança da informação, e a documentação existente sobre o QNRCS servirá como linha orientadora para o plano de implementação do SGSI.

Estudou-se a definição do Contexto e do Processo de Análise de Risco, como componente fundamental na gestão de segurança da informação, e analisou-se o guia para Gestão de Riscos em Segurança da Informação e Cibersegurança, disponibilizado pelo CNCS, o qual constitui uma ferramenta de apoio à realização de um processo de gestão dos riscos em matérias de segurança da informação e cibersegurança, permitindo implementar um Plano de Segurança da Informação em conformidade com as diretrizes do QNRCS.

Apresentou-se o QACC, como uma ferramenta que permite avaliar a maturidade e eficácia das práticas de cibersegurança numa organização.

Por fim, verificaram-se os normativos e legislação específica, aplicável aos municípios, importantes para garantir a segurança da informação. Ainda neste âmbito, foram também estudadas as normas e regulamentos internos específicos das au-

tarquias, tais como, a NCI e o PPRGIC, fundamentais para alinhar o plano de implementação do SGSI com as necessidades das autarquias.

Conclui-se que existem normas gerais que tem de ser verificados pelos municípios na implementação do SGSI, tais como Lei relativa à Proteção de Dados Pessoais (Lei n.º 58/2019), e que também existem normas especificas que os municípios tem de respeitar, tais como, as normas relacionados com a gestão de serviços críticos essenciais, descritas no Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança e impõe medidas específicas de segurança para proteger infraestruturas vitais, entre outras.

Foram ainda analisados vários trabalhos de investigação relacionados com a implementação de um SGSI.

4

PROPOSTA DE PLANO DE IMPLEMENTAÇÃO DO SGSI

No presente capítulo, é apresentado o desenvolvimento da Proposta de Plano de Implementação do Sistema de Gestão de Segurança da Informação (SGSI).

Este capítulo apresenta de forma detalhada as etapas necessárias para a efetiva implementação do SGSI, tendo como base o QNRCS e ferramentas associados, e de acordo com as melhores práticas e normas internacionais de segurança da informação.

Propõe ainda um conjunto de documentos, considerados protótipos de políticas e normas de segurança de informação, direcionados para utilização numa autarquia de pequena e média dimensão.

4.1 NORMA DE CONTROLO INTERNO, PLANO DE GESTÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS E A IMPLEMENTAÇÃO DO SGSI

Para implementar um SGSI num município, é fundamental alinhar o sistema com as normas e regulamentos internos específicos da organização. A utilização da NCI e do PGRGIC, para a construção das políticas de um SGSI, poderá ajudar a garantir que estas políticas sejam eficazes e estejam devidamente alinhadas com as necessidades das autarquias.

Neste trabalho, alinhou-se um Plano de Implementação de um SGSI em consonância com as normas e regulamentos municipais, de modo a integrar os controlos de segurança da informação com os processos municipais existentes, e assim procurar garantir uma implementação mais direcionada e eficaz.

Procurou-se adaptar o plano de implementação do SGSI de modo a permitir responder aos requisitos específicos dos regulamentos municipais, incorporando normas e procedimentos normalmente definidos nesses documentos.

Assim, como trabalho preparatório à implementação do SGSI numa autarquia, será vantajoso analisar previamente as Normas e Regulamentos em vigor, de modo a serem integradas no processo de implementação do SGSI.

4.1.1 *Norma de Controlo Interno vs. SGSI*

Pelo estudo das várias componentes de uma NCI (subcapítulo 3.7.1), verifica-se alguma correspondência e interesse na utilização da NCI para a construção das políticas de um SGSI.

A NCI pode ser utilizada na construção das várias políticas que compõem um SGSI, nomeadamente nos seguintes âmbitos:

- Política de segurança da informação: Esta política estabelece os princípios e diretrizes gerais para a proteção da informação. A NCI pode ser alterada/atualizada para definir os objetivos e requisitos específicos para a segurança da informação nas autarquias.
- Política de gestão de riscos: Esta política estabelece o processo para identificar, avaliar e mitigar os riscos à segurança da informação. A NCI pode ser alterada/atualizada para definir os critérios para a avaliação dos riscos e para a implementação de medidas de mitigação.
- Política de gestão de incidentes: Esta política estabelece o processo para responder a incidentes de segurança da informação. A NCI pode ser alterada/atualizada para definir os procedimentos para a notificação, investigação e resolução de incidentes.
- Política de formação e sensibilização: Esta política estabelece o programa de formação e sensibilização para a segurança da informação. A NCI pode ser alterada/atualizada para definir os objetivos e conteúdos da formação e sensibilização.

4.1.2 *Plano de Gestão de Riscos de Corrupção e Infrações Conexas vs. SGSI*

Conforme verificado pelo estudo das várias componentes de um PGRCIC (subcapítulo 3.7.2), este plano é um documento importante para as autarquias, pois visa prevenir, detetar e corrigir riscos de gestão, incluindo os riscos de corrupção e infrações conexas, de forma similar a algumas medidas de um SGSI, que visam proteger a informação de uma organização contra ameaças e riscos.

O PGRCIC pode ser útil na construção das várias políticas que compõem um SGSI, nomeadamente nos seguintes âmbitos:

- Política de gestão de riscos: o PGRCIC pode ajudar a identificar os riscos específicos relacionados com a segurança da informação e a definir os critérios para a avaliação desses mesmos riscos.

- Política de formação e sensibilização: o PGRCIC pode ajudar a identificar as necessidades de formação e sensibilização dos colaboradores para a prevenção e pode ser um instrumento que pode ser utilizado para definir o programa de formação e sensibilização.

Da análise de vários PGRCIC, verifica-se que este é composto por uma matriz de risco, que têm a mesma estrutura básica da matriz de risco de um SGSI, incluindo pelo menos os seguintes pontos:

- Identificação do risco.
- Probabilidade do risco.
- Impacto do risco.
- Nível de risco.
- Medidas de mitigação.

A principal similaridade entre as duas matrizes é que ambas utilizam a mesma estrutura para avaliar a probabilidade e o impacto dos riscos.

No entanto, existem também algumas diferenças entre as duas matrizes. A matriz de risco para o PGRCIC é geralmente mais abrangente do que a matriz de risco para o SGSI. Isso ocorre porque o PGRCIC deve considerar todos os riscos que podem afetar a organização, incluindo os riscos de corrupção e infrações conexas, enquanto que a matriz de risco para o SGSI, é focada nos riscos que podem afetar a segurança da informação, com o objetivo de proteger a informação da organização contra ameaças.

4.2 ESTRUTURA DO PLANO DE IMPLEMENTAÇÃO

Na figura n.º 9, é apresentado o roadmap do plano de implementação do SGSI proposto neste trabalho. Este roadmap foi adaptado do roadmap típico de implementação de um SGSI, de acordo com a norma ISO 27001 (27001.pt, 2023), com algumas modificações específicas para se adequar ao cenário de uma autarquia de pequena e média dimensão.

Para otimizar o processo e simplificar a implementação numa autarquia de pequena e média dimensão, foram eliminadas algumas fases do roadmap utilizado como referência bibliográfica, tais como, a fase de Formação no âmbito da preparação do SGSI, a fase de Análise de GAP e a fase de Autoria interna.

Em substituição, entendeu-se introduzir novas fases que respondem melhor às necessidades e realidades deste contexto específico.

Duas dessas novas fases, são as seguintes:

- Reuniões/Trabalhos Preparatórios (fase 3): Esta fase envolve a organização de reuniões iniciais e a realização de trabalhos preparatórios essenciais. O objetivo é garantir um entendimento comum dos objetivos do SGSI, alinhar as expectativas dos participantes e preparar o terreno para as etapas subsequentes.
- Diagnóstico da Situação Atual (fase 4): Nesta fase, realiza-se uma avaliação da situação atual da autarquia em termos de segurança da informação. O diagnóstico é fundamental para identificar os pontos fortes e fracos do sistema existente e as áreas que necessitam de melhorias, fornecendo uma base sólida para delinear as etapas seguintes.

Na fase relacionada com a Operação do SGSI, foi eliminada a fase de Auditoria Interna prevista na norma, conforme já indicado no parágrafo anterior, pois considerou-se que numa autarquia de pequena e média dimensão, esta fase pode ser incorporada na fase de Testes, Análise e Revisão, e desta forma podemos otimizar recursos.

Finalmente, a fase de Certificação, embora entendida como uma fase importante no processo de implementação de um SGSI, foi excluída deste roadmap, uma vez que o foco deste trabalho está no plano de implementação do SGSI, e não na obtenção de certificação por um auditor independente.

Conforme verificado na figura n.º 9, a implementação de um SGSI tem várias etapas importantes, sendo que começa com a consciencialização e o comprometimento do Presidente da Câmara Municipal e/ou dirigente máximo da entidade.

Em seguida, segue-se a definição do âmbito e a criação de uma estratégia para gerir o próprio SGSI.

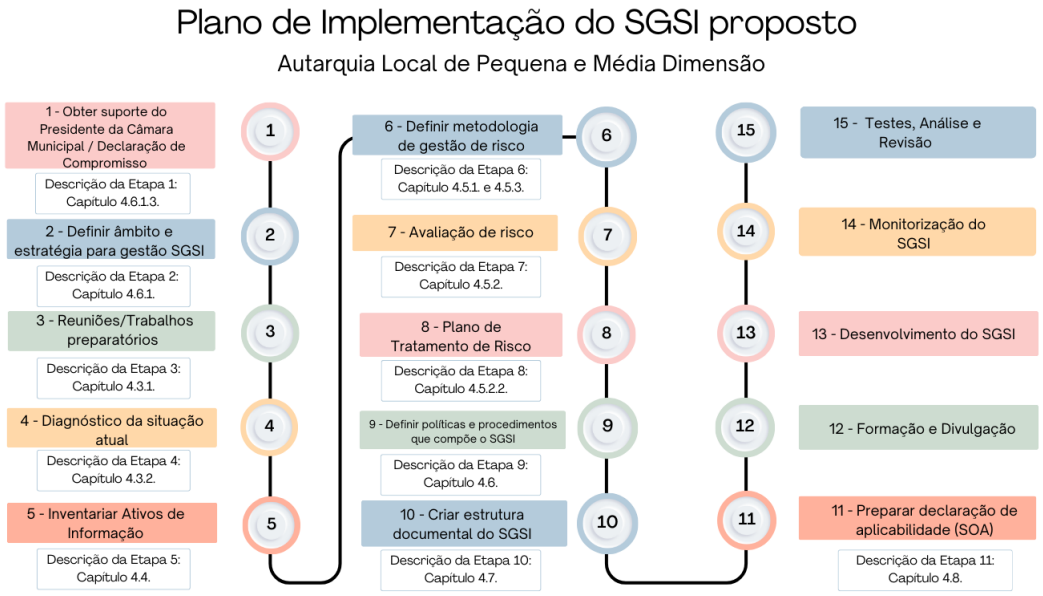


Figura 9: Estrutura do plano de implementação de um SGSI, numa Autarquia Local de Pequena e Média Dimensão

No seguimento serão necessárias reuniões de trabalho para definir trabalhos preparatórios, bem como fazer uma análise da situação atual da segurança da informação na organização, de modo a identificar lacunas e áreas de melhoria.

A fase seguinte envolve inventariação de ativos de informação, seguida pelas etapas de definição da metodologia de gestão, avaliação e tratamento de risco.

Posteriormente, avança-se para a criação de políticas, procedimentos e controlos de segurança da informação, personalizados de acordo com as necessidades e caraterísticas específicas da autarquia. Após esta fase, desenvolve-se a estrutura documental que integra o SGSI.

Paralelamente deverá ser preparada uma Declaração de Aplicabilidade, documento que descreve os controlos de segurança da informação selecionados pela autarquia e que indicam como estão a ser aplicados/implementados, para tratar os riscos de segurança de informação identificados.

A Declaração de Aplicabilidade, é uma ferramenta importante para auxiliar a autarquia a documentar e a comunicar o compromisso que detêm com a segurança da informação.

Seguidamente será investir em consciencialização e formação dos funcionários sobre práticas de segurança da informação, de modo a garantir que todos compreendem sua importância e a responsabilidade que cada um detêm neste processo.

Após a implementação das várias políticas e controlos, ou seja, o desenvolvimento do SGSI, é efetuada a monitorização e são realizados testes, efetuadas análises e recolhidos feedbacks internos, para identificar áreas de melhoria, e proceder à revisão, se necessário, de políticas e controlos.

Verificamos que o roadmap apresentado neste trabalho inclui um total de quinze etapas, no entanto, considerando os objetivos deste trabalho, são abordadas apenas as fases até à décima primeira etapa. As etapas subsequentes são referentes à Operação e Desenvolvimento do SGSI, que estão fora do âmbito deste estudo.

4.3 TRABALHOS PREPARATÓRIOS E DIAGNÓSTICO DA SITUAÇÃO ATUAL

Conforme referido no capítulo referente às Normas e regulamentos internos dos municípios, um dos trabalhos preparatórios para implementação do SGSI, será a recolha de informação relacionada com o funcionamento da autarquia.

Nesse âmbito, propõe-se no subcapítulo seguinte, um conjunto de pontos a serem abordados nas reuniões a realizar, assim como documentos internos a serem solicitados, bem como uma proposta de questionário estruturado, que poderá funcionar como guideline na implementação do SGSI.

4.3.1 *Trabalhos preparatórios*

Para o desenvolvimentos dos trabalhos preparatórios, os seguintes pontos e elementos, poderão ser abordados e solicitados, nas reuniões a realizar com os responsáveis das várias unidades orgânicas da autarquia:

- Identificação das áreas orgânicas, que servem a autarquia na sua missão e que são consideradas críticas;
- Levantamento da infraestrutura TICE e classificação dos ativos;
- Ligações contratuais/formais com entidades externas e respetivas áreas orgânicas;
- Serviços subcontratados no âmbito da infraestrutura dos sistemas e telecomunicações;
- Informação crítica e/ou sensível;
- Consequências prováveis na divulgação de certa informação por partes não autorizadas;
- Leis e regulamentos relacionadas com o tratamento de risco ou segurança da informação que se aplicam à autarquia.

Nessa mesma reunião, deverão ser solicitados também os seguintes documentos internos:

- Regulamentos e Normas internas da autarquia;
- Arquitetura Geral da Rede LAN/WAN;
- Lista de servidores e Aplicações (Serviços Aplicacionais);
- Lista de Equipamentos Ativos de Rede.

4.3.2 *Diagnóstico da situação atual*

Com o objetivo de efetuar uma verificação rápida do cenário atual, de modo a aferir em que nível se situa a autarquia na implementação das capacidades mínimas em cibersegurança, sugere-se o questionário de diagnóstico apresentado nas figura n.º 10, 11, 12, 13 e 14, o qual está estruturado em cinco capítulos, que correspondem com os cinco objetivos da Cibersegurança referenciados no QNRCS (QACC Centro Nacional de Cibersegurança, 2023), e que deverá ser respondido pelos responsáveis pelos Sistemas de Informação. Neste questionário, baseado na ferramenta CiberCheckUp (Centro Nacional de Cibersegurança de Portugal, 2022), produto complementar ao QNRCS, são formuladas várias questões específicas, para cada controlo de referência e respetivo objetivo.

Identificar

O primeiro capítulo ou objetivo, com a designação de Identificar, conforme figura n.º 10, consiste em definir o âmbito da abordagem da gestão do risco de cibersegurança, numa visão transversal à autarquia, no que concerne a todas as suas redes, sistemas de informação, pessoas, ativos, dados e processos/capacidades relevantes.

Assim, deverão ser conhecidos todos os recursos importantes e os respetivos riscos que lhes estão associados, conseguindo desta forma definir prioridades nos esforços a serem implementados.

Questões	Aplicado			Evidências	Localização
	Sim	Não	N/A		
1 - IDENTIFICAR					
1.1 A missão, visão, valores, estratégias e objetivos encontram-se definidos e comunicados?					
1.2 Os dispositivos físicos, redes e sistemas de informação da autarquia encontram-se inventariados?					
1.3 Os ativos necessários para a prestação de bens e serviços encontram-se classificados?					
1.4 Os ativos críticos estão identificados?					
1.5 As vulnerabilidades dos ativos encontram-se identificadas?					
1.6 As redes e sistemas de informação externos encontram-se identificados e catalogados?					
1.7 As redes e fluxos de dados são mapeados?					
1.8 As aplicações e plataformas de software são inventariadas?					
1.9 A política de segurança da informação está definida e comunicada?					
1.10 O processo de gestão de risco encontra-se definido?					
1.11 O plano de resposta e recuperação de desastre é exercitado com os fornecedores?					
1.12 As ameaças internas e externas são identificadas e classificadas?					
1.13 A autarquia partilha informações sobre ameaças em grupos de interesse?					
1.14 A gestão do risco é efetuada com base na análise de ameaças, vulnerabilidades, probabilidades e impactos?					
1.15 A estratégia de tratamento do risco encontra-se definida?					
1.16 Os requisitos legais e regulamentares para a cibersegurança são cumpridos?					
1.17 Os requisitos de resiliência para a prestação de serviços críticos estão definidos?					

Figura 10: Questionário referente à situação atual - Objetivo Identificar

Proteger

No objetivo proteger, e conforme figura n.º 11, implementam-se as medidas necessárias ou reforçam-se as existentes, de modo a assegurar a continuidade da prestação de serviços ou fornecimento de bens de determinada organização, no caso de ocorrência de um incidente de cibersegurança. Este reforço de capacidade, passa por implementar procedimentos, processos e tecnologias de proteção da informação, bem como, realização de formação interna, sensibilização para as questões da cibersegurança, entre outras medidas.

Questões	Aplicado			Evidências	Localização
	Sim	Não	N/A		
2 - PROTEGER					
2.1 São utilizados mecanismos de verificação para confirmar a integridade de software, firmware e dados?					
2.2 São realizadas, mantidas e testadas cópias de segurança dos dados da organização?					
2.3 São implementados mecanismos de resiliência em situações adversas?					
2.4 São implementadas proteções que evitem exfiltração de informação?					
2.5 Os utilizadores com acesso privilegiado compreendem quais são os seus papéis e responsabilidades?					
2.6 Os suportes de dados amovíveis são protegidos e a sua utilização é restrita de acordo com a política definida?					
2.7 Os sistemas estão configurados apenas com os serviços necessários?					
2.8 Os processos de proteção são melhorados continuamente?					
2.9 Os princípios de menor privilégio e segregação de funções são aplicados na Gestão de Acessos?					
2.10 Os planos de resposta e recuperação são testados e exercitados?					
2.11 Os dados são destruídos de acordo com a política definida?					
2.12 Os dados em circulação são protegidos?					
2.13 Os dados armazenados encontram-se protegidos?					
2.14 Os colaboradores têm formação em segurança da informação?					
2.15 Os ativos são geridos durante os procedimentos de remoção, transferência e aprovisionamento?					
2.16 Os acessos remotos são geridos?					
2.17 O ciclo de vida de gestão das identidades encontra-se definido?					
2.18 Existem registos de auditoria?					
2.19 Existem controlos de acesso físico para aceder às redes e sistemas de informação?					
2.20 Existe um processo de gestão de alterações?					
2.21 Está implementado o ciclo de vida de desenvolvimento seguro de software?					
2.22 É providenciada capacidade adequada para garantir a disponibilidade das redes e dos sistemas de informação?					
2.23 As vulnerabilidades dos ativos são geridas?					
2.24 As redes de comunicações e de controlo são protegidas?					
2.25 As manutenções remotas são revistas, aprovadas, executadas e registadas?					
2.26 As atividades de manutenção e reparação dos ativos da autarquia são realizadas e registadas em programas e planos aprovados e controlados?					
2.27 A integridade das redes de comunicações encontra-se protegida?					
2.28 A gestão de topo compreende as suas funções e responsabilidades?					
2.29 A configuração base de redes e sistemas de informação incorpora os princípios de segurança?					
2.30 A cibersegurança é contemplada nos processos de gestão de recursos humanos?					

Figura 11: Questionário referente à situação atual - Objetivo Proteger

Detetar

Neste objetivo, e conforme figura n.º 12, é dado enfoque à implementação de processos e mecanismos de deteção precoce de ocorrência de eventos de cibersegurança, com recurso à monitorização sistemática das redes e sistemas de informação.

Questões	Aplicado			Evidências	Localização
	Sim	Não	N/A		
3 - DETETAR					
3.1 Os processos de deteção são testados?					
3.2 Os eventos são coletados e correlacionados a partir de várias fontes e sensores?					
3.3 Os eventos detetados são analisados para se identificarem os alvos e os métodos de ataque?					
3.4 Os ambientes físicos são monitorizados para se detetar potenciais incidentes de segurança?					
3.5 O impacto dos eventos é classificado?					
3.6 O código malicioso é detetado?					
3.7 Estão definidos os papeis e as responsabilidades na deteção de eventos anómalos?					
3.8 As vulnerabilidades dos ativos são detetadas automaticamente?					
3.9 As redes e sistemas de informação são monitorizados para detetar potenciais incidentes?					
3.10 As deteções de eventos são comunicadas?					
3.11 As atividades dos prestadores de serviços são monitorizadas?					
3.12 As aplicações não autorizadas em dispositivos móveis são detetadas?					
3.13 A atividade dos colaboradores é monitorizada para se detetar potenciais incidentes?					

Figura 12: Questionário referente à situação atual - Objetivo Detetar

Responder

Com este objetivo, e conforme figura n.º 13, o resultado a atingir, será verificar se a autarquia está capacitada com a implementação de práticas que se traduzam em ações de resposta a incidentes de cibersegurança detetados. Com estes procedimentos, de planeamento de resposta a incidentes, de comunicação com as partes interessadas relevantes, da análise e mitigação de incidentes, a autarquia deverá estar pronta a conter os impatos de um potencial incidente.

Questões	Aplicado			Evidências	Localização
	Sim	Não	N/A		
4 - RESPONDER					
4.1 São realizadas análises forenses?					
4.2 Os planos de resposta são executados durante ou após a ocorrência de um incidente?					
4.3 Os incidentes são mitigados?					
4.4 Os incidentes são contidos?					
4.5 Os colaboradores conhecem as suas responsabilidades na resposta a um incidente?					
4.6 O impacto dos incidentes é avaliado?					
4.7 Existem processos para receber, analisar e responder a vulnerabilidades provenientes de fontes internas e externas?					
4.8 Existem critérios para reportar incidentes?					
4.9 Existe partilha voluntária de informação com partes interessadas externas?					
4.10 As vulnerabilidades identificadas são mitigadas ou documentadas como riscos aceites?					
4.11 As notificações dos sistemas de deteção são investigadas?					
4.12 As informações são partilhadas de acordo com o plano de resposta?					
4.13 A coordenação com as partes interessadas ocorre conforme os planos de resposta?					

Figura 13: Questionário referente à situação atual - Objetivo Responder

Recuperar

O objetivo recuperar, conforme figura n.º 14, consiste em criar e operacionalizar um conjunto de boas práticas, bem como manter um plano de resiliência (planos de continuidade do negócio e de recuperação) que assegurem o restauro de alguma capacidade e/ou serviço que tenha sido comprometido por um evento de cibersegurança, minimizando os impactos negativos na autarquia do referido evento.

Questões	Aplicado			Evidências	Localização
	Sim	Não	N/A		
5 - RECUPERAR					
5.1 Está implementado um plano de comunicação?					
5.2 As atividades de recuperação são comunicadas às partes interessadas, internas e externas, bem como às equipas executivas e de gestão?					
5.3 A autarquia segue um plano de recuperação durante ou após um incidente?					

Figura 14: Questionário referente à situação atual - Objetivo Recuperar

4.4 GESTÃO DE ATIVOS

Neste subcapítulo são abordadas as estratégias e práticas essenciais para a administração eficaz dos ativos de uma organização, como um município.

Inicialmente, discute-se "O desafio da gestão de ativos nos municípios", destacando as complexidades e particularidades enfrentadas pelos municípios neste processo.

Posteriormente, explora-se o "Processo de gestão dos ativos de informação", onde são delineadas as etapas e metodologias necessárias para a execução do mesmo.

4.4.1 *O desafio da gestão de ativos*

No âmbito da implementação de um programa de segurança de informação, não conseguimos proteger determinado ativo se não soubermos que ele existe.

Segundo a Gartner, cerca de 70% das organizações apresentam uma discrepância de aproximadamente 30% entre o inventário planeado e o inventário atual (Security, 2023) e os municípios não estarão imunes a este cenário. Para além disso, estão a enfrentar atualmente um aumento significativo no número de ativos de IoT, impulsionado por projetos como a Estratégia Nacional de Smart Cities (Digital, 2023).

Face às imposições legais e também à necessidade de manter planos de segurança de informação que incluam informação atualizada e em tempo real de todos os ativos, a temática da gestão de ativos em cibersegurança, tem tido a atenção das empresas e organizações nos últimos tempos, verificando-se atualmente um maior investimento por partes das empresas e organizações nesta área.

Nas empresas e organizações de maiores dimensões, desde sempre existiu a preocupação de gestão de ativos por parte das equipas internas de TI, que fazem a administração de hardware, mas nos municípios mais pequenos esta atenção pode não ocorrer.

Nos últimos anos, esta gestão de ativos tem vindo a evoluir, para assegurar a execução das competências do responsável de segurança de informação (Gabinete Nacional de Segurança, 2016), sendo mesmo, considerada a espinha dorsal de um plano de segurança de informação.

Uma das atividades essenciais da Gestão de Ativos, que é referida pela NIST Cybersecurity Framework (conjunto de diretrizes e práticas recomendadas para ajudar as organizações a construir e melhorar sua postura de segurança), com a designação de função Identificar, é estabelecer as bases para um programa eficaz de segurança de informação. Uma dessas atividades inclui identificar ativos físicos

e de software, e Identificar as vulnerabilidades de ativos, bem como as ameaças a recursos da organização internos e externos.

A gestão de ativos torna-se um desafio cada vez maior para os municípios, dada a atual transformação que vemos a ocorrer nas infraestruturas digitais destas entidades, e ao conjunto de novas competências que têm vindo a assumir nos últimos anos.

Para se conseguir tratar de forma eficaz os problemas de segurança, os municípios necessitam de um inventário abrangente e confiável.

Verificamos ainda, com o crescente desempenho de funções em regime de teletrabalho ou em regime híbrido, que os municípios têm ativos cada vez mais diversificados (incluindo equipamentos cedidos pelos próprios funcionários) e que com regularidade são desenvolvidas ou adquiridas novas plataformas, integrados novos dispositivos IoT, etc.

Acresce a esta problemática, o fato destes ativos estarem cada vez mais distribuídos, sendo assim mais difícil o processo de inventário e gestão.

4.4.2 *Processo de gestão dos ativos de informação*

Conforme referido no capítulo anterior, com a atual transformação que vemos a ocorrer nas infraestruturas digitais dos municípios, as vulnerabilidades que podem ser exploradas por diversas ameaças e, assim, comprometer os sistemas de informação destas entidades, são cada vez maiores. Assim, torna-se imperativo, mensurar e gerir riscos, para garantir que as informações relevantes, estratégicas e confidenciais estejam protegidas, e ao mesmo tempo, assegurar que a imagem, reputação e valor de mercado da autarquia fiquem protegidos. Para colmatar esta situação necessitamos de uma gestão de ativos que inclua o respetivo risco. Neste subcapítulo, iremos verificar como o risco pode se incluído numa gestão de ativos.

A norma ISO 31000, define risco como o "efeito da incerteza no alcance dos objetivos da organização". No âmbito deste trabalho e no contexto de Segurança da Informação, essas incertezas estão relacionadas com as vulnerabilidades que podem existir em ativos (informação digital ou física, hardware, software, pessoa ou ambiente físico). Podemos considerar o risco, como o resultado obtido quando uma potencial ameaça passa a explorar as vulnerabilidades que estão presentes num ou mais ativos de informação, e que podem trazer impatos significativos e negativos ao funcionamento e continuidade do negócio da organização.

O processo de identificação dos riscos existentes, terá de ser precedido de uma análise de riscos de segurança da informação, que consiste em detetar vulnerabilidades e ameaças e avaliar os possíveis impatos aos ativos da organização, para depois, ajudar na adoção dos melhores controlos necessários para os proteger.

Devemos considerar como ativo todos elementos que agreguem valor ao negócio/atividade da autarquia, tais como, informação digital ou física, hardware, software, pessoa ou ambiente físico, e cuja quebra da confidencialidade, integridade ou disponibilidade pode trazer prejuízo/dano, e assim deve ser protegido de forma adequada.

4.4.2.1 *Operacionalizar a gestão dos riscos dos ativos*

O risco dos ativos pode ser incluído na gestão de ativos, atribuindo um nível de severidade a cada ativo, que irá variar de Informativo para Crítico e podendo ainda atribuir uma pontuação de risco (score). Essa severidade varia, e terá de ser definida de acordo com o ambiente e regras de negócio previamente definidas. A severidade de um ativo tem de representar a importância do ativo para a autarquia. A título de exemplo, um servidor Active Directory normalmente tem uma severidade Crítica. Pelo contrário, uma impressora na maioria das instituições possui uma severidade Baixa.

Ao efetuarmos a Gestão de Ativos, podemos criar um grupo de ativos, e a cada grupo de ativos atribuir uma determinada severidade. Deste modo, permite focar e isolar determinadas áreas ou processos de negócio da instituição. Por outro lado, conseguimos ainda ter uma visão segmentada da evolução do programa de segurança de informação e definir prioridades nos esforços que devemos dedicar os ativos com maior nível de severidade.

Para efetuarmos estes processos de gestão de ativos e respetiva gestão do risco, devemos investir numa plataforma adequada, para obtermos ganhos de eficiência na priorização das nossas ações em consonância com as necessidades e os objetivos da instituição.

Registo atualizado de localização dos equipamentos

É necessário dispor de uma forma de rastrear os equipamentos, porque caso um ativo seja extraviado ou desativado, podemos ter de adotar medidas de proteção. Por exemplo, quando um ativo é solicitado, a gestão de ativos deve dispor de campos que identifiquem para quem o ativo vai ser cedido, a localização futura do ativo, o modelo do ativo solicitado, o intervalo de datas previsto para utilização e o motivo ou a justificação para a necessidade desse ativo.

Este rastreamento irá permitir saber quem deve estar na posse de determinado ativo, quem o tem na sua posse, e que ativos estão disponíveis.

Registo de dados financeiros e de contratos

Para uma gestão de ativos de TI completa, a plataforma que irá permitir operacionalizar essa mesma gestão, deverá dispor de campos que permitam guardar

informação relativa a dados financeiros (relacionadas com as faturas de compras), e de contratos associados aos ativos.

Categorias de ativos de TI

Os ativos de TI, de uma forma geral enquadram-se nas seguintes categorias: físicos, software, hardware, tecnologia móvel, IOT, e cloud.

Na gestão de ativos de TI, os principais tipos são:

- Software - envolve registo de software instalado em computadores, licenças de software, e caraterísticas como, requisitos de conformidade, licenciamento. Os ativos de software têm de ser monitorizados e revistos de forma contínua.
- Hardware - estes ativos físicos incluem computadores, impressoras, fotocopiadoras, notebooks, dispositivos móveis, servidores e todo o tipo de hardware utilizado nos sistemas de informação da instituição.
- Cloud - inclui SaaS (Software as a service, software como serviço), IaaS (Infrastructure as a service, infraestrutura como serviço) e PaaS (Platform as a service, plataforma como serviço). Todos estes recursos são considerados ativos que tem de ser geridos, nomeadamente, em termos de conformidade.

4.4.2.2 *Gerir o ciclo dos ativos*

Num programa de segurança de informação temos de garantir o rastreio do ciclo de vida completo dos ativos de TI, e com uma Gestão de Ativos conseguimos assegurar esse procedimento.

O ciclo de vida de um ativo de TI pode ser dividido em 6 etapas, embora, cada município possa definir um ciclo diferente:

1. Requisição interna/Proposta de Despesa;
2. Aquisição (requisição externa);
3. Instalação;
4. Monitorização;
5. Manutenção;
6. Eliminação.

Resumidamente, o ciclo começa com a manifestação da necessidade (requisição interna). Nesta fase, são definidos aspetos importantes, como os ativos que são necessários, como adquirir e como serão utilizados.

Depois entra a fase de aquisição, onde é efetuada a compra do ativo (requisição externa), aquisição do serviço (locação de software) ou aquisição de licenciamento do ativo.

Posteriormente ocorre a instalação, em que é supervisionada a instalação do ativo.

Uma vez em produção, inicia-se a fase de monitorização, que verifica se os ativos estão a funcionar de forma eficaz.

Na fase seguinte, a manutenção, os ativos são atualizados e sujeitas a manutenção preventiva, para prolongar a respetiva vida útil.

Por fim, temos a fase de eliminação, que ocorre quando os ativos deixam de ser necessários, e em que são desativados e eliminados. Nesta última fase, tem de se fazer a transição de utilizadores para ativos alternativos, atualizar os registos, cancelar eventuais contratos ou rescisão de licenças e limpeza de todos os dados que possam estar armazenados no mesmo.

4.5 INSTRUMENTO PARA O PROCESSO DE ANÁLISE DO RISCO

Conforme referido na Lei n.º 46/2018, de 13 de agosto, relativa ao Regime Jurídico da Segurança do Ciberespaço, entende-se risco como "uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação", sendo identificados na referida lei os diversos conceitos a ter em conta: ameaça, vulnerabilidade, impato e risco.

A Gestão de Risco é definida como o processo através do qual as organizações analisam metodicamente os riscos inerentes às respetivas atividades, com o objetivo de atingirem uma vantagem sustentada em cada atividade individual e no conjunto de todas as atividades.(Associações de Gestão de Riscos, 2003)

A Estrutura da Gestão de Risco é definida como um conjunto de elementos que fornecem os fundamentos e disposições organizacionais, para conceber, implementar, monitorizar, rever e melhorar continuamente a gestão do risco em toda a organização.(Qualidade, 2009)

A gestão do risco desempenha um papel fundamental na condução da estratégia de qualquer organização, com o objetivo de agregar valor, especialmente ao impulsionar um desenvolvimento consistente e controlado. Isso traduz-se na melhoria das decisões, do planeamento e na definição de prioridades, resultando numa utilização mais eficiente dos recursos e na otimização da eficiência operacional. Além disso, a gestão do risco visa reduzir a incerteza e volatilidade, contribuindo para a proteção dos ativos, e ainda, melhorar a imagem da organização.

O cerne de uma gestão eficaz de riscos reside na identificação e tratamento desses riscos, visando consistentemente agregar valor a todas as atividades da organização.

Para alcançar esse objetivo, a gestão de riscos deve funcionar como um processo contínuo e em constante evolução, alinhado com a estratégia da organização e à implementação dessa mesma estratégia.

Deve ser efetuada uma análise metódica de todos os riscos associados às atividades passadas, presentes e, especialmente, futuras da organização.

A gestão de riscos deve ser integrada na cultura da organização e o programa deve ser conduzido pela direção de topo.

Pretende-se, nos subcapítulos seguintes, apresentar um instrumento orientador para a gestão do risco e de suporte ao planeamento e tomada de decisões, e estabelecer um conjunto de métodos e passos, direcionados para diminuir a probabilidade de ocorrência de situações de risco e/ou prevenir e mitigar o seu impato, e assim reduzir ao máximo o efeito desses riscos.

4.5.1 *Definição do contexto da análise de risco*

Antes de iniciar o processo de análise de riscos propriamente dito, deve-se definir o Contexto da mesma, para compreender os critérios, decisões, recursos e matérias internas e externas relevantes para a missão da autarquia. Num cenário de implementação, deve-se identificar nesta fase os recursos humanos e materiais que irão garantir a correta execução do processo, tais como, ferramentas de suporte e processos para o tratamento do risco, bem como, o âmbito e fronteiras do processo de gestão de riscos que irá ocorrer, com o objetivo de definir e delimitar todos os pontos fronteira.

Conforme já referido neste estudo no capítulo referente à Revisão de Literatura, o guia para Gestão de Riscos Segurança da Informação e Cibersegurança disponibilizado pelo CNCS (G. G. d. R. Centro Nacional de Cibersegurança, 2023) , constitui uma ferramenta interessante de apoio à realização de um processo de gestão dos riscos em matérias de segurança da informação e cibersegurança.

Seguindo o referido guia, verificamos que o processo de análise de risco, poderá ter subjacentes as seguintes fases: Levantamento de Riscos, Tratamentos dos Riscos, Comunicação e Consulta do risco, Monitorização e Revisão dos riscos.

Nesse sentido, nos subcapítulos seguintes, apresenta-se uma metodologia para elaborar o processo de análise do risco numa autarquia.

4.5.2 *Processo de Análise de Riscos*

Ao longo dos próximos subcapítulos, são detalhadas as etapas necessárias para identificar, avaliar, tratar e monitorizar os riscos que podem impactar uma organização.

No subcapítulo "Processo de Levantamento de Riscos", são discutidas as metodologias utilizadas para identificar, analisar e avaliar possíveis ameaças e vulnerabilidades.

Em seguida, no "Processo de Tratamento do Risco", são exploradas as estratégias para mitigar, transferir, aceitar ou evitar os riscos identificados, que se materializam na implementação de um ou mais planos de ação, que servem para documentar as opções de tratamento que foram selecionadas e de que maneira, e em que ordem deverão ser implementadas.

O subcapítulo "Comunicação e Consulta do Risco"destaca a importância de envolver todas as partes interessadas através de uma comunicação eficaz, através do plano de comunicação e consulta do risco.

Finalmente, em "Monitorização e Revisão dos Riscos", são apresentados os mecanismos para acompanhar continuamente os riscos e rever as estratégias adotadas.

4.5.2.1 *Processo de levamento de riscos*

Nesta fase, devemos identificar, reconhecer, quantificar e descrever os riscos. O objetivo é avaliá-los e priorizá-los de acordo com a perceção que temos da sua gravidade e com outros critérios estabelecidos.

O levantamento dos riscos pode ser efetuado nas seguintes três etapas: identificação do risco, análise do risco e avaliação do risco.

Etapa 1 - Identificação do risco

Na primeira etapa, denominada identificação do risco, pretende-se determinar as ocorrências que poderão causar uma potencial perda à organização e deixar bem definido como, onde e porquê esta perda pode acontecer.

O guia sugere para a identificação do risco, os seguintes exemplos:

- Análise de vulnerabilidades internas e externas;
- Brainstorming com os recursos envolvidos nos processos avaliados;
- Questionários com gestores ou responsáveis pelos processos avaliados;
- Análise de cenários de ameaça internas e externas;
- Oficinas de avaliação de riscos (workshops);
- Investigação de incidentes de cibersegurança;
- Auditorias de segurança;
- Comunicação com fornecedores, parceiros e clientes;
- Avaliações de riscos de segurança da informação e cibersegurança.

Para identificamos o risco é imprescindível efetuarmos um processo de identificação e valorização de ativos.

Todas as organizações devem dispor de um inventário de ativos. Nesse inventário são registadas dados relevantes dos ativos, bem como os respetivos responsáveis.

Uma forma de determinar a criticidade dos ativos é avaliar o valor de reposição, incluindo custos de recuperação, limpeza ou substituição da informação.

Outro ponto importante é a identificação das ameaças. Como vimos, uma ameaça pode criar impactos e consequências negativas nos ativos da organização.

Recorrendo ao guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023), a informação sobre possíveis ameaças pode ser obtida das seguintes formas:

- Revisão de incidentes ocorridos;
- Auscultação do responsável pelo ativo;
- Perceção dos utilizadores;
- Pareceres de especialistas de segurança da informação e segurança física;
- Informações dos departamentos jurídicos;
- Informação veiculada através de meios de comunicação;
- Informação comunicada por instituições públicas e/ou outras com relevo para a segurança da organização ou nacional;
- Catálogo de ameaças comuns;
- Catálogo de ameaças da sua área de atuação.

No âmbito do levantamento dos riscos, temos de efetuar uma identificação dos controlos existentes. Temos de levar em consideração, que um controlo ou vários, que estejam incorretamente implementados podem converter-se em potenciais vulnerabilidades para a organização.

Assim, será de verificar a eficácia dos controlos implementados, tais como as medidas de segurança documentadas no QNRCS (QNRCS Centro Nacional de Cibersegurança, 2023), organizadas através dos cinco objetivos, de Identificar, Proteger, Detetar, Responder e Recuperar.

Neste âmbito, tendo como referência o guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023), as atividades que podem ser desenvolvidas são:

- Revisão de documentos que contenham informações sobre a implementação dos controlos;
- Verificação junto dos responsáveis pela segurança da informação e cibersegurança (por exemplo: CISO) sobre quais são os controlos que se encontram efetivamente implementados;
- Realização de uma avaliação presencial, no local, para aferir a implementação dos controlos físicos,
- Comparando os que estão devidamente implementados com a lista dos controlos que deveriam estar e, verificando entre os implementados, se estes se encontram correta e eficazmente operacionalizados.

Por fim, será de efetuar a identificação das vulnerabilidades. Uma vulnerabilidade é um ponto fraco de um ativo ou de um controlo. No referido guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023), encontramos descritas um conjunto de vulnerabilidades catalogadas, de forma a auxiliar a sua utilização no processo de gestão dos riscos.

Etapa 2 - Análise do risco

Nesta segunda etapa do processo de levantamento de riscos, denominada análise do risco, temos de verificar a origem dos riscos identificados na etapa anterior, as consequências, impactos e probabilidade de ocorrência.

A metodologia usada para esta análise do risco, pode ser analítica, com caráter qualitativo, quantitativo ou por uma combinação de ambas.

Os critérios a utilizar para definir a probabilidade e impacto dos riscos, deve ser associado ao contexto definido inicialmente, em linha com os objetivos de negócio da organização, e os objetivos particulares de gestão de riscos.

A determinação do nível de risco é efetuada relacionando o potencial impacto dos riscos ao negócio e a probabilidade de materialização desses riscos. Finalmente, conforme referido no guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023), o nível do risco poderá ser representado de acordo com a seguinte escala:

- 5 – Muito alto;
- 4 – Alto;
- 3 – Médio;
- 2 – Baixo;
- 1 – Muito baixo.

Esta definição possibilita que se estabeleça uma ordem de priorização para o tratamento dos riscos críticos, de acordo com o nível que receberem.

No caso particular dos municípios que podem ser Operadores de Serviços Essenciais, por prestarem um serviço essencial (ex. abastecimento de água), verifica-se que uma falha ou interrupção de um serviço essencial terá um impacto mais relevante ou substancial na sociedade, pelo que o Guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023) propõe a utilização de uma Matriz de Riscos mais conservadora.

Etapa 3 - Avaliação dos riscos

A última etapa do processo de levantamento de riscos é a avaliação dos riscos. Nesta etapa, o objetivo é auxiliar na tomada de decisão sobre o tratamento dos riscos, baseando-se principalmente na premissa de um nível aceitável dos riscos, permitindo decidir de forma consciente o tratamento que deve ser usado a cada um dos riscos, e por que ordem (priorizar).

Para fazer esta avaliação, podemos começar por identificar a maturidade dos controlos existentes.

Ao analisar os controlos para mitigar o risco, conhecemos o nosso risco real, sendo necessário verificar a eficácia desses controlos, já implementados na organização, se são eficazes e eficientes, ao evitar custos e trabalho desnecessários, tais como, por

exemplo, na duplicação de controlos. Estes controlos podem ser processos, políticas, dispositivos, práticas ou outras ações que modifiquem o risco. Ao verificar o correto funcionamento de um controlo, está-se a mitigar o risco, já que um controlo mal implementado pode originar uma vulnerabilidade.

O QNRCS (QNRCS Centro Nacional de Cibersegurança, 2023) define os três níveis de capacidade para cada medida de cibersegurança, sendo que podemos recorrer a esse quadro para avaliar a maturidade de cada controlo.

Conforme indicado no Guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023), será de avaliar as consequências no negócio, com uma avaliação propriamente dita dos cenários de eventos identificados como relevantes para as atividades do município, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos, controlos existentes e processos de negócio, visando medir o potencial impacto sobre a autarquia. Devem ser consideradas as consequências de violações da segurança da informação, como, por exemplo: perda de confidencialidade, integridade ou disponibilidade dos ativos.

Estando definidos pelo município os critérios de aceitação do risco, deverá agora ser identificado o limite de aceitação do risco, para o qual é necessária autorização formal da administração da organização, para que esse risco seja aceite, priorizando o risco de acordo com a relevância para a missão da organização.

De realçar, caso o processo ou ativo, esteja definido como seja de baixa importância, logo os riscos associados a ele devem ser menos relevantes, do que os riscos que causam impactos em processos, atividades ou ativos mais importantes.

4.5.2.2 *Processo de tratamento do risco*

Após o levantamento dos riscos, estes têm de ser tratados. Assim, esta fase consiste na identificação, formalização e implementação de um ou mais planos de ação, que servem para documentar as opções de tratamento que foram selecionadas e de que maneira, e em que ordem deverão ser implementadas. Estes planos têm como objetivo controlar e/ou mitigar as causas dos riscos identificados anteriormente. Caso a caso, deve ser verificado o nível dos riscos em questão, os custos e esforço para implementação do tratamento escolhido, e confrontar com os benefícios ou custos que está a evitar ou prevenir, para o município.

Com base nas diretrizes para o tratamento do risco, definidas pela norma ISO/IEC 27005:2008 (*ISO/IEC 27005* 2008), o tratamento do risco passa pela implementação de medidas que permitam aumentar o controlo do risco existente. Como tal, existem quatro opções de tratamento do risco, mitigação, aceitação, resolução e transferência, conforme demonstrado na figura n.º 15.

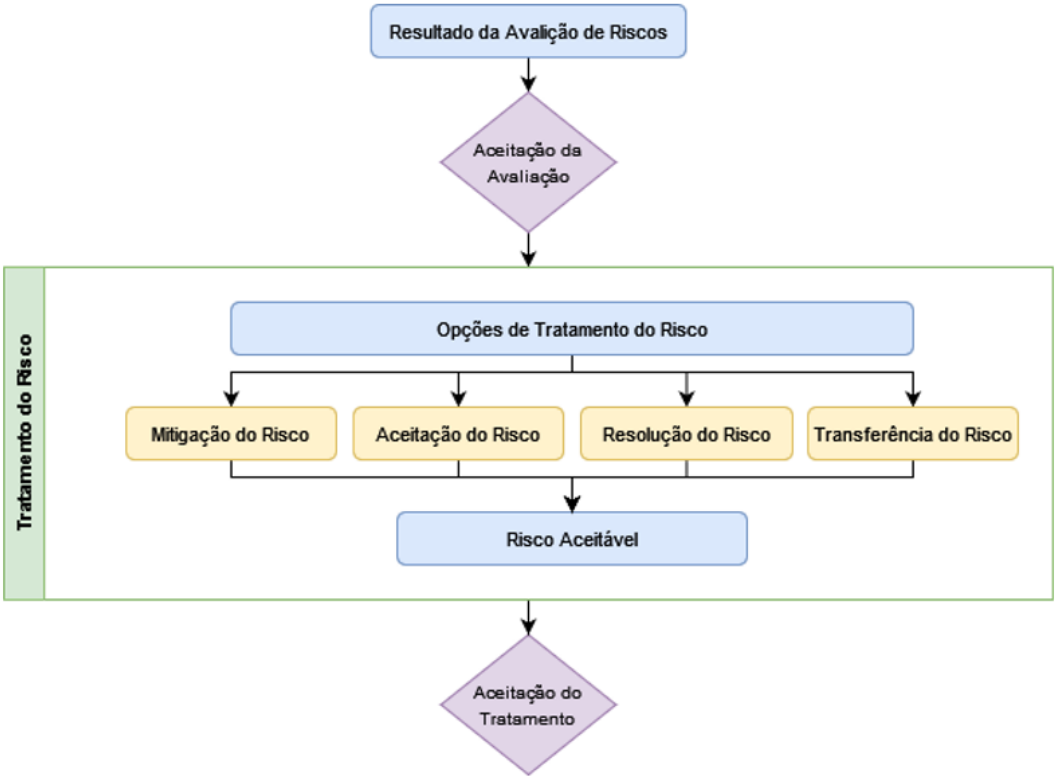


Figura 15: Processo de Tratamento do Risco. Fonte:*ISO/IEC 27005* 2008

A opção de Mitigação do risco, prevê a aplicação dos controlos apropriados e devidamente justificados, de forma a satisfazer os requisitos legais, regulatórios e contratuais. Esta opção deverá ter em conta custos e prazos para a implementação dos controlos, além de aspetos técnicos, culturais e ambientais.

Relativamente à opção, Aceitação do risco, prevê a possibilidade de aceitação das condições do risco, sem a necessidade de implementação de controlos adicionais. Contudo, a aceitação do risco deve apenas ser opção, a quando na existência de um plano de tratamento de riscos da autarquia, as condições definidas como aceitáveis e as condições do risco encontrado são semelhantes.

A opção Resolução do risco, prevê a possibilidade de um dado risco vir a ser evitado por completo, por via da eliminação de uma atividade ou por via de alteração nas condições de operação das atividades. Por norma, a presente opção ocorre no caso de identificação de riscos considerados como muito elevados e no caso do custo de implementação de outras opções de tratamento de riscos excederem os benefícios.

A opção Transferência do risco, prevê a possibilidade da transferência de certos riscos com entidades externas, no entanto, com esta transferência podem surgir novos riscos ou modificar os riscos existentes. A Transferência do risco pode acontecer através da contratação de um seguro, cuja cobertura abranja as consequências de um risco, ou através da contratação de parceiros com o objetivo de monitorização e atuação imediata contra determinados ataques.

Contudo, para que exista um tratamento dos riscos coerente dentro de uma autarquia, é recomendada a definição de um plano de tratamento de riscos onde deve constar de forma clara a ordem de prioridade, assim como formas específicas de tratamento do risco a serem implementadas e os prazos aceitáveis de execução. Ainda, deverão ser continuamente partilhadas as informações sobre os riscos entre os responsáveis de decisão e todas as outras partes interessadas envolvidas. O desenvolvimento do plano de comunicação dos riscos deverá contemplar as operações normais e rotineiras, mas também, as situações de emergência.

4.5.2.3 *Comunicação e consulta do risco*

Nesta fase, procuram-se consensos sobre gerir os riscos de segurança da informação e cibersegurança, através da troca e/ou partilha das informações entre os responsáveis e as outras partes interessadas, devendo ser criado um plano de comunicação e consulta do risco, para assim, assegurar o compromisso dos responsáveis, internos ou externos. É essencial o envolvimento de toda a organização, porque sem a consolidação de uma cultura de gestão dos riscos, os objetivos e a segurança que pretendemos operacionalizar poderão estar comprometidos.

4.5.2.4 *Monitorização e revisão dos riscos*

Nesta fase, o Guia (G. G. d. R. Centro Nacional de Cibersegurança, 2023) define que o departamento responsável pela gestão dos riscos da organização, de acordo com o processo definido para a Gestão do Risco e conforme figura n.º16, tem de monitorizar com regularidade o ambiente da organização, de forma que se identifique atempadamente qualquer alteração que possa ter existido no contexto e que se possa traduzir numa alteração à perceção do risco.

Como referido, a gestão de riscos implica realizar regularmente a monitorização e uma análise crítica dos planos de gestão de riscos, conforme representado na figura, com o objetivo de avaliar o progresso e o estado de implementação dos controlos estabelecidos, bem como a sua eficácia.

A gestão de riscos inclui confirmar se as ações para evitar riscos estão a ser aplicadas efetivamente e verificar se as mudanças no ambiente não afetam os riscos e proceder à revisão e atualização do Plano quando necessário.

Os resultados desse processo de gestão de riscos devem ser documentados e comunicados por meio de mecanismos apropriados, facilitando assim o processo de comunicação e a tomada de decisões.

Figura 16: Processo de Gestão dos Riscos. Fonte:*ISO/IEC 27005* 2008

Deverá ser definida uma unidade orgânica da autarquia, com competências e atribuições, para monitorizar e avaliar regularmente o instrumento para Análise de Riscos de Segurança de Informação.

Uma gestão eficaz de riscos requer a presença de uma comunicação interna bem estabelecida, que assegure de maneira eficiente a identificação e avaliação dos riscos. Já o processo de monitorização deve esclarecer se as medidas propostas foram apropriadas para os objetivos pretendidos, sendo necessário verificar, de forma regular, se o processo de análise de riscos está em conformidade com as melhores práticas, para que continue a ser eficaz ao longo do tempo.

As principais atividades incluídas no processo de monitorização e revisão são:

- Acompanhamento Contínuo: Monitorizar constantemente as ameaças e vulnerabilidades que podem impactar a segurança da informação.
- Revisão de Medidas de Controlo: Avaliar regularmente as medidas de controlo implementadas para garantir que continuam a ser apropriadas e eficazes.
- Atualização da Avaliação de Riscos: Rever periodicamente a avaliação de riscos para incluir novas ameaças, mudanças no ambiente de segurança e atualizações nos ativos de informação.

4.5.3 *Proposta de Matriz para Identificação, Análise e Avaliação do risco nas Autarquias*

De modo a apresentar uma proposta de metodologia para o processo Identificação, Análise e Avaliação do risco nas Autarquias, propõe-se a utilização da matriz indicada na figura n.º 17, para permitir documentar os resultados obtidos, alinhada com a matriz de riscos que eventualmente pode já existir no âmbito do PPRGIC, facilitando a posterior análise dos dados.

1. Identificação da Unidade Orgânica: Serviço ABC													
Unidade orgânica	ID	Principais Atividades	Riscos Identificados	Ativo	Categoria do Risco	Qualificação do Risco			Medidas Preventivas a Implementar	Tipo de Tratamento	Responsável	Estado de Implementação	Obs.
						Prob (1)	Imp (2)	Risco (3)					

Figura 17: Matriz de análise de riscos

Esta matriz irá permitir a avaliação e apresentação dos dados recolhidos. Este modelo irá auxiliar na tomada de decisões, com base nos resultados obtidos na análise de riscos, sobre os riscos com necessidade de tratamento e a prioridade para a implementação do tratamento.

A matriz tem na sua composição a estrutura de um formato documental, que permite a recolha e inserção dos seguintes dados:

- Campo Unidade Orgânica - destina-se à identificação da Divisão ou Equipa com competência no âmbito da atividade identificada.
- Campo ID - destina-se à identificação numérica dos riscos encontrados durante a análise de risco, com formato R-YY-XXXX. Onde YY é os últimos dois dígitos do ano em que o risco foi identificado e XXXX é o número sequencial do risco. Por exemplo R-23-0001.
- Campo Identificação do risco - destina-se à descrição da vulnerabilidade que causa o risco encontrado.
- Campo Ativo - destina-se ao identificador dos ativos associados ao risco encontrado, com formato AA-T-XXX. Onde AA refere-se à categoria do ativo (AF – Ativo Físico, AH – Ativo Humano e AA – Ativo Aplicacional), T indica o tipo de ativo (S – Servidor, T – Telemóvel e C – Computador) e XXX é o número sequencial do risco. Por exemplo AF-S-001.
- Campo Categoria do risco - destina-se à indicação da categoria à qual se adequa à área de atuação do risco, as hipóteses definidas são: Humano, Legalidade, Estratégia, Financeiro e Operacional.

  Relativamente à Categorização do risco, a escala proposta na figura n.º18, tem a finalidade de compreender as várias categorias de risco predominantes numa autarquia.
- Campo Probabilidade - destina-se à indicação do valor quantitativo do nível de probabilidade de um incidente ocorrer, envolvendo o fator de risco em avaliação. Para a obtenção desse valor, tem-se como base escala de probabilidade indicada na figura n.º19.

Humano	Riscos relacionados com a gestão dos recursos humanos.
Legalidade	Riscos relacionados com requisitos da legislação e regulamentos vigentes.
Estratégia	Riscos relacionados com a implementação da estratégia da autarquia.
Financeiro	Riscos relacionados com a gestão financeira e contratação pública.
Operacional	Riscos associados às operações da autarquia, como desempenho operacional, questões ambientais, segurança das infraestruturas e equipamentos.

Figura 18: Tabela de categorização do risco

Nível	Classificação	Descrição
1	Raro	Probabilidade de 1 ocorrência até uma vez em cada 50 anos.
2	Pouco Provável	Probabilidade de 1 ocorrência em cada 5 anos.
3	Improvável	Probabilidade de 1 ocorrência em cada ano.
4	Provável	Probabilidade de 1 ocorrência por mês.
5	Frequente	Probabilidade de ocorrência mais do que uma vez por mês.

Figura 19: Escala de probabilidades

- Campo Impacto - conforme figura n.º 20, destina-se à indicação do valor quantitativo do nível de impacto causado à autarquia se o risco identificado ocorrer.

  Este dado pode ser determinado com base na avaliação e processamento de resultados obtidos com a ocorrência de eventos similares ou pela extrapolação de estudos experimentais ou dados registados do passado. O valor deve estar concordante com as definições apresentadas na tabela da figura n.º 20.

Nível	Classificação	Descrição
1	**Muito Baixo**	Degradação de operações, atividades, projetos, programas ou processos da autarquia, que causam impactos mínimos nos objetivos relacionados com as metas ou padrões ou com a capacidade de entrega de produtos/serviços às partes interessadas. (prazos, custo qualidade, imagem, etc.)
2	**Baixo**	Degradação de operações, atividades, projetos, programas ou processos da autarquia, causando impactos pequenos nos objetivos.
3	**Médio**	Interrupção de operações ou atividades da autarquia, de projetos, programas ou processos, que causam impactos significativos nos objetivos, porém recuperáveis.
4	**Alto**	Interrupção de operações, atividades, projetos, programas ou processos da autarquia, que causam impactos de reversão muito difícil nos objetivos.
5	**Muito Alto**	Paralisação de operações, atividades, projetos, programas ou processos da autarquia, que causam impactos irreversíveis nos objetivos.

Figura 20: Tabela de impatos

- Campo Risco - conforme figura nº 21, trata-se do valor obtido com a combinação dos níveis de probabilidade e impacto, descritas anteriormente. A função definida para determinar qualitativamente o nível de risco passa pela multiplicação dos níveis de probabilidade e impacto associados a um risco identificado.

Impacto \ Probabilidade		1	2	3	4	5
		Raro	Pouco Provável	Improvável	Provável	Frequente
1	Muito Baixo	1	2	3	4	5
2	Baixo	2	4	6	8	10
3	Médio	3	6	9	12	15
4	Alto	4	8	12	16	20
5	Muito Alto	5	10	15	20	25

Figura 21: Tabela de avaliação do nível de risco

Com base no nível de risco avaliado, é possível e aconselhado o estabelecimento de níveis de atuação base relacionados com valor do risco encontrado, definindo uma tabela de prioridade conforme figura n.º 22.

Nível	Classificação	Descrição
1	**Raro**	Probabilidade de 1 ocorrência até uma vez em cada 50 anos.
2	**Pouco Provável**	Probabilidade de 1 ocorrência em cada 5 anos.
3	**Improvável**	Probabilidade de 1 ocorrência em cada ano.
4	**Provável**	Probabilidade de 1 ocorrência por mês.
5	**Frequente**	Probabilidade de ocorrência mais do que uma vez por mês.

Figura 22: Tabela de prioridades

- Campo Medidas preventivas a implementar - destina-se à indicação das medidas/controlos de segurança recomendadas para implementação, de modo a mitigar o risco encontrado.
- Campo Tipo de tratamento - destina-se à indicação do tipo de tratamento a aplicar ao risco encontrado. As hipóteses definidas são: mitigação, aceitação, resolução e transferência.
- Campo Responsável - destina-se à indicação da área de trabalho ou pessoa responsável pelo acompanhamento do processo de implementação do tratamento do risco.
- Campo Estado de implementação - destina-se à indicação do ponto de situação em que se encontra o processo de tratamento do risco, podendo ter os seguintes estados: “Em Análise”, “Em Validação”, “Em Implementação”, “Implementado”, “Em Monitorização” ou “N/A”.

- Campo Observações - destina-se à colocação de informação relevante que não se encontre contemplada no âmbito dos campos já referidos.

4.6 PROPOSTA DE PROCEDIMENTOS OPERACIONAIS DE IMPLEMENTAÇÃO

De modo a estruturar a implementação das várias políticas e procedimentos que compõe o SGSI, numa autarquia de pequena e média dimensão, sugere-se a divisão e execução do processo, em cinco linhas de ação:

- A - Estratégia para gestão do SGSI;
- B - Gestão de infraestrutura física e ambiental;
- C - Gestão da tecnologia;
- D - Gestão dos ativos humanos no âmbito dos SI;
- E - Compliance.

Ao longo deste capítulo, são apresentadas várias medidas a desenvolver, para cada umas das linhas de ação acima referenciadas.

Em apêndice A.6, e nas figuras n.º 43, 44 e 45, é apresentado o quadro síntese das medidas que constam na framework proposta, organizado pelas várias áreas de ação, com indicação da respetiva Regulamentação/Legislação ou Norma/Controlo aplicável.

As medidas propostas foram selecionadas tendo em consideração os seguintes pressupostos:

- Necessidade da medida, justificada com base no conhecimento público do tipo de risco existente numa autarquia de pequena e média dimensão;
- Medida enquadrada no cenário de uma autarquia de pequena e média dimensão, e que em simultâneo, seja mensurável, alcançável dentro de um prazo aceitável e realista em termos de implementação;
- Medida, em que a respetiva implementação, resulte na criação de procedimentos ou instruções de trabalho para resolver ou mitigar um problema;
- Medida que prioriza e vai de encontro com a implementação de um modelo de Sistema de Gestão de Segurança da Informação.

4.6.1 *A - Estratégia para gestão do SGSI*

Esta primeira linha de ação, denominada Estratégia para Gestão e Operacionalização do SGSI, descreve os procedimentos a seguir para implementar, operacionalizar, monitorizar, manter e melhorar o SGSI.

A figura n.º 23, apresenta uma síntese das medidas que constam desta ação, com indicação da respetiva Regulamentação/Legislação ou Norma/Controlo aplicável.

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA

Área de ação	Políticas e área dos Planos a implementar	Regulamentação/Legislação/Controlo
A - Estratégia para gestão do SGSI	1 - Política Macro de Segurança da Informação	ISO/IEC 27001: A.5.1.1.
		QNRCS: ID.GV
	2 - Definição de Responsabilidade e Cargos	ISO/IEC 27001: A.6.1.1.
		QNRCS: ID.AO / ID.AO-2 / ID.AO-3 / ID.AO-4 / ID.AO-5
	3 - Comunicação/declaração de comprometimento, do Dirigente máximo, para com o SGSI	ISO/IEC 27001: A.5.1.
		QNRCS: ID.GV
	4 - Criar um conjunto de documentos, com políticas e normas do SGSI	ISO/IEC 27001: A.7.
		QNRCS: PR.PI

Figura 23: A-Plano estratégico para a gestão do SGSI - síntese de medidas

Assim, nesta fase e conforme figura n.º 28 e n.º 29, disponíveis em apêndice A.1, são definidas as seguintes medidas, bem como, respetivas ações/procedimentos, descrição, responsáveis, estado de implementação, localização das evidências, data prevista de conclusão, como parte integrante da estratégia para a gestão do SGSI:

1. Política de Segurança da Informação;
2. Definição de Responsabilidade e Cargos;
3. Comunicação/declaração de comprometimento, do Dirigente máximo, para com o SGSI;
4. Criação de um conjunto de documentos, com políticas e normas de Segurança da Informação.

4.6.1.1 *Política de Segurança da Informação*

A Política de Segurança da Informação (PSI) é um documento macro que define os princípios e diretrizes a aplicar na gestão da segurança da informação numa organização.

Destacam-se algumas características de uma PSI:

1. Alto nível: define os princípios e diretrizes gerais, sem entrar em detalhes técnicos;
2. Estruturada: Organizada em diversos capítulos que referem diferentes aspetos da segurança da informação;
3. Aprovada pela administração/dirigente máximo: deste modo fica demonstrado o compromisso da organização com a segurança da informação.

Uma PSI deverá incluir os seguintes capítulos:

1. Introdução: apresenta a política e respetivos objetivos;
2. Âmbito: define o âmbito de aplicação da política;
3. Princípios: define os princípios fundamentais da segurança da informação na organização;
4. Regras e Práticas: define um conjunto de regras e práticas para a gestão da segurança da informação;
5. Responsabilidades: define os papeis e responsabilidades das diferentes partes interessadas;
6. Revisão e atualização: define um processo interno de revisão e atualização da política.

4.6.1.2 *Definição de Responsabilidade e Cargos*

A definição de responsabilidades e cargos é essencial na implementação de um Sistema de Gestão de Segurança da Informação (SGSI).

O capítulo da PSI que clarifica a definição de responsabilidades e cargos identifica os diferentes papéis e responsabilidades que tem de existir e ser criados no contexto do SGSI.

Atribui ainda responsabilidades específicas a cada cargo ou função, de forma clara e concisa, para que não haja dúvidas sobre quem é responsável por quê.

Este capítulo deve ser revisto periodicamente, para garantir que as responsabilidade e cargos definidos, continuam a ser adequadas às necessidades da organização.

4.6.1.3 *Comunicação/declaração de comprometimento, do Dirigente máximo, para com o SGSI*

No âmbito da implementação de um Sistema de Gestão de Segurança da Informação (SGSI), a Comunicação/Declaração de Compromisso do Dirigente Máximo é um documento fundamental que demonstra o apoio total e envolvimento da administração neste processo.

Este tipo de Declaração deverá conter o seguinte conteúdo:

1. Afirmação inequívoca do compromisso da administração com a segurança da informação;
2. Reconhecer a importância da segurança da informação para o sucesso da organização;

3. Referir as responsabilidades da administração na implementação e manutenção do SGSI;
4. Comprometer-se em fornecer os recursos necessários para este processo;
5. Referência ao pedido de envolvimento e compromisso de todos os colaboradores com a segurança da informação.

4.6.1.4 *Conjunto de documentos, com políticas e normas do SGSI*

Neste âmbito, tem de ser preparados vários documentos que acabam por definir e documentar o sistema de gestão da segurança da informação da organização.

Este conjunto de documentos, com políticas e normas do SGSI, podem ser:

1. Normas internas de Segurança da Informação, as quais especificam os requisitos de segurança para diferentes unidades orgânicas, como acesso à informação, controlo de ativos, etc.
2. Instruções de Trabalho: conjunto de instruções detalhadas a serem seguidas para realizar uma tarefa específica relacionada com procedimentos de segurança da informação.
3. Relatórios e registos: funcionam como evidência de implementação do SGSI e documentam vários tipos de informações, tais como, auditorias, incidentes de segurança, etc.

No capítulo 4.7, são apresentados vários protótipos de políticas, planos e normas que deverão integrar o SGSI de uma autarquia local de pequena e média dimensão.

4.6.2 *B - Gestão de infraestrutura física e ambiental*

A segunda linha de ação proposta, é referente à Gestão da Infraestrutura Física e Ambiental e aborda aspetos relacionados com a segurança física das instalações de uma organização, onde estão em produção os sistemas informáticos, e zonas operacionais que possam dispor de informação sensível ou crítica, para funcionamento das referidas atividades.

O conjunto de medidas definidas nesta linha de ação, tem o objetivo de garantir a prevenção de incidentes graves na ocorrência de catástrofes, que possam causar danos físicos significativos, comprometendo o normal funcionamento da organização e o acesso à informação.

Neste sentido, será necessário definir vários procedimentos e meios que possam responder de forma eficaz a falhas ou interrupções previsíveis, além de proteger contra atividades não autorizadas.

A figura n.º 24, apresenta uma síntese das medidas que constam desta ação, com indicação da respetiva Regulamentação/Legislação ou Norma/Controlo aplicável.

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA

B - Gestão de infraestrutura física e ambiental	1 - Executar testes para falhas previsíveis nos Data Centers	ISO/IEC 27001: A.17.1.1.
		QNRCS: ID.AO-5 / ID.GL-5
	2 - Criar plano de resposta e de recuperação de incidente	ISO/IEC 27001: A.17.1.1.
		ISO/IEC 27001: A.17.1.2.
		QNRCS: PR.PI-9
	3 - Gestão de ativos de informação físicos	ISSO/IEC 27001: A.8.1.1, A.8.1.2
		QNRCS: ID.GA-1
	4 - Procedimentos de segurança para proteção de equipamentos e ativos em utilização fora das instalações	ISO/IEC 27001: A.6.1.1. / A.6.1.2. QNRCS:
		QNRCS: PR.GA-3
	5 - Infraestruturas técnicas da rede de comunicação de dados	ISO/IEC 27001: A.11.2.2.
		ISO/IEC 27001: A.11.2.4.
		ISO/IEC 27001: A.11.2.5.
		QNRCS: ID.GA-1, ID.GA-3, ID.GA-4
	6 - Data Centers	ISO/IEC 27001: A.11.2.2.
		QNRCS: DE.MC-1

Figura 24: B-Plano de gestão da infraestrutura física e ambiental - síntese de medidas

Assim, nesta fase, e conforme figura n.º 30, 31 e 32, disponíveis em Apêndice A.2, são definidas as seguintes medidas, bem como, respetivas ações/procedimentos, descrição, responsáveis, estado de implementação, localização das evidências, data prevista de conclusão, como parte integrante da gestão de infraestrutura física e ambiental:

1. Executar testes para falhas previsíveis nos Data Centers;
2. Criar plano de resposta e de recuperação de incidente;
3. Criar procedimentos de segurança para proteção de equipamentos e ativos em utilização fora das instalações;
4. Verificar/avaliar infraestruturas técnicas da rede de comunicação de dados;
5. Verificar/avaliar Data Centers.

4.6.3 *C - Gestão da tecnologia*

Esta terceira linha de ação, relacionada com a Gestão da Tecnologia, pretende assegurar medidas que garantam o adequado armazenamento de dados, comunicação e processamento de dados bem como informação de forma segura.

A figura n.º 25, apresenta uma síntese das medidas que constam desta ação, com indicação da respetiva Regulamentação/Legislação ou Norma/Controlo aplicável.

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA

C - Gestão da tecnologia	1 - Sistemas e aplicações	ISO/IEC 27001: A.17.1.
		ISO/IEC 27001: A.12.1.3.
		QNRCS: ID.GA-1 / ID.GA-2 / ID.GA-4 / PR.GA-2 / PR.SD-4 / PR.PI-1/ DE.MC-1/ DE.MC-5
	2 - Controlo do acesso à informação	ISO/IEC 27001: A.9.1.1./9.1.2.
		ISO/IEC 27001: A.9.2.1./9.2.3./9.2.4. /9.2.5./9.2.6.
		ISO/IEC 27001: A.9.3.
		ISO/IEC 27001: A.9.4.3.
		ISO/IEC 27001: A.9.4.3.
		ISO/IEC 27001: A.15.1.
		QNRCS: PR.GA
	3 - Infraestrutura da rede de dados	ISO/IEC 27001: A.17.1./17.2.
		ISO/IEC 27001: A.11.2.3.
		QNRCS: ID.GA-1 / ID.GA-3 / ID.GA-4 / PR.GA / PR.SD / PR.MA
	4 - Sistemas de Firewall, IDS e SIEM	ISO/IEC 27001: A.11.1.1./4.
		ISO/IEC 27001: A.14.1.
		QNRCS: PR.GA-5 / PR.TP-4 / DE.AE-1 / DE.MC-1
	5 - Software de Segurança contra Malware	ISO/IEC 27001: A.12.2.
		QNRCS: DE.MC-4 / RS.AN-4 / RS.MI-1 /

Figura 25: C-Plano de gestão da tecnologia - síntese de medidas

Assim, nesta fase, e conforme figura n.º 33, 34, 35, 36, 37, 38 e 39, disponíveis em Apêndice A.3, são definidas as seguintes medidas, bem como, respetivas ações/procedimentos, descrição, responsáveis, estado de implementação, localização das evidências, data prevista de conclusão

- Sistemas e aplicações;
- Controlo do acesso à informação;
- Infraestrutura da rede de dados.

4.6.4 *D - Gestão dos ativos humanos no âmbito da SI*

A quarta linha de ação proposta, é referente à gestão dos ativos humanos no âmbito da Segurança da Informação.

A figura n.º 26, apresenta uma síntese das medidas que constam desta ação, com indicação da respetiva Regulamentação/Legislação ou Norma/Controlo aplicável.

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA

D - Plano de gestão dos ativos humanos no âmbito dos SI	1 - Norma de segurança de informação que define os termos do contrato e os recursos relacionados com a função	ISO/IEC 27001: A.7.1.1.
		ISO/IEC 27001: A.7.2.1.
		ISO/IEC 27001: A.7.3.1.
		ISO/IEC 27001: A.9.1./9.2.
		QNRCS: PR.GA-6 / DE.MC-3
	2 - Plano de sensibilização em segurança da informação	ISO/IEC 27001: A.5.1.2.
		ISO/IEC 27001: A.7.2.1./7.2.2./7.2.3.
		ISO/IEC 27001: A.9.3./9.4.
		QNRCS: PR.FC
	3 - Ações de formação técnica especializada	ISO/IEC 27002: A.7.2.
		QNRCS: PR.FC

Figura 26: D-Plano de gestão dos ativos humanos no âmbito da SI - síntese de medidas

Nesta fase, e conforme figura n.º 40 e n.º 41, disponíveis em Apêndice A.4, são definidas as seguintes medidas, bem como, respetivas ações/procedimentos, descrição, responsáveis, estado de implementação, localização das evidências, data prevista de conclusão:

- Funções e responsabilidades;
- Formação especializada para equipa de TI;
- Formação, consciencialização e divulgação.

4.6.5 *E - Compliance*

A quinta e última linha de ação proposta, apresenta um conjunto de medidas para assegurar conformidade legal e regulamentar.

A figura n.º 27, apresenta uma síntese das medidas que constam desta ação, com indicação da respetiva Regulamentação/Legislação ou Norma/Controlo aplicável.

Nesta fase, e conforme figura n.º 42, disponível em Apêndice A.5, são definidas as seguintes medidas, bem como, respetivas ações/procedimentos, descrição, res-

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA

E - Compliance	1 - Encarregado da Proteção de Dados	Regulamento (UE) 2016/679, artigo 37º RGPD; Lei n.º 58/2019, de 08 de Agosto (RGPD)
	2 - Sistemas e os dados pessoais	Regulamento (UE) 2016/679 / Lei n.º 58/2019, de 08 de Agosto (RGPD)

Figura 27: E-Compliance - síntese de medidas

ponsáveis, estado de implementação, localização das evidências, data prevista de conclusão:

- Encarregado da Proteção de Dados;
- Sistemas e os dados pessoais.

4.7 PROPOSTA DE ESTRUTURA DOCUMENTAL

Conforme referido no capítulo 4.6.1.4 (Conjunto de documentos, com políticas e normas do SGSI), será necessário preparar documentação que irá permitir definir e documentar o SGSI.

Neste sentido e ao longo dos próximos três subcapítulos, propõe-se um conjunto de documentos, considerados protótipos de políticas e normas de segurança de informação, direcionados para utilização numa autarquia de pequena e média dimensão.

4.7.1 *Normas Internas de Segurança da Informação*

As políticas, normas ou planos de segurança, são procedimentos definidos dentro da organização para proteger os ativos de informação contra ameaças, garantir a confidencialidade, integridade e disponibilidade desses ativos. Para além disso promovem o cumprimento de regulamentações e padrões de segurança.

As Normas e Planos apresentados, foram criados baseados no QNRCS e no conjunto de manuais de boas práticas, no âmbito da Segurança das Redes e Sistemas de Informação, que o CNCS tem disponibilizado.

Foram ainda verificadas alguns frameworks reconhecidos internacionalmente, como ISO/IEC 27001, NIST Cybersecurity Framework, entre outros.

Estes planos estão construídos para serem aplicáveis às diversas unidades orgânicas de uma autarquia, e fornecem orientações claras sobre como os funcionários devem proteger os sistemas e dados da autarquia.

De acordo com os pressupostos referenciados no início do capítulo 4.6, neste trabalho são incluídas as seguintes políticas e planos:

- Política Geral de Segurança da Informação (Apêndice B.1);
- Política de Uso Aceitável (PUA) para os recursos de TI (Apêndice B.2);
- Plano de resposta a incidentes de segurança da informação (PRI) (Apêndice B.3);
- Plano de comunicação de incidentes (Apêndice B.3);
- Plano de testes ao PRI (Apêndice B.3);
- Plano de divulgação interna e forma do PRI (Apêndice B.3);

4.7.2 *Instruções de Trabalho*

No seguimento dos pressupostos referenciados no início do capítulo 4.6, são incluídas neste trabalho, as seguintes instruções de trabalho detalhadas, a serem seguidas para realizar uma tarefa específica, relacionada com um determinado tipo de incidente de segurança de informação:

- Playbook para incidente de Phishing (Apêndice B.6);
- Playbook para incidente de Acesso Não Autorizado (Apêndice B.7);
- Playbook para incidente Ransomware (Apêndice B.8).

4.7.3 *Relatórios e registos*

A produção e conservação de diversos tipos de relatórios e registos irá permitir a avaliação contínua e a demonstração da eficácia do SGSI, além de serem necessários para auditorias e demonstrar a conformidade com normas e regulamentos.

Um dos objetivos dos Relatórios e Registos, será funcionarem como evidências de que os processos e controlos de segurança da informação estão implementadas e são assegurados conforme planeado.

Outro objetivo será demonstrar conformidade com normas como QNRCS e a ISO/IEC 27001, e outros requisitos legais e regulamentares.

Também a produção de diversos tipos de relatórios auxiliará no processo de melhoria contínua do SGSI, já que poderão permitir identificar áreas de melhoria.

Relativamente aos Tipos de Relatórios e Registos que poderão ser produzidos, destacam-se os seguintes:

- Relatórios de Incidentes de Segurança: relatórios que documentam falhas de segurança da informação, ações corretivas e preventivas tomadas;
- Relatórios de Análises de Riscos: relatórios que documentam os registos das análises de risco realizadas, incluindo a identificação de ameaças, vulnerabilidades e medidas de mitigação;
- Relatórios de Monitorização: documentam os registos relacionados com a implementação e monitorização dos controlos de segurança, como logs de acesso, monitorização da rede, etc;
- Relatórios de Formação e Consciencialização: documentam as formações realizadas e as medidas adotadas para a consciencialização dos funcionários sobre segurança da informação.

4.8 DECLARAÇÃO DE APLICABILIDADE (SOA)

Após a conclusão das dez fases de implementação do SGSI, conforme o roadmap apresentado neste trabalho (figura n.º 9), deverá ser criada uma Declaração de Aplicabilidade (SOA).

Esta declaração é exigida às organizações no âmbito do processo de implementação do SGSI e que inclua a certificação segundo a norma ISO/IEC 27001.

Apesar do plano de implementação do SGSI proposto neste trabalho, não abordar a fase de Certificação, a Declaração de Aplicabilidade é de particular importância na gestão da segurança da informação, porque descreve os controlos de segurança selecionados pela autarquia e detalha se esses controlos estão aplicados ou implementados, para mitigar os riscos de segurança da informação identificados, permitindo atingir os seguintes objetivos:

- Documentar os Controlos Selecionados: apresenta todos os controlos de segurança da informação que foram escolhidos com base na análise de riscos, tal como, controlos técnicos, administrativos e físicos, necessários para proteger os ativos de informação da autarquia.
- Detalhar a Implementação dos Controlos: informa o estado de implementação de cada controlo.
- Comunicar o Compromisso com a Segurança de Informação: demonstra o compromisso da autarquia com a segurança da informação. A Declaração de Aplicabilidade é um documento oficial para ser partilhado com as partes interessadas, como por exemplo, funcionários, parceiros e auditores, etc. Desta forma mostra o compromisso da autarquia com a proteção dos dados.

Conforme as diretrizes e requisitos especificados na norma ISO/IEC 27001, uma Declaração de Aplicabilidade inclui pelo menos os seguintes elementos:

- Introdução: Uma visão geral do propósito do documento e a importância do mesmo para a gestão de segurança da informação.
- Metodologia de Seleção dos Controlos: Descrição do processo utilizado para identificar e selecionar os controlos de segurança, incluindo uma referência à análise de riscos realizada.
- Lista de Controlos: Uma tabela ou lista detalhada de todos os controlos selecionados. Cada controlo deve ser identificado pelo seu número ou código.
- Implementação dos Controlos: Informação acerca do estado de implementação de cada controlo.

- Justificação para a Inclusão ou Exclusão de Controlos: Indicar o motivo de por que certos controlos foram selecionados ou excluídos. Para controlos que não sejam aplicáveis, deve ser indicada uma justificação.
- Responsáveis pela Implementação e Manutenção: Identificar os indivíduos ou equipas responsáveis por implementar e manter cada controlo de segurança.

Em síntese, a Declaração de Aplicabilidade pode ser considerada uma ferramenta fundamental para apoiar a autarquia na documentação e comunicação do seu compromisso com a segurança da informação.

Para além disso, a Declaração de Aplicabilidade também pode ser utilizada durante auditorias para demonstrar a sua conformidade com a proteção de dados e e reforçar a cultura de segurança da informação dentro da autarquia.

Ao proporcionar uma visão clara e detalhada dos controlos de segurança em vigor, a Declaração de Aplicabilidade ajuda a garantir que todas as partes interessadas estejam cientes das medidas adotadas para proteger os ativos de informação da autarquia.

4.9 SÍNTESE

Ao longo deste capítulo, apresenta-se um plano abrangente para a implementação de um Sistema de Gestão de Segurança da Informação, em municípios de pequena e média dimensão.

Começa-se por explorar a possibilidade de integração das várias políticas do SGSI com a NCI e o PPRGIC, de modo a alinhar o sistema com as normas e regulamentos internos específicos da organização.

Posteriormente, detalha-se a estrutura do plano de implementação do SGSI, apresentando um roadmap detalhado e personalizado para a implementação do SGSI nos municípios de pequena e média dimensão, cobrindo as várias etapas necessárias para uma implementação bem-sucedida, em áreas como, Estratégia para Gestão do SGSI, Gestão dos Ativos de Informação, Análise de Risco, Políticas, Procedimentos e Controlos de Segurança de Informação e, por fim, a Estrutura Documental para o SGSI.

No subcapítulo referente a Trabalhos Preparatórios e Diagnóstico da Situação Atual, define-se um conjunto de pontos a serem abordados nas reuniões a realizar, são indicados os documentos internos a serem solicitados, bem como uma proposta de questionário estruturado, que poderá funcionar como guideline na implementação do SGSI.

Explora-se também o Processo de Gestão dos Ativos de Informação, descrevendo todo o processo, efetuadas algumas abordagens ás estratégias e práticas essenciais para a administração eficaz dos ativos de informação de uma organização, como um município.

No subcapítulo referente ao Instrumento para o Processo de Análise do Risco, apresenta-se um instrumento orientador para a gestão do risco e de suporte ao planeamento e tomada de decisões, o qual estabelece um conjunto de métodos e passos, direcionados para diminuir a probabilidade de ocorrência de situações de risco e/ou prevenir e mitigar o seu impato, e assim reduzir ao máximo o efeito desses riscos.

No âmbito do subcapítulo referente à Proposta de Procedimentos Operacionais de Implementação, apresenta-se uma metodologia de implementação das várias políticas e procedimentos que compõe o SGSI, divida nas seguintes cinco linhas de ação: A-Estratégia para gestão do SGSI; B-Gestão de infraestrutura física e ambiental; C-Gestão da tecnologia; D-Gestão dos ativos humanos no âmbito dos SI e E-Compliance.

No subcapítulo seguinte, denominado Quadro Síntese da Framework Proposta por Áreas de Ação, apresenta-se um resumo das medidas que constam na framework proposta neste trabalho, organizado pelas várias áreas de ação, com indicação da respetiva Regulamentação/Legislação ou Norma/Controlo aplicável.

Neste capítulo, é incluindo ainda um subcapítulo referente à Proposta de Estrutura Documental, com Normas Internas de Segurança da Informação, onde se propõe um conjunto de documentos, considerados protótipos de políticas e normas de segurança de informação, direcionados para utilização numa autarquia de pequena e média dimensão, tais como, Política Geral de Segurança da Informação, Política de Uso Aceitável (PUA) para os recursos de TI, Plano de Resposta a Incidentes, Playbook para incidente de Phishing, entre outros documentos.

Por fim, no último subcapítulo efetuou-se a descrição e uma referência à importância da Declaração de Aplicabilidade, bem como, os elementos que devem constituir a mesma.

5

CONCLUSÕES

Com a conclusão deste trabalho, verifica-se que a adoção de um Sistema de Gestão da Segurança da Informação nos municípios de pequena e média dimensão, baseado no QNRCS, pode constituir uma estratégia eficaz para proteger os ativos de informação e enfrentar os riscos e desafios complexos da cibersegurança na atualidade.

Através da caraterização dos municípios de pequena e média dimensão, concluiu-se que estes possuem particularidades e desafios específicos na gestão da segurança da informação. A gestão de ativos de informação foi identificada como uma área especialmente desafiante, devido à transformação contínua das suas infraestruturas digitais e às novas competências assumidas nos últimos anos. A revisão das normas, regulamentos e legislação aplicáveis aos municípios, juntamente com a análise dos regulamentos internos, revelou a existência de um vasto conjunto de normativos, impondo um esforço considerável para o cumprimento das regras.

Em síntese, pode-se afirmar que os objetivos e contributos propostos por este trabalho foram totalmente alcançados. Conforme os objetivos inicialmente definidos, foi apresentado um roadmap detalhado e personalizado para a implementação do SGSI nos municípios de pequena e média dimensão, cobrindo as várias etapas necessárias. Essas etapas incluem a Avaliação dos Riscos de cibersegurança e apresentação de uma proposta de Matriz para Identificação, Análise e Avaliação do risco nas Autarquias.

Define-se ainda as ações a adotar no campo da gestão de ativos de informação e apresenta-se um conjunto de procedimentos operacionais de implementação, incluindo controlos de prevenção e de deteção necessários, a sua aplicabilidade e forma de operacionalizar, divido pelas seguintes linhas de ação: Estratégia para Gestão do SGSI, Gestão de Infraestrutura Física e Ambiental, Gestão da Tecnologia, Gestão dos Ativos Humanos no âmbito da SI e Compliance.

É também apresentada uma estrutura documental para o SGSI, incluindo um protótipo de Política Geral de Segurança da Informação, protótipo de Política de Uso Aceitável (PUA) para os recursos de TI e proposta de Plano de Resposta a Incidentes e respetivos documentos acessórios, tais como, Plano de testes ao PRI, Plano de divulgação interna e formação do, Playbook para incidente de Phishing, Playbook para incidente de Acesso Não Autorizado e Playbook para incidente de Ransomware.

Conclui-se que, com a adoção das práticas e propostas aqui apresentadas, este trabalho pode funcionar como um guia prático e adaptado às especificidades dos municípios de pequena e média dimensão, e pode contribuir significativamente para a melhoria da resiliência e da segurança da informação nos municípios, promovendo um ambiente mais seguro e confiável para a administração pública local e para os cidadãos.

Limitações e Recomendações para Trabalhos Futuros

Conforme mencionado no capítulo 4.2, referente à Estrutura do Plano de Implementação, o roadmap apresentado neste trabalho inclui um total de quinze etapas. No entanto, considerando os objetivos específicos deste estudo, foram abordadas apenas as fases até a 11ª etapa. As etapas subsequentes, que se referem à Operação e Desenvolvimento do SGSI, estão fora do âmbito deste estudo. Essas fases podem ser desenvolvidas em trabalhos futuros, o que permitirá avaliar a qualidade e a aplicabilidade do plano de implementação proposto.

Embora esta dissertação forneça um guia para a implementação do SGSI, algumas limitações podem vir a ser identificadas. A implementação prática das propostas pode variar conforme a capacidade técnica e os recursos disponíveis em cada município. Além disso, a rápida evolução das ameaças de cibersegurança e o crescente aumento da superfície de ataque nos municípios, exigirá atualizações frequentes nas políticas, planos e procedimentos sugeridos.

Para trabalhos futuros, é importante destacar a necessidade de desenvolvimento de planos específicos para a ativação de Business Continuity Planning (BCP) e Disaster Recovery Planning (DRP) pelo município. Este estudo centrou-se na estruturação do plano de implementação inicial do SGSI, e não foram incluídos planos detalhados de BCP e DRP, sendo estes cruciais para garantir a resiliência e a continuidade das operações do município em situações de crise. Com a elaboração e devidos testes aos referidos planos, o município ficará com uma framework robusta, que assegura a continuidade dos serviços essenciais e a recuperação rápida em caso de incidentes com grande gravidade.

BIBLIOGRAFIA

27001.pt (2023). *ISO/IEC 27001:2022 — Security Techniques — Information Security Management Systems — Requirements*. https://www.27001.pt/iso27001_6.html. data de acesso: 2023-12-13.

AlgarData (2024). *Smart City: 5 Tecnologias para Criar Cidades Inteligentes*. data de acesso: 2024-01-14. URL: https://algardata.com/blog/tecnologia/smart-city-5-tecnologias-para-criar-cidades-inteligentes/.

Associações de Gestão de Riscos, FERMA - Federação Europeia de (2003). *Norma de Gestão de Riscos*. Disponível em: https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-portuguese-version.pdf. Local de Publicação.

Boeira, Jéssica Martins (2023). *Importância da conscientização em segurança nas organizações*. Artigo. URL: https://www.linkedin.com/pulse/import%C3%A2ncia-da-conscientiza%C3%A7%C3%A3o-em-seguran%C3%A7a-nas-jess%C3%A9-martins-boeira/?originalSubdomain=pt.

Cávado e do Ave e Universidade do Minho, Instituto Politécnico do (2022). *Anuário Financeiro dos Municípios Portugueses 2022*. Documento. URL: https://www.calameo.com/read/0003249817a18c13df59c.

Centro Nacional de Cibersegurança, Guia Gestão dos Riscos (2023). *Guia de Gestão dos Riscos*. Documento. URL: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos.pdf.

Centro Nacional de Cibersegurança, QACC (2023). *Quadro de Avaliação de Capacidades de Cibersegurança*. Documento. URL: https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf.

Centro Nacional de Cibersegurança, QNRCS (2023). *Quadro Nacional de Referência para a Cibersegurança*. URL: https://www.cncs.gov.pt/pt/quadro-nacional/.

Centro Nacional de Cibersegurança, Roteiro (2023). *Roteiro para as Capacidades Mínimas de Cibersegurança*. Documento. URL: https://www.cncs.gov.pt/pt/roteiro-capacidades-minimas-ciberseguranaa/.

Centro Nacional de Cibersegurança de Portugal (2022). *Ferramenta cibercheckup*. data de acesso: 2023-12-13. URL: https://www.cncs.gov.pt/pt/quadro-nacional/#cibercheckup (acedido em 13/12/2023).

CNCS (2022). *Regulamento n.º 183/2022, de 21 de fevereiro*. URL: https://www.cncs.gov.pt/docs/regulamento-183-2022.pdf.

CNCS (2023). *Cibersegurança, CNCS*. data de acesso: 2023-12-13. URL: https://www.cncs.gov.pt/pt/sobre-nos/#oquee.

Comissão Nacional de Proteção de Dados, CNPD (2023). *Diretriz/2023/1, de 10 de janeiro, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais*. Diretriz. URL: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122048.

Conselho da União Europeia, Parlamento Europeu e (2016). *Regulamento Geral sobre a Proteção de Dados (RGPD)*. Regulamento. URL: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.

Conselho Nacional de Cibersegurança, Recomendação Boas Práticas (2022). *Recomendação n.º 2/2022, de 28 de abril, sobre boas práticas de cibersegurança*. Recomendação. URL: https://diariodarepublica.pt/dr/detalhe/recomendacao/2-2022-182431768.

Correia, Carlos Manuel Rosa (2016). *Plano de Implementação da Norma ISO/IEC 27001 no INEM*.

Digital, Portugal (2023). *Estratégia Nacional de Smart Cities*. data de acesso: 2024-01-14. URL: https://portugaldigital.gov.pt/promover-servicos-publicos-mais-digitais/territorios-mais-digitais/estrategia-nacional-de-smart-cities/ (acedido em 14/01/2024).

DigitalSign (2024). *Smart Cities*. data de acesso: 2024-05-21. URL: https://www.digitalsign.pt/smartcities/ (acedido em 21/05/2024).

Forbes Portugal (2023). *Centro Nacional de Cibersegurança alerta para risco de ciberataques a câmaras municipais*. data de acesso: 2023-12-13. URL: https://www.forbespt.com/centro-nacional-de-ciberseguranca-alerta-para-risco-de-ciberataques-a-camaras-municipios/.

Gabinete Nacional de Segurança (2016). *Boas Práticas na Implementação de Sistemas de Informação*. URL: https://www.gns.gov.pt/docs/boas-praticas-i.pdf.

InfoSec, GAT (2023). *Gestão de Ativos de Informação*. Artigo. URL: https://www.gatinfosec.com/blog/gestao-de-ativos-de-informacao/.

ISO/IEC 27001:2013 (2013). International Organization for Standardization. URL: https://www.iso.org/standard/54534.html.

ISO/IEC 27005 (2008). ISO/IEC 27005. ISO.

Leiria, Câmara Municipal de (2022a). *Norma de Controlo Interno da Câmara Municipal de Leiria*. URL: https://www.cm-leiria.pt/uploads/2622/norma_de_controlo_interno___2013.pdf.

— (2022b). *Plano de Prevenção de Riscos de Gestão, incluindo os de Corrupção e Infrações Conexas*. URL: https://www.cm-leiria.pt/municipio/camara-municipal/planeamento-e-controlo-de-gestao/programa-de-cumprimento-normativo/plano-de-prevencao-de-riscos-de-gestao.

Magalhães, Pedro Miguel Machado (setembro de 2023). *CSE4CI - Cybersecurity Ecosystem For Critical Infrastructures*.

Ministros, Conselho de (2018). *Resolução do Conselho de Ministros n.º 22/2018, de 26 de fevereiro*. Resolução. URL: https://diariodarepublica.pt/dr/detalhe/diario-republica/22-2018-114596530.

Mirandela, Câmara Municipal de (2020a). *Norma de Controlo Interno da Câmara Municipal de Mirandela*. URL: https://www.cm-mirandela.pt/uploads/1725/norma-controlo-interno-2020.pdf.

— (2020b). *Plano de Prevenção de Riscos de Gestão, incluindo os de Corrupção e Infrações Conexas*. URL: https://www.cm-mirandela.pt/pages/264?folders_list_44_folder_id=964.

NIST (2012). *Guide for Conducting Risk Assessments*. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

Notícias, SIC (2023). *Ciberataques a autarquias aumentam com a transição digital*. data de acesso: 2023-12-13. URL: https://sicnoticias.pt/pais/2023-10-18-Ciberataques-a-autarquias-aumentam-com-a-transicao-digital-e984cece.

Nuvem, Muito Além da (2023). *Segurança Cibernética: Tendências e Desafios para Pequenas e Médias Empresas*. URL: https://www.linkedin.com/pulse/seguran%C3%A7a-cibern%C3%A9tica-tend%C3%AAncias-e-desafios-para-pequenas-m%C3%A9dias-ss0hf/?originalSubdomain=pt.

Qualidade, Instituto Português da (2009). *NP ISO 31000:2009 - Gestão de Riscos, Princípios e Linhas de Orientação*. Lisboa, Portugal. URL: http://qualitividade.pt/wp-content/uploads/2016/04/NPISO031000_2012.pdf.

República, Assembleia da (2013a). *Lei n.º 53/2013, de 17 de agosto, que estabelece as competências e atribuições dos municípios, das freguesias e das regiões autónomas*. Lei. URL: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2013-56366098-56359576.

— (2013b). *Lei n.º 75/2013, de 12 de setembro, que estabelece o Regime Jurídico das Autarquias Locais*. Lei. URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1990&tabela=leis.

— (2018). *Lei n.º 50/2018, de 16 de agosto, que estabelece o quadro da transferência de competências para as autarquias locais e para as entidades intermunicipais*. Lei. URL: https://diariodarepublica.pt/dr/detalhe/lei/50-2018-116068877.

— (2019a). *Lei n.º 58/2019, de 8 de agosto*. Lei. URL: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982.

— (2019b). *Lei n.º 59/2019, de 8 de agosto*. Lei. URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3123&tabela=leis&nversao=.

República, Assembleia da (3 de nov. de 2023). *Constituição da República Portuguesa*. Constituição. URL: https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf.

Resolução do Conselho de Ministros n.º 41/2018 de 28 de março, Resolução (2018). *Orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais*. Resolução. URL: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/41-2018-114937034.

Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, Conselho de Ministros (2019). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Resolução. URL: https://dre.pt/application/conteudo/122498962.

RJSE, DL 65/2021 (2021). *Regulamenta o Regime Jurídico da Segurança do Ciberespaço*. URL: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.

Security, IT (2023). *Visibilidade completa dos ativos de IT, OT e IoT para assegurar a conformidade com a NIS2*. data de acesso: 2023-12-16. URL: https://www.itsecurity.pt/news/slabs/visibilidade-completa-dos-ativos-de-it-ot-e-iot-para-assegurar-a-conformidade-com-a-nis2 (acedido em 16/12/2023).

Segurança do Ciberespaço, Regime Jurídico da (2018). *Lei n.º 46/2018, de 13 de Agosto*. Lei. URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2930&tabela=leis&ficha=1&pagina=1.

Smart Cities Marketplace (2024). *Smart Cities Marketplace*. data de acesso: 2024-01-14. URL: https://smart-cities-marketplace.ec.europa.eu/.

Smith, S. (2010). *Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization*.

Soure, Câmara Municipal de (2016). *Plano de Prevenção de Riscos de Gestão*. URL: https://www.cm-soure.pt/transparencia/2016_plano_prevencao_riscos_gestao.pdf.

— (2021). *Norma de Controlo Interno da Câmara Municipal de Soure*. URL: https://www.cm-soure.pt/transparencia/bdoc/normas/norma-de-controlo-interno-2021.pdf.

APÊNDICES

A

IMPLEMENTAÇÃO - LINHAS DE AÇÃO

A.1 ESTRATÉGIA PARA GESTÃO DO SGSI

Estratégia para gestão do SGSI

Plano estratégico para gestão do SGSI

A - Plano estratégico para gestão do SGSI

1 - Política de Segurança da Informação								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Definir e Aprovar a Política de Segurança da Informação (PSI)			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Estabelecer PSI	Documento que define a estratégia e objetivos para a segurança da informação de acordo com a missão da autarquia.							
A.2 - Rever PSI	Definir plano de revisão da política de segurança de informação.							
B. Divulgar e comunicar a Política de Segurança da Informação								
B.1 - Definir ações de comunicação da PSI	Definir um plano de comunicação da PSI junto de todos os colaboradores, parceiros e prestadores de serviços e assegurar o comprometimento das partes envolvidas com a PSI.							
B.2 - Disponibilizar a PSI	Disponibilizar a PSI em várias plataformas internas (intranet) e externas (portal da autarquia), de modo a estar sempre acessível e atualizada.							

2 - Definição de Responsabilidade e Cargos								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Responsabilidade e cargos			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Atribuir responsabilidade e cargos	Criar uma estrtutura organizacional, enquadrada com a Segurança da Informação, com os vários cargos e autoridades, sendo necessário que o Dirigente máximo assegure os recursos humanos necessários para o SGSI.							
B. Contato com autoridades competentes e grupos de interesse								
B.1 - Estabelecer protocolos de contatos com autoridades públicas	Estabeler protocolo com o Gabinete Nacional de Segurança; CERT.PT (Centro Nacional de Cibersegurança); CNPD (Comissão Nacional Proteção de Dados) e ANACOM (Autoridade Nacional de Comunicações).							
B.2 - Manter contatos com grupos especializados em segurança de informação	Assegurar que são mantidos contatos com grupos e entidades especializadas em segurança da informação, como por exemplo, Universidades que muitas vezes têm especialistas em segurança da informação que estão envolvidos em pesquisas avançadas sobre novas ameaças e técnicas de defesa, comunidades de profissionais e grupos de interesse que reúnem especialistas em cibersegurança, para trocar conhecimentos, discutir melhores práticas e colaborar em projetos, entre outros.							

Figura 28: Plano estratégico para gestão do SGSI

A - Plano estratégico para gestão do SGSI (cont.)

3 - Comunicação/declaração de comprometimento, do Dirigente máximo, para com o SGSI								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Assegurar alinhamento na PSI			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Comprometimento e apoio visível do órgão máximo para com o SGSI	O dirigentes máximo, deve assegurar que a PSI está alinhada e integrada com a estratégia e missão da autarquia, e assim comunicar a importância da mesma, destacando que todos as funções são importantes para atingir os resultados pretendidos.							
B. Promover a melhoria contínua								
B.1 - Estabeler mecanismos de melhoria contínua no SGSI	Definir, com os dirigentes máximos, um plano para a melhoria contínua do SGSI.							

4 - Conjunto de documentos, com políticas e normas do SGSI								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A.Estrutura de documentos			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Criar a estrutura de documentos que compõe o SGSI	A estrutura de documentos necessária para uma autarquia no âmbito do SGSI, deverá incluir políticas e normas que ajudam a orientar as atividades diversas na proteção de informação, bem como, auxiliar na preparação de documentos que funcionam, como evidências de implementação.							
B. Responsabilidades pela estrutura de documentos								
B.1 - Definir os responsáveis que terão de criar as políticas e normas, e aprovação	As políticas e normas criadas, deverão respeitar o que for inscrito na sua estrutura, no que concerne à elaboração e aprovação.							

Figura 29: Plano estratégico para gestão do SGSI (cont.)

Gestão de infraestrutura física e ambiental

Plano de Gestão da Infraestrutura Física e Ambiental

B - Plano de gestão de infraestrutura física e ambiental

1 - Executar testes para falhas previsíveis nos Data Centers								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Simulacros operacionais em caso de falha energética			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		Evidência
A.1 - Organizar e executar exercícios de simulação para lidar com falhas previsíveis no fornecimento de energia elétrica.	Verificar a capacidade de recuperação dos serviços de TI após a ocorrência de uma falha energética. Existe delay entre a passagem da UPS para o Gerador. É necessário validar o tempo útil de autonomia da UPS com os procedimentos de shutdown/start-up dos sistemas de informação. Avaliar comportamento (em contínuo) do gerador em funcionamento.							
B. Promover a melhoria contínua								
B.1 - Registar todos os procedimentos da operação e ligação com os plano de recuperação de desastre dos sistemas de informação.	Deve ser documentado o método operacional, com a identificação dos atores do processo, a definição do escalation procedure, tempos de resposta e de resolução. Com um plano de simulacro, é possível mitigar riscos de forma controlada, melhorar os procedimentos e validar os procedimentos entre as partes envolvidas.							

2 - Criar plano de resposta e de recuperação de incidente								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Plano de continuidades das operações (plano recuperação de incidente)			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Criar e validar o plano de continuidade das operações, entre as partes envolvidas.	Deve-se obter a validação do plano de continuidade operacional por todas as unidades orgânicas envolvidas. A participação e envolvimento nessas atividades contribuem para um conhecimento partilhado do plano de forma mais ampla e contribuem para uma melhoria contínua.							
B. Rever e avaliar o plano de continuidade das operações								
B.1 - Analisar e avaliar regularmente o plano de continuidade das operações.	A eventual implementação de mudanças operacionais, tecnológicas ou nos sistemas de informação, requer uma revisão do plano de contingência. Investir em ações de formação regulares também é benéfico para melhorar a resposta a situações previsíveis.							

Figura 30: Plano de Gestão da Infraestrutura Física e Ambiental

B - Plano de gestão de infraestrutura física e ambiental (cont.)

3 - Gestão de ativos de informação físicos								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Política de gestão de ativos informação físicos			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Efetuar e manter o inventário de ativos de informação atualizado.	Implementar uma política de gestão de ativos informação físicos eficaz. O inventário deve ser dinâmico e capaz de acompanhar as mudanças na infraestrutura organizacional à medida que vão acontecendo.							

4 - Procedimentos de segurança para proteção de equipamentos e ativos em utilização fora das instalações								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Protocolo a seguir em caso de roubo, acesso indevido ou extravio de computadores portáteis			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Definir um procedimento para tratar a perda, roubo ou acesso indevido a computadores portáteis (laptops e tablets) e outros dispositivos móveis.	Deve-se obter a validação do plano de continuidade operacional por todas as unidades orgânicas envolvidas. A participação e envolvimento nessas atividades contribuem para um conhecimento partilhado do plano de forma mais ampla e contribuem para uma melhoria contínua.							
B. Políticas para equipamentos não vigiados								
B.1 - Estabelecer e implementar uma política para tratar os equipamentos não supervisionados e adotar uma política de secretária limpa de papéis e suportes.	Elaborar uma política para proteger os equipamentos localizados em áreas não supervisionadas, para evitar interrupções nas operações da organização. Estabelecer uma política de manter a mesa de trabalho livre de papéis e dispositivos de armazenamento de dados removíveis, além de manter os écrãs dos computadores limpos/livres.							

Figura 31: Plano de Gestão da Infraestrutura Física e Ambiental (cont.)

B - Plano de gestão de infraestrutura física e ambiental (cont.)

5 - Infraestruturas técnicas da rede de comunicação de dados								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Sistema de refrigeração e ligação a uma rede elétrica protegida			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Verificar a existência de um sistema de refrigeração e ligação da energia a uma rede protegida com UPS (Uninterruptible Power Supply).	Ao avaliar a rede de distribuição de dados, é importante identificar se há bastidores técnicos com demasiados equipamentos instalados. É recomendável implementar um sistema de refrigeração e conectar os equipamentos a uma rede elétrica protegida com UPS (Uninterruptible Power Supply), visando antecipar possíveis falhas de serviço e garantir a disponibilidade contínua dos sistemas.							
B. Organização da instalação de cabos e equipamentos em bastidores, bem como limpeza e documentação								
B.1 - Definir e aplicar um procedimento standard para organizar a instalação de cabos e equipamentos em bastidores, manter a limpeza e garantir a documentação adequada dos mesmos.	Estabelecer diretrizes com as melhores práticas para organizar a instalação de cabos (passivos) e equipamentos ativos nos bastidores técnicos. Este procedimento deve incluir a definição de normas de limpeza, a elaboração de documentação técnica e a realização de auditorias.							
C. Auditoria aos procedimentos operacionais definidos								
C.1 - Estabelecer um cronograma de auditorias periódicas para validar os procedimentos operacionais.	Com a auditoria irão ser validados os procedimentos e assim será assegurada a sua eficácia. Cria também oportunidade de aprender e aperfeiçoar as práticas aplicadas.							

6 - Data Centers								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Localização de centros de dados (Data Centers)			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Avaliação da localização dos centros de dados.	Analisar e avaliar diferentes opções de localização para os centros de dados, tendo em consideração critérios, como disponibilidade de energia, acesso físico, segurança, riscos ambientais, conectividade à rede, infraestrutura de suporte e eventuais requisitos regulamentares, com o objetivo de identificar a localização mais adequada que responda às necessidades operacionais, de segurança e de continuidade de negócio da organização.							

Figura 32: Plano de Gestão da Infraestrutura Física e Ambiental (cont.)

Gestão da tecnologia

Plano de Gestão da Tecnologia

C - Plano de gestão da tecnologia

1 - Sistemas e aplicações								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Alterações ou novas necessidades de sistemas e aplicações devem ser enquadradas com uma proposta de definição de objetivos e requisitos			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		Evidência
A.1 - Manifestar a necessidade de forma clara e precisa, com objetivos e requisitos que o sistema e a aplicação devem responder.	A formalização da necessidade de alterações ou um novo sistema e/ou aplicação, implica enquadrar de forma precisa os objetivos e requisitos para esse sistema ou aplicação, o que por sua vez possibilita o planeamento adequado da infraestrutura de Tecnologia da Informação. Será necessário identificar e determinar os requisitos específicos de segurança da informação que devem ser respeitados, para garantir que o sistema ou aplicação é desenvolvido e implementado de acordo com as normas e políticas de segurança estabelecidas pela organização.							
B. Planeamento e validação de novos sistemas ou alterações em sistemas existentes.								
B.1 - Estabelecer critérios e procedimentos para determinar se os novos sistemas e aplicações respondem aos requisitos de segurança estabelecidos.	Com a formalização da necessidade para novos ou alterações de sistemas/aplicações, elaborar-se-á um plano para reduzir os riscos de falhas nos sistemas/aplicações em causa, avaliação dos requisitos de desempenho, capacidade de processamento e segurança da informação. O objetivo será procurar impedir que as vulnerabilidades das aplicações sejam exploradas por ameaças, seja por desenvolvimento interno improvisado ou pela aquisição de software de fornecedores externos cujo código fonte não está disponível para a organização. Ao formalizar as necessidades, serão definidos os requisitos essenciais para os novos sistemas e aplicações, o que permite planear de forma eficaz, e efetuar testes de segurança e avaliações de desempenho antes da implementação. Evitamos assim o desenvolvimento improvisado interno e procuram-se soluções externas confiáveis, o que reduz a probabilidade de vulnerabilidades.							
C. Alterações em sistemas e serviços de tecnologia da informação								
C.1 - Estabelecer procedimentos para quando ocorrem alterações em sistemas e serviços de tecnologia da informação, sejam efetuadas de acordo com as melhores práticas.	Quando ocorrem alterações em sistemas e serviços de tecnologia da informação devem ser envolvidos para colaboração e participação os representantes de diferentes áreas impactadas diretamente pelas mudanças propostas. Esses intervenientes têm a responsabilidade de interagir, contribuir e assumir responsabilidades pelas decisões e ações planeadas durante o processo de implementação das alterações. Para facilitar essa coordenação, deve ser definido um elemento, que é encarregado de estabelecer a comunicação com todos os intervenientes do processo, recolher as informações necessárias e gerir as prioridades das alterações a serem implementadas. Este processo de gestão de alterações abrange diferentes tipos de mudanças, tais como: alterações solicitadas, manutenção (configurações, novas instalações ou atualizações de versões, incluindo componentes de sistema operativo ou de servidores), resolução de falhas/problemas e alterações de emergência.							

Figura 33: Plano de Gestão da Tecnologia

C - Plano de gestão da tecnologia (cont.)

D. Gestão de ativos aplicacionais								
D.1 - Inventariar e classificar as aplicações de acordo com sua importância e criticidade em termos de operações e funcionalidades, bem como classificar os dados e informações geridos com essas aplicações.	No processo de inventariação distinguir aplicações consideradas críticas e altamente críticas em termos de sua disponibilidade operacional e funcional. É necessário identificar o tipo (classificação) de dados/informação que essas aplicações processam, tratam e armazenam, bem como as unidades orgânicas que as utilizam. Tem de ser registados os termos contratuais relacionados com essas aplicações, os níveis de serviço acordados e os procedimentos de escalonamento operacional em caso de problemas ou interrupções.							
D.2 - Definir os responsáveis por administrar e manter cada uma das aplicações e do processo associado.	Todas as aplicações, que esteja em produção ou desenvolvimento, ou mesmo em fim de vida, deve ter definido uma pessoa como Responsável pela Aplicação, e que será encarregue de diversas tarefas, tais como, atribuir e controlar os níveis de acesso à aplicação, acompanhar a sua evolução funcional e gerir os contratos associados, seja internamente ou com fornecedores externos.							
D.3 - Manter o inventário de aplicações atualizado.	O processo de melhoria contínua e a evolução da organização, obriga que, tanto as aplicações quanto as estruturas associadas sejam alteradas ao longo do tempo. Portanto, a relação matricial entre essas aplicações e estruturas deve refletir os diferentes estados dessa evolução. O inventário deve ser dinâmico e capaz de acompanhar as mudanças nas aplicações e na infraestrutura organizacional à medida que vão acontecendo. Essas alterações decorrentes da evolução normal, podem ser referentes ao desenvolvimento de novas funcionalidades, atualizações tecnológicas, adatações às necessidades do negócio e mudanças nas políticas e/ou regulamentação.							

Figura 34: Plano de Gestão da Tecnologia (cont.)

C - Plano de gestão da tecnologia (cont.)

2 - Controlo do acesso à informação

Ações / procedimento	Descrição	Responsável e participante	Estado da implementação					Data prevista de conclusão
A. Políticas de gestão de identidades e do acesso aos ativos da organização			✓ Implementada		Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Criar, manter e disseminar a política de gestão de acesso à rede e serviços.	Criar um conjunto de diretrizes para gerir e administrar os vários sistemas da organização. Esses procedimentos devem abranger atividades como criação, modificação e exclusão de contas de utilizador, atribuição de permissões e acesso a recursos, configuração de políticas de segurança e outras tarefas relacionadas com a administração de identidades e acessos. Esses procedimentos devem garantir que apenas colaboradores e prestadores de serviços devidamente autorizados, tenham acesso aos recursos dentro desses sistemas.							
B. Política de acessos para ligações a partir do exterior								
B.1 - Criar procedimentos para controlar e regular o acesso de utilizadores a sistemas e recursos da organização quando se ligam remotamente, ou seja, fora da rede física da empresa.	As ligações remotas representam uma potencial porta de entrada para acessos não autorizados, pelo que o acesso deve ser sujeito a autenticação. Determinar o nível de proteção necessário envolve uma análise de risco detalhada e o uso de sub-redes lógicas protegidas por VPN e autenticação com geração de códigos de acesso em tempo real, como por exemplo, one-time passwords. Devem ser implementado um controlo rigoroso e verificar periodicamente a validade dos acessos remotos. Esse controlo inclui monitorizar as ligações, verificar regularmente as credenciais dos utilizadores e avaliar se os níveis de acesso continuam adequados com base nas políticas de segurança estabelecidas.							
C. Responsabilização dos utilizadores na utilização aos sistemas e tecnologias de informação.								
C.1 - Criar um conjunto der regras para definir o comportamento e as responsabilidades dos utilizadores na utilização dos equipamentos e sistemas de informação.	Os utilizadores devem ter conhecimento das suas responsabilidades na utilização e aplicação eficaz das melhores práticas relacionadas com a segurança da informação e a utilização dos equipamentos de informática. Aplicar medidas que garantam a proteção do posto de trabalho, tais como, bloqueio de ecrã, encerrando sessões ativas após a conclusão de tarefas. Outras medidas para deverão ser aplicadas, poderão ser: desativar automaticamente sessões de trabalho e acessos a aplicativos após períodos de inatividade e limitar o tempo de conexão à rede em conexões não seguras. Os utilizadores, devem entender a importância de adotar práticas de segurança da informação no dia a dia de trabalho, o que inclui proteger seus próprios computadores e dados.							

Figura 35: Plano de Gestão da Tecnologia (cont.)

C - Plano de gestão da tecnologia (cont.)

D. Política de acessos para prestadores de serviços								
D.1 - Criar procedimentos para regular e controlar o acesso concedido a fornecedores ou prestadores de serviços.	Criar uma política que defina o acesso à rede da organização para entidades externas, nomeadamente, as que sejam responsáveis pelo suporte e manutenção dos sistemas de informação e comunicação. A política tem de incluir procedimentos para o acesso lógico e físico à rede, bem como restrições de acesso baseada na necessidade de conhecimento e função. Devem ser criados controlos como, verificação de registos de entrada e saída, para monitorizar as atividades dessas entidades enquanto estiverem ligadas à rede da organização. Devem ser emitidos relatórios detalhados sobre as intervenções realizadas por essas entidades, de forma a garantir transparência e responsabilização. Com os referidos relatórios é possível obter uma visão abrangente das atividades realizadas, permitindo uma análise precisa e oportuna de qualquer evento relacionado com a segurança de informação ou a integridade dos sistemas de informação e comunicação.							
E. Política de gestão de acesso dos utilizadores								
E.1 - Definir procedimento para criar, ativar, inativar, modificar e remover contas de utilizadores, bem como monitorização periódica.	Criar um procedimento formal que abranja todas as fases do ciclo de vida do acesso do utilizador, desde o registo inicial de novos colaboradores até à sua eliminação. Este procedimento inclui a criação de um processo estruturado para registar novos colaboradores nos sistemas de informação, atribuindo-lhes os acessos apropriados com base nas suas funções e responsabilidades. Deve ainda ser definido um mecanismo para monitorizar de forma contínua os direitos de acesso dos utilizadores, fazendo verificações periódicas e auditorias detalhadas para determinar quem tem acesso a quê e porquê. Estas atividades devem ser documentadas e registadas formalmente, de modo a manter um registo completo de todos os colaboradores e entidades que utilizam os serviços. Esta informação irá auxiliar na verificação de conformidade com os requisitos legais e regulamentares.							
F. Política de níveis de permissões								
E.1 - Definir permissões e acessos específicos que correspondam às responsabilidades e funções de um determinado cargo ou grupo de utilizadores.	Criar um conjunto de permissões e acessos específicos que correspondam às responsabilidades e funções de um determinado cargo ou grupo de utilizadores dentro da organização. Os níveis de acesso devem ser atribuídos e concedidos de acordo com as funções na organização de determinado utilizador, sendo que deve ser estabelecido um perfil funcional básico sempre que possível, e concedidos privilégios adicionais apenas quando necessário.							
G. Política de gestão de palavras-passe								
G.1 - Criar e manter uma política de gestão de palavras-passe.	Criar um procedimento formal na atribuição de palavras-passe e forçar a mudança periódica das mesmas. Estabelecer regras específicas para a criação e atribuição de palavras-passe, incluindo a geração segura e aleatória de palavras-passe. Isso significa que as senhas devem ser complexas o suficiente para resistir a tentativas sucessivas de adivinhar a senha (ataques de força bruta) por parte de atacantes, e devem ser geradas de forma que não possam ser facilmente deduzidas. Devem ainda ser implementadas regras automáticas para obrigar a alteração regular de palavras-passes, com base em períodos de tempo definidos, para reduzir o risco de comprometimento da segurança devido a palavras-passe antigas que possam ter sido comprometidas ou descobertas por terceiros.							

Figura 36: Plano de Gestão da Tecnologia (cont.)

C - Plano de gestão da tecnologia (cont.)

H. Política de verificação/auditoria de privilégios dos utilizadores								
H.1 - Controlar o acesso aos dados e serviços aplicacionais.	Para garantir um controlo efetivo sobre o acesso aos dados e serviços de informação, é fundamental implementar formalmente um procedimento que assegure auditorias periódicas aos direitos e privilégios dos utilizadores. Essas auditorias garantem que os acessos concedidos estão alinhados com as necessidades operacionais e as políticas de segurança da organização, e se necessário permite identificar e corrigir quaisquer discrepâncias ou riscos potenciais. As permissões devem ser revistas regularmente, idealmente, pelo menos duas vezes ao ano e especialmente quando houver mudança de função ou serviço. As autorizações de acessos especiais e de exceção devem ser revistas com mais frequência, devido ao potencial de risco que representam.							
I. Gestão de logs e de correlação de eventos de segurança								
H.1 - Implementar ferramenta para a gestão centralizada de logs e a sua fusão.	Instalar um sistema que permita a recolha, armazenamento e análise de registos (logs) de diferentes fontes de dados num local centralizado. Desta forma os eventos relevantes são identificados e recolhidos de forma contínua. Esses eventos ficam armazenados num repositório centralizado para posterior análise e criação de relatórios detalhados sobre a saúde e segurança do sistema, além de auxiliar na deteção e resposta a incidentes de segurança. Esses eventos podem incluir atividades de login, acesso a ficheiros, alterações de configuração, entre outros.							

3 - Infraestrutura da rede de dados								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Arquitetura de rede local redundante			✓ Implementada		Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Reestruturar a arquitetura da rede local e implementar redundância.	Com o crescimento tecnológico, incluindo serviços críticos, tais como, serviços públicos essenciais e centro municipal de proteção civil, a infraestrutura de rede deverá estar preparada ao nível do core, data center e distribuição com equipamentos redundantes e links redundantes. Será necessário efetuar um levantamento que inclua a identificação de pontos críticos, a seleção de equipamentos redundantes, a definição de caminhos de comunicação alternativos e a implementação de protocolos de redundância. A redundância pode ser efetuada com switches de rede redundantes, placas de rede duplas em servidores, fontes de alimentação redundantes e links de comunicação alternativos. Ao nível do configurações, deverão ser configurados protocolos de redundância nos switches de rede, balanceamento de carga e failover em servidores (transferência automática e transparente das operações de um servidor para outro servidor funcional em caso de falha ou interrupção).							

Figura 37: Plano de Gestão da Tecnologia (cont.)

C - Plano de gestão da tecnologia (cont.)

B. Gestão centralizada da rede local (LAN) e sem fio (WLAN)								
B.1 - Implementar um software avançado para monitorização e gestão centralizada da rede local (LAN) e sem fio (WLAN).	Dispor de uma monitorização em tempo real, de forma centralizada da infraestrutura de rede com correlação e geração de alarmes para eventos relevantes, incluindo ativos de rede e pontos de acesso sem fio (AP - Access Points). Este sistema de gestão centralizada deverá permitir descobrir e mapear todos os dispositivos de rede na LAN e WLAN, incluindo, switches, routers, pontos de acesso sem fio, servidores e end points.							

4 - Sistemas de Firewall, IDS e SIEM								
Ações / procedimento	Descrição	Responsável e participante	Estado da implementação					Data prevista de conclusão
A. Arquitetura de firewall em alta disponibilidade			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Implementar uma arquitetura de firewall redundante e com IDS (Intrusion Detection System) e SIEM (Security Information and Event Management).	Assegurar que o sistema de firewall detecta o tráfego nas portas de entrada do core da rede, de forma redundante e com a utilização da tecnologia de Sistema de Detecção de Intrusões (IDS). Será necessário a configuração de mais do que uma firewall em paralelo, para garantir alta disponibilidade e confiabilidade na proteção da rede contra ameaças externas. O sistema IDS deverá ser incorporado para monitorizar de forma continua o tráfego de rede na tentativa de encontrar atividades suspeitas ou comportamentos maliciosos. para permitir uma resposta rápida a possíveis incidentes de segurança. O SIEM irá complementar a solução já que centralizar a recolha e análise de logs de segurança dos diversos dispositivos da rede, incluindo sistema IDS, bem como, servidores e endpoints. O SIEM irá correlacionar os logs recolhidos para identificar padrões e anomalias que podem indicar constituir um ataque. Com esta visão mais holística da atividade da rede consegue-se a detecção precoce de ameaças, e também facilita a investigação e a resposta a incidentes de segurança.							

Figura 38: Plano de Gestão da Tecnologia (cont.)

C - Plano de gestão da tecnologia (cont.)

5 - Software de Segurança contra Malware								
Ações / procedimento	Descrição	Responsável e participante	Estado da implementação					Data prevista de conclusão
A. Política de proteção contra Malware em todos os dispositivos cliente e servidores			✓ Implementada		⌛ Parcialmente		☒ Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Implementar sistema antivírus em todos os dispositivos cliente e servidores.	Implementar uma política que obrigue a presença de software antivírus, em funcionamento e atualizado, em todos os computadores pessoais (PCs), laptops e tablets conectados à rede de dados da autarquia.							
B. Monitorização do antivírus								
B.1 - Implementar procedimento de criação de relatórios periódicos de eficácia e status da implementação do antivírus.	A criação periódica (mensal) de relatórios de desempenho do antivírus funciona como uma oportunidade para avaliar os tipos de ameaças "em ataque", a eficácia da resposta do antivírus a essas ameaças e os arquivos que foram corrigidos após a deteção de infeções. Com os relatórios sobre o estado atual da instalação do antivírus, consegue-se analisar os dispositivos ligados à rede com o antivírus ativado ou desativado, a versão do antivírus em utilização, e deste modo, será um apoio no planeamento das tarefas administrativas relacionadas com essa ferramenta de segurança da informação.							

Figura 39: Plano de Gestão da Tecnologia (cont.)

Gestão dos ativos humanos no âmbito da SI

PLANO DE GESTÃO DOS ATIVOS HUMANOS NO ÂMBITO DA SI

Plano de gestão dos ativos humanos no âmbito da SI

D - Plano de gestão dos ativos humanos no âmbito dos SI

1 - Norma de segurança de informação que define os termos do contrato e os recursos relacionados com a função								
Ações / procedimento	**Descrição**	**Responsável e participante**	**Estado da implementação**					**Data prevista de conclusão**
A. Processo de contratualização			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Verificar termos de contratualização de novos colaboradores e prestadores de serviço.	Será necessário estabelecer acordos de confidencialidade e sigilo antes de permitir acesso aos dados ou sistemas de informação da autarqquia.							
B. Perfil Funcional								
B.1 - Atribuir um perfil funcional adequadas ao nível de acesso e aos recursos aplicacionais.	Em consonância com as exigências e responsabilidades da função, atribuir um Perfil Funcional específico para regular o acesso à rede e aos recursos aplicacionais. Qualquer alteração na função ou responsabilidades ao longo do contrato resultará numa modificação correspondente no Perfil Funcional.							
C. Monitorização do acesso aos recursos durante a vigência do vínculo contratual								
C.1 - Estabelecer medidas de controlo para detetar acessos não autorizados a sistemas e serviços.	Com recursos ao sistema que permite a gestão de utilizadores e de identidades, rever e confirmar a correta correspondência entre os acessos aos recursos aplicacionais, nos diversos níveis, e as responsabilidades atribuídas aos colaboradores e/ou prestadores de serviços.							
D. Procedimento formal para cessação ou alteração de contrato								
D.1 - Criar e implementar um procedimento, com critérios formais, a seguir no encerramento ou alteração de contrato.	No encerramento ou alteração de contrato, no que concerne a funções/responsabilidades, é essencial garantir um procedimento formal que assegure a devolução ou recolha dos equipamentos na posse do colaborador e garantir a inativação da entidade e dos respetivos acessos aos sistemas informáticos.							

Figura 40: Plano de gestão dos ativos humanos no âmbito da SI

D - Plano de gestão dos ativos humanos no âmbito dos SI (cont.)

2 - Plano de sensibilização em segurança da informação

Ações / procedimento	Descrição	Responsável e participante	Estado da implementação					Data prevista de conclusão
A. Norma para a utilização dos sistemas de informação			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Criar e implementar uma PUA - Política de Uso Aceitável dos Sistemas de Informação.	Divulgar as regras relacionados com a utilização aceitável dos sistemas de informação e tecnologias associadas, que tem de ser seguidas pelos funcionários das várias unidades orgânicas. Esta política deverá conter um tipo de procedimento disciplinar formal que possa ser acionado em caso de violação da destga norma de segurança da informação.							
B. Formação acerca de segurança da informação								
B.1 - Implementar iniciativas de capacitação em matéria de segurança da informação.	Todos os funcionários e colaboradores da autarquia, que utilizam diretamente ou indiretamente os serviços da rede informática ou recursos aplicacionais, devem participar nas iniciativas de capacitação em segurança da informação. Deverá existir uma evidência, escrita pelo próprio funcionário, a confirmar que recebeu a referida formação.							
C. Consciencialização sobre a utilização da Política Geral de Segurança de Informação								
C.1 - Dar conhecimento da Política Geral de Segurança de Informação	Todos os funcionários e colaboradores da autarquia, tem de ter conhecimento da PGSI, e que a mesma está de acordo com os objetivos estratégicos da autarquia e respetiva missão. Definir de forma clara, que todas as unidades orgânicas e respetivos funcionários são responsáveis por implementar a segurança da informação de acordo com as normas e procedimentos divulgados.							
D. Divulgação de informação relacionada com segurança da informação								
D.1 - Criar plataforma interna de divulgação, consulta e auto-formação.	Disponibilizar uma plataforma acessível a todos os colaboradores, parceiros e prestadores de serviços, com informações diversas relacionadas com segurança da informação, nomeadamente, ameaças atuais ou regras para criar palavras-passe, para garantir deste modo, que os utilizadores estão cientes e preparados para aplicar a Política Geral de Segurança da Informação. Deverá ser implementada uma plataforma de e-learning com formação sobre temas de segurança da informação.							

3 - Ações de formação técnica especializada

Ações / procedimento	Descrição	Responsável e participante	Estado da implementação					Data prevista de conclusão
A. Plano anual de formação técnica especializada			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		
A.1 - Criar e executar um plano anual de formação técnica especializada	Para efetuar a gestão do risco de segurança da informação é exigido colaboradores com adequada formação em tecnologias de segurança da informação, administração de sistemas, servidores e redes. Deste modo, é necessário criar e executar um plano de formação anual, específico para a equipa técnica relacionada, o que permitirá acompanhar a evolução tecnológica e adquirir competências alinhadas com as medidas e tratamentos a serem aplicados.							

Figura 41: Plano de gestão dos ativos humanos no âmbito da SI (cont.)

Compliance

COMPLIANCE

Compliance

E - Compliance

1 - Encarregado da Proteção de Dados

Ações / procedimento	Descrição	Responsável e participante	Estado da implementação					Data prevista de conclusão
A. Nomear Encarregado da Proteção de Dados			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		Evidência
A.1 - Definir o Encarregado da Proteção de Dados	Nomear o Encarregado da Proteção de Dados, que exercerá as seguintes funções: indicar diretrizes e aconselhamento à autarquia, bem como aos seus funcionários, sobre as suas obrigações legais em relação à proteção de dados; monitoriza o controlo do consentimento dos cidadãos; monitoriza e garante o cumprimento das regulamentações aplicáveis em matéria de proteção de dados; identifica e avalia os riscos associados ao processamento de dados pessoais pela autarquia e implementa medidas para mitigar esses riscos; em caso de violações de dados ou outras questões relacionadas com a proteção de dados, o DPO serve como ponto de contato principal para as autoridades de proteção de dados e coopera com elas conforme necessário; sensibiliza e promove a ética e a responsabilidade da privacidade dos utilizadores finais; efetua auditorias internas para garantir que os processos e procedimentos relacionados com a proteção de dados são aplicados corretamente e identifica eventuais áreas de melhoria.							
B. Gestão de Notificações de Incidentes relacionados com Proteção de Dados								
B.1 - Implementar uma plataforma de registo de incidentes	Desenvolver e implementar uma plataforma que permita o registo de incidentes relacionados com a proteção de dados pessoais. Devem ser desenvolvidos sistemas de deteção e alerta no caso de violação de dados pessoais. Como entidade responsável pelo tratamento de dados, a autarquia deve ser capaz de provar que o munícipe deu o seu consentimento à operação de tratamento dos dados, bem como permitir que o munícipe retire esse consentimento.							
C. Comunicação com a Comissão Nacional de Proteção de Dados								
C.1 - Implementar protocolo de comunicação com a Comissão Nacional de Proteção de Dados	Estabelecer um canal de comunicação com a autoridade de supervisão (Comissão Nacional de Proteção de Dados) para notificar violações de dados pessoais (incidentes de violação de dados), onde a notificação deve ocorrer, sempre que possível, dentro de 72 horas após o conhecimento do incidente.							

2 - Sistemas e os dados pessoais

Ações / procedimento	Descrição	Responsável e participante	Estado da implementação					Data prevista de conclusão
A. Avaliar sistemas que contêm dados pessoais			✓ Implementada		Parcialmente		Não implementada	
			Evidência	Localização	Evidência	Localização		Evidência
A.1 - Verificar os sistemas em produçaõ que contêm dados pessoais	Identificar os sistemas que armazenam dados pessoais e avaliar a necessidade de alterações tecnológicas para garantir o tratamento adequado dos dados pessoais em todas as funcionalidades, incluindo recolha, processamento, partilha, arquivo e controlo, de modo a que estejam em conformidade com as regras estabelecidas pelo Regulamento Geral de Proteção de Dados.							
B. Relação com prestadores de serviços								
B.1 - Assegurar o cumprimento do RGPD, avaliandos os termos da contratação	Rever os termos de contratação com prestadores de serviços, fazendo referência que o RGPD estabelece o princípio da responsabilidade proativa, para os prestadores de serviços, que são responsáveis por garantir o cumprimento e a execução adequada na gestão de dados pessoais. Isso inclui tanto o desenvolvimento de software quanto o processamento de dados, e impõe sanções em caso de não conformidade.							

Figura 42: Compliance

Quadro síntese da framework proposta

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA, POR ÁREAS DE AÇÃO

Área de ação	Políticas e área dos Planos a implementar	Regulamentação/Legislação/Controlo
A - Estratégia para gestão do SGSI	1 - Política Macro de Segurança da Informação	ISO/IEC 27001: A.5.1.1.
		QNRCS: ID.GV
	2 - Definição de Responsabilidade e Cargos	ISO/IEC 27001: A.6.1.1.
		QNRCS: ID.AO / ID.AO-2 / ID.AO-3 / ID.AO-4 / ID.AO-5
	3 - Comunicação/declaração de comprometimento, do Dirigente máximo, para com o SGSI	ISO/IEC 27001: A.5.1.
		QNRCS: ID.GV
	4 - Criar um conjunto de documentos, com políticas e normas do SGSI	ISO/IEC 27001: A.7.
		QNRCS: PR.PI
B - Gestão de infraestrutura física e ambiental	1 - Executar testes para falhas previsíveis nos Data Centers	ISO/IEC 27001: A.17.1.1.
		QNRCS: ID.AO-5 / ID.GL-5
	2 - Criar plano de resposta e de recuperação de incidente	ISO/IEC 27001: A.17.1.1.
		ISO/IEC 27001: A.17.1.2.
		QNRCS: PR.PI-9
	3 - Gestão de ativos de informação físicos	ISSO/IEC 27001: A.8.1.1, A.8.1.2
		QNRCS: ID.GA-1
	4 - Procedimentos de segurança para proteção de equipamentos e ativos em utilização fora das instalações	ISO/IEC 27001: A.6.1.1. / A.6.1.2. QNRCS:
		QNRCS: PR.GA-3
	5 - Infraestruturas técnicas da rede de comunicação de dados	ISO/IEC 27001: A.11.2.2.
		ISO/IEC 27001: A.11.2.4.
		ISO/IEC 27001: A.11.2.5.
		QNRCS: ID.GA-1, ID.GA-3, ID.GA-4
	6 - Data Centers	ISO/IEC 27001: A.11.2.2.
		QNRCS: DE.MC-1

Figura 43: Quadro Síntese da Framework proposta

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA, POR ÁREAS DE AÇÃO (cont.)

C - Gestão da tecnologia	1 - Sistemas e aplicações	ISO/IEC 27001: A.17.1.
		ISO/IEC 27001: A.12.1.3.
		QNRCS: ID.GA-1 / ID.GA-2 / ID.GA-4 / PR.GA-2 / PR.SD-4 / PR.PI-1/ DE.MC-1/ DE.MC-5
	2 - Controlo do acesso à informação	ISO/IEC 27001: A.9.1.1./9.1.2.
		ISO/IEC 27001: A.9.2.1./9.2.3./9.2.4. /9.2.5./9.2.6.
		ISO/IEC 27001: A.9.3.
		ISO/IEC 27001: A.9.4.3.
		ISO/IEC 27001: A.9.4.3.
		ISO/IEC 27001: A.15.1.
		QNRCS: PR.GA
	3 - Infraestrutura da rede de dados	ISO/IEC 27001: A.17.1./17.2.
		ISO/IEC 27001: A.11.2.3.
		QNRCS: ID.GA-1 / ID.GA-3 / ID.GA-4 / PR.GA / PR.SD / PR.MA
	4 - Sistemas de Firewall, IDS e SIEM	ISO/IEC 27001: A.11.1.1./4.
		ISO/IEC 27001: A.14.1.
		QNRCS: PR.GA-5 / PR.TP-4 / DE.AE-1 / DE.MC-1
	5 - Software de Segurança contra Malware	ISO/IEC 27001: A.12.2.
		QNRCS: DE.MC-4 / RS.AN-4 / RS.MI-1 /

Figura 44: Quadro Síntese da Framework proposta (cont.)

QUADRO SÍNTESE DA FRAMEWORK PROPOSTA, POR ÁREAS DE AÇÃO (cont.)

D - Plano de gestão dos ativos humanos no âmbito dos SI	1 - Norma de segurança de informação que define os termos do contrato e os recursos relacionados com a função	ISO/IEC 27001: A.7.1.1.
		ISO/IEC 27001: A.7.2.1.
		ISO/IEC 27001: A.7.3.1.
		ISO/IEC 27001: A.9.1./9.2.
		QNRCS: PR.GA-6 / DE.MC-3
	2 - Plano de sensibilização em segurança da informação	ISO/IEC 27001: A.5.1.2.
		ISO/IEC 27001: A.7.2.1./7.2.2./7.2.3.
		ISO/IEC 27001: A.9.3./9.4.
		QNRCS: PR.FC
	3 - Ações de formação técnica especializada	ISO/IEC 27002: A.7.2.
		QNRCS: PR.FC
E - Compliance	1 - Encarregado da Proteção de Dados	Regulamento (UE) 2016/679, artigo 37º RGPD; Lei n.º 58/2019, de 08 de Agosto (RGPD)
	2 - Sistemas e os dados pessoais	Regulamento (UE) 2016/679 / Lei n.º 58/2019, de 08 de Agosto (RGPD)

Figura 45: Quadro Síntese da Framework proposta

B

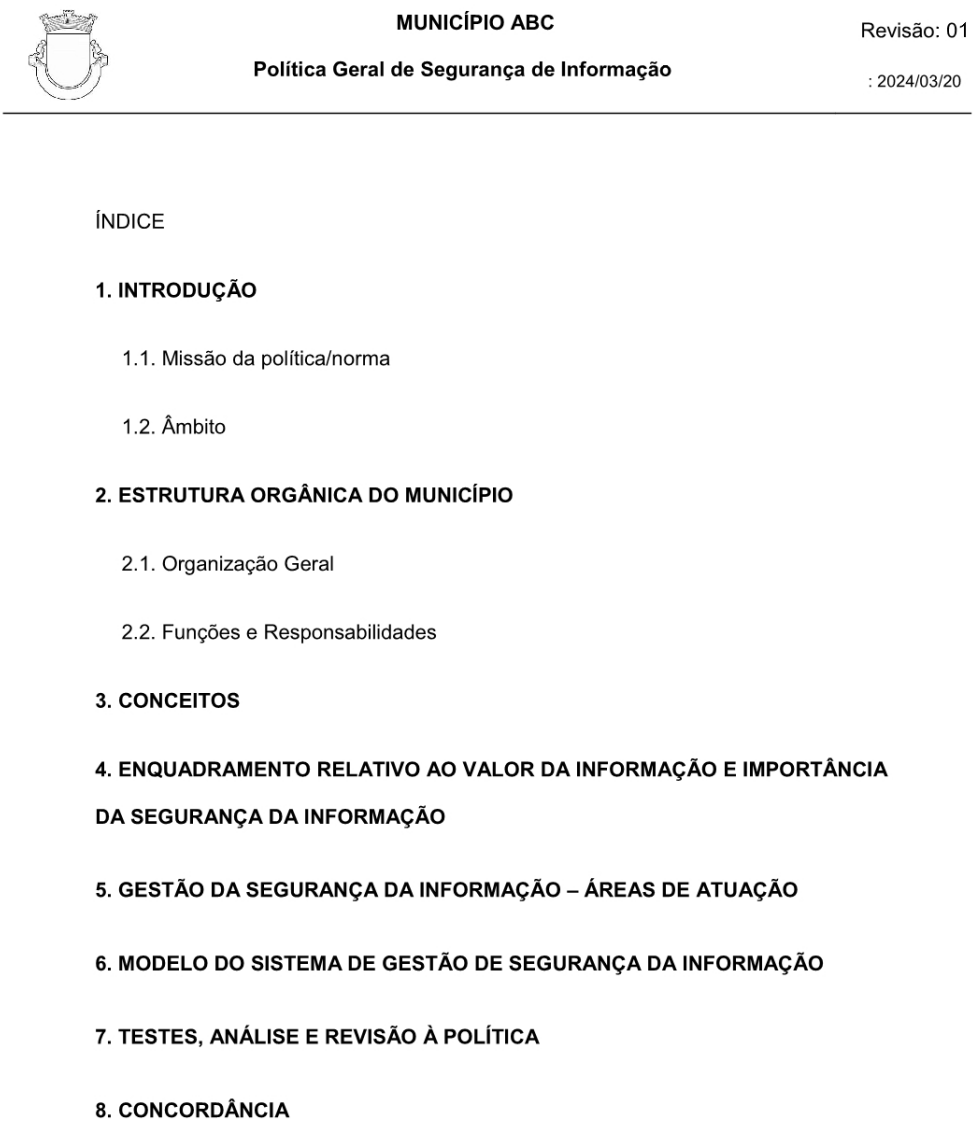
NORMAS INTERNAS DE SEGURANÇA DA INFORMAÇÃO

B.1 POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

Política Geral de Segurança de Informação

PROPOSTA DE ESTRUTURA E DE LAYOUT

A figura seguinte, apresenta uma Proposta de Estrutura e de Layout, para criação de uma Política Geral de Segurança de Informação, a utilizar num Município de Pequena e Média Dimensão. Esta proposta tem como base de trabalho, as disposições da norma ISO/IEC 27001.



MUNICÍPIO ABC

Revisão: 01

Política Geral de Segurança de Informação

: 2024/03/20

ÍNDICE

Figura 46: Proposta de Estrutura de PGSI

INTRODUÇÃO

MISSÃO DA POLÍTICA/NORMA

A principal missão da Política Geral de Segurança da Informação, delineada neste documento, é estabelecer as diretrizes abrangentes de Segurança da Informação para o Município ABC, e que vá de encontro com os seguintes objetivos:

1. Manter a confiança dos colaboradores, parceiros, munícipes e demais entidades que interagem com a autarquia, e na capacidade do Município ABC tem para proteger a informação que tem sob a sua responsabilidade;
2. Confirmar que os ativos de informação estão protegidos contra utilização, divulgação, alteração ou destruição não autorizados, de acordo com sua importância;
3. Dispor de uma resposta eficaz a possíveis incidentes de segurança da informação, minimizando o impacto financeiro, reputacional e operacional;
4. Cumprir as obrigações legais e regulamentares relacionadas com a atividade do Município ABC, no que diz respeito à Segurança da Informação.

A adoção de uma Política de Segurança da Informação para o Município ABC, permite estabelecer uma base de trabalho única para todos as unidades orgânicas, e assim promover a utilização de padrões de segurança organizacional e práticas eficazes na gestão da segurança da informação. Visa ainda, garantir confiança nas relações com terceiros, bem como cumprir imposições legais provenientes de normas comunitárias e nacionais, relacionadas com a segurança da informação.

O órgão executivo do Município ABC, em conformidade com as melhores práticas internacionais, o QNRCS e com a legislação e regulamentação em vigor, compromete-se a cumprir e manter os referidos requisitos legais da Política Geral de Segurança da Informação, além de garantir a melhoria contínua da política por meio de monitorização e revisão regular.

Esta política define os princípios gerais que cada unidade orgânica deve seguir em relação aos ativos de informação que gere.

Está estruturada em vários capítulos, incluindo objetivo, valor da informação, importância da segurança da informação, diretrizes para a gestão da segurança da informação, modelo do sistema de gestão de segurança da informação, políticas detalhadas de segurança da informação, organização e responsabilidades na segurança

da informação, bem como manutenção e comunicação das políticas e respetivos procedimentos de segurança.

ÂMBITO

Esta política é aplicável, a todos os colaboradores, consultores externos, estagiários, consultores temporários, prestadores de serviços, qualquer tipo de entidade externa com acesso aos ativos de informação do Município ABC e que com este, participem no tratamento de Informação. Aplica-se ainda a todos os ativos de informação que se encontrem sob a jurisdição ou responsabilidade do Município ABC.

ESTRUTURA ORGÂNICA DO MUNICÍPIO ABC

ORGANIZAÇÃO GERAL

Este capítulo deverá ser desenvolvido com informação relativa à estrutura orgânica do Município ABC, incluindo, o organograma da autarquia, entre outras informações relevantes relacionadas com o funcionamento da entidade.

FUNÇÕES E RESPONSABILIDADES

A competência para aprovar a Política Geral de Segurança da Informação e suas políticas setoriais correspondentes, é da Câmara Municipal, sendo igualmente da sua responsabilidade a alocação dos recursos humanos e financeiros necessários para implementar as ações desenvolvidas.

A unidade orgânica, nomeada para administração e gestão desta política, tem as seguintes responsabilidades:

1. Rever e monitorizar a implementação do Plano Geral de Segurança da Informação.
2. Gerir e controlar a aplicação das Políticas Gerais e Setoriais de Segurança da Informação do Município ABC, e efetuar a coordenação da implementação em normas, procedimentos e configurações de segurança.
3. Preparar a produção de indicadores internos e externos de Segurança da Informação.
4. Diligenciar e apoiar as unidades orgânicas na avaliação do risco de Segurança da Informação, bem como, definição dos requisitos e preparação dos planos com medidas de ação para mitigação correspondentes.
5. Gerir a atribuição de acessos a utilizadores internos e externos.
6. Promover a consciencialização e sensibilização de todas as entidades cuja presente política é aplicável, sobre segurança da informação.
7. Definir e gerir o SGSI.

Todas as unidades orgânicas do Município ABC têm a responsabilidade de aplicar e fazer cumprir esta política.

As entidades cuja presente política é aplicável e que deliberadamente infrinjam esta política estarão sujeitos a medidas disciplinares ou legais, que podem incluir a rescisão de contratos de trabalho e a notificação às autoridades judiciais sobre situações que sugiram a prática de crime.

É importante destacar que qualquer utilização inadequada dos equipamentos do Município ABC, bem como dispositivos pessoais ligados aos recursos do Município ABC, rede institucional, sistema de e-mail ou qualquer outra aplicação de manipulação de informações ou recursos do Município ABC, incluindo utilização para atividades ilícitas, pode resultar em consequências graves para o Município. Exemplo disso, inclui ações como acesso não autorizado aos sistemas informáticos, dados ou ativos, introdução de malware, roubo ou divulgação de informação confidencial do Município, bem como o roubo ou utilização indevida de dados pessoais.

Informação

Informação é o resultado do processamento, manipulação e organização de dados numa forma que se some ao conhecimento da pessoa que o recebe.

A Informação também pode ser definida como Conhecimento organizado, ou seja, a Informação é qualquer conhecimento que tenha sido processado, manipulado e organizado a partir de dados ou outros elementos.

A Informação é um recurso valioso para o Município ABC, pois representa conhecimento que pode ser usado para tomar decisões, melhorar processos e gerar valor para a organização.

A Informação pode ter os seguintes formatos:

- Não estruturada: Textos, imagens, vídeos, áudios.
- Eletrónica: Documentos digitais, aplicações, websites.
- Física: Documentos impressos, livros, manuscritos.

Fases do Ciclo de Vida da Informação

O ciclo de vida da informação tem várias fases, que descrevem o fluxo de dados desde o momento da criação até à destruição ou arquivo.

As principais fases desse ciclo são:

- Criação: Geração da informação.
- Transmissão: Partilha da informação entre diferentes pessoas ou sistemas.
- Manutenção: Atualização e correção da informação.
- Destruição: Eliminação segura da informação quando deixar de ser necessária.

Ativo de Informação

Um ativo de informação é definido como qualquer informação ou dispositivo que processa, transmite ou armazena informação com valor para uma organização. Esta definição abrange uma variedade de elementos, tais como:

- Hardware: Computadores, servidores, redes de dados.
- Software: Aplicações de negócio, sistemas operativos, bancos de dados.
- Informação: Documentos, emails, imagens, vídeos.

- Pessoas: Colaboradores, consultores, formadores.

Colaboradores

Os colaboradores são indivíduos que trabalham no Município ABC, tais como, funcionários, consultores, formadores, ou outros.

Os colaboradores têm acesso à informação do Município ABC e são responsáveis por usá-la de forma segura e responsável.

Incidentes de Segurança da Informação

Todos os eventos ou situações que comprometem a confidencialidade, integridade ou disponibilidade dos ativos de informação do Município ABC, com prejuízo financeiro e/ou reputacional e/ou operacional.

Alguns exemplos comuns de incidentes de segurança da informação são:

- Ataques cibernéticos, como Malware, phishing ou ransomware.
- Perda ou roubo de informação.
- Erros humanos que comprometem a segurança da informação.
- Exploração de vulnerabilidades, aproveitando falhas de segurança em sistemas, aplicativos ou redes para obter acesso não autorizado ou executar atividades maliciosas.
- Violação de Dados, quando ocorre acesso não autorizado a dados sensíveis, como informações pessoais de munícipes, dados financeiros, o que resulta na exposição ou comprometimento dessas informações.

Sistema de Gestão de Segurança da Informação

O Sistema de Gestão de Segurança da Informação é um processo permanente e contínuo, que visa os seguintes objetivos:

- Avaliar os riscos à segurança da informação do Município ABC.
- Implementar medidas de controlo para mitigar esses riscos.
- Monitorizar a efetividade das medidas de controlo.
- Melhorar continuamente o sistema de gestão de segurança da informação.

Os principais benefícios, que decorrem da implementação de um Sistema de Gestão de Segurança da Informação, são:

- Proteger a informação do Município ABC contra perdas e danos.
- Assegurar a conformidade com leis e regulamentos.
- Aumentar a confiança dos stakeholders no Município ABC.
- Melhorar a tomada de decisões e a eficiência operacional.

ENQUADRAMENTO RELATIVO AO VALOR DA INFORMAÇÃO E A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

VALOR DA INFORMAÇÃO

A informação pode assumir diferentes formas, como impressa em papel, armazenada eletronicamente, transmitida por correio ou meios eletrónicos, entre outras. Independentemente do meio, utilização ou suporte, é importante protegê-la de forma apropriada, de acordo com a sua importância e valor.

A manutenção da confidencialidade, integridade e disponibilidade da informação requer uma abordagem sistemática ao risco, de modo a minimizar incidentes que possam comprometer a sua segurança.

O acesso à informação é fundamental para o funcionamento do Município ABC, sendo a eficiência do serviço prestado aos munícipes diretamente dependente da disponibilidade dos sistemas de informação. Portanto, a segurança no tratamento e transmissão da informação é crucial para manter essa eficiência.

Qualquer interrupção no funcionamento dos serviços, exfiltração de informação para partes não autorizadas ou modificação não autorizada de dados pode resultar na perda de confiança e/ou violação das obrigações para com os munícipes, parceiros ou incumprimento de obrigações legais e regulamentares.

Para alcançar os objetivos de segurança da informação, as unidades orgânicas do Município ABC dependem do funcionamento adequado de seus sistemas de informação e comunicações. No entanto, isso só é possível com a identificação contínua dos riscos aos quais os ativos do Município ABC estão expostos e a implementação de controlos e mecanismos de segurança para garantir a sua correta e controlada utilização.

É da responsabilidade de todos os colaboradores do Município ABC, bem como de outros envolvidos abrangidos por esta política, contribuir proativamente para a proteção da informação, inclusive ao partilhar informações sensíveis, mesmo verbalmente. Da mesma forma, é responsabilidade dos mesmos, reportar qualquer ameaça, concretizada ou potencial, que possa impatar a disponibilidade, integridade ou confidencialidade da informação.

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

A informação gerida pelo Município ABC, bem como todos os processos de suporte, sistemas, aplicativos e redes, são ativos valiosos para a autarquia. Qualquer comprometimento da confidencialidade, integridade e/ou disponibilidade desses ativos pode resultar na perda de confiança nos serviços prestados pelo Município ABC.

Neste sentido, a Segurança da Informação deve ser aplicada em todas as etapas do ciclo de vida da informação. Controlar as operações de recolha, processamento, armazenamento, transferência, análise, pesquisa e destruição da informação é tão importante quanto garantir a funcionalidade de um aplicativo. Assim, é essencial manter um nível de qualidade e segurança consistentemente alto para prevenir a materialização de riscos e limitar os danos potenciais causados por vulnerabilidades ou incidentes de segurança, para deste modo garantir que a atividade da autarquia se desenvolva conforme esperado.

A Segurança da Informação é um requisito fundamental para o sucesso dos serviços prestados pelo Município ABC, e todos os colaboradores, fornecedores, parceiros ou outras entidades que tenham acesso à informação são responsáveis por sua proteção.

As ameaças à Segurança da Informação estão em constante evolução, exigindo uma adaptação contínua das medidas de segurança para acompanhar as mudanças tecnológicas, legislativas e sociais. Essas medidas devem ser tanto técnicas quanto economicamente viáveis e não devem prejudicar de forma desnecessária a produtividade e eficiência do Município ABC. Os riscos residuais devem ser conhecidos pelos órgãos autárquicos e pelos funcionários que têm responsabilidades operacionais sobre os ativos associados.

GESTÃO DA SEGURANÇA DA INFORMAÇÃO – ÁREAS DE ATUAÇÃO

O Município ABC, segue as seguintes áreas de atuação, para a gestão da segurança da informação:

- Gestão dos ativos humanos - A segurança da informação aplica-se a todos os colaboradores da Município ABC, incluindo todas as unidades orgânicas, de forma abrangente. Em determinadas funções devem ser atribuídas responsabilidades específicas relacionadas com a segurança da informação.
- Gestão do risco - Todos os sistemas, em produção ou com futura implementação, devem ter um nível de segurança adequado, de acordo com o risco que o Município ABC está disposto a aceitar. A análise de risco deve indicar as preocupações técnicas em linguagem compreensível.
- Definição de responsabilidades - A responsabilidade pelos acessos e respetivo tipo, utilização e proteção da informação existente nos sistemas é dos responsáveis afetos. Assim, é responsabilidade do Município ABC, estabelecer e aprovar normas e procedimentos que criem os níveis de segurança da informação que sejam definidos pelas entidades proprietária/responsáveis pela informação e monitorizar a sua aplicabilidade e eficácia.
- Regras de segurança - O Município ABC tem a responsabilidade de aprovar normas de segurança que definam os objetivos a atingir por todos os sistemas de informação, independentemente do ambiente em que funcionam.
- Procedimentos de segurança - Os procedimentos de segurança devem ser detalhados e devem ser objetivos quanto à forma de atingir o nível pretendido de segurança, e devem indicar qual é o tipo de intervenção humana na manutenção dos sistemas de informação, tendo a preocupação de não deixar áreas de atuação no âmbito da manutenção, indefinidas.

MODELO DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

O modelo do SGSI do Município ABC, segue as diretivas do QNRCS, como ferramenta de apoio à implementação, que está estruturado num conjunto de medidas de segurança, que traduzem cinco objetivos específicos: Identificar, Proteger, Detetar, Responder e Recuperar (figura 42).

Identificar - consiste em definir o âmbito da abordagem da gestão do risco de cibersegurança, numa visão transversal à autarquia, no que concerne a todas as suas redes, sistemas de informação, pessoas, ativos, dados e processos/capacidades relevantes.

Proteger - no objetivo proteger, implementam-se as medidas necessárias ou reforçam-se as existentes, de modo a assegurar a continuidade da prestação de serviços ou fornecimento de bens de determinada organização, no caso de ocorrência de um incidente de cibersegurança. Este reforço de capacidade, passa por implementar procedimentos, processos e tecnologias de proteção da informação, bem como, realização de formação interna, sensibilização para as questões da cibersegurança, entre outras medidas.

Detetar - neste objetivo, é dado enfoque à implementação de processos e mecanismos de deteção precoce de ocorrência de eventos de cibersegurança, com recurso à monitorização sistemática das redes e sistemas de informação.

Responder - com este objetivo, o resultado a atingir, será verificar se a autarquia está capacitada com a implementação de práticas que se traduzam em ações de resposta a incidentes de cibersegurança detetados. Com estes procedimentos, de planeamento de resposta a incidentes, de comunicação com as partes interessadas relevantes, da análise e mitigação de incidentes, a autarquia deverá estar pronta a conter os impatos de um potencial incidente.

Recuperar - o objetivo recuperar, consiste em criar e operacionalizar um conjunto de boas práticas, bem como manter um plano de resiliência (planos de continuidade do negócio e de recuperação) que assegurem o restauro de alguma capacidade e/ou serviço que tenha sido comprometido por um evento de cibersegurança, minimizando os impactos negativos na autarquia do referido evento.

Este modelo de SGSI assenta nos três pilares da Segurança da Informação:

- Confidencialidade - esta propriedade refere que a informação não pode ser divulgada a pessoas ou entidades não autorizadas, ou segundo processos não

Figura 47: Cinco objetivos segurança - Fonte: QNRCS

autorizados (ISO/IEC 27000), tendo assim garantia de que a informação está acessível apenas por pessoas e processos devidamente autorizadas para o efeito;

- Integridade - propriedade de salvaguardar o caráter exato e completo da informação e dos ativos (ISO/IEC 27000), ou seja, salvaguarda da exatidão da informação e dos métodos de processamento;
- Disponibilidade - propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada (ISO/IEC 27000), tendo assim a garantia de que utilizadores e processos autorizados têm acesso à informação sempre que necessário.

Conforme referido anteriormente, os mecanismos de segurança da informação existentes no Município ABC, visam a confidencialidade, integridade e disponibilidade da informação, e assim, devem ser normalizados, por uma estrutura documental, com normas e políticas detalhadas, processos e procedimentos de segurança da informação, conforme apresentado nos capítulos seguintes.

Normas Internas de Segurança da Informação

Propõe-se a implementação do seguinte conjunto de documentos, com políticas e normas de segurança de informação:

1. Política de Uso Aceitável (PUA) para os recursos de TI;
2. Plano de resposta a incidentes de segurança da informação;
3. Plano de comunicação de incidentes;
4. Plano de testes ao PRI;
5. Plano de divulgação interna e forma do PRI;
6. Plano de gestão do ciclo de vida dos utilizadores;
7. Plano de registo e monitorização de atividade (logs);
8. Plano para controlo dos sistemas em produção (atualizações);
9. Plano para instalação de novo hardware e software;
10. Plano para as cópias de segurança;

11. Plano para os serviços de computação em nuvem;
12. Plano para os suportes de dados (proteção, eliminação);
13. Plano para a instalação e proteção dos equipamentos;
14. Plano de manutenção de equipamentos/sistemas;
15. Plano para a subcontratação de serviços;
16. Planos de emergência e de continuidade de negócio.

Entre outras opções possíveis, este trabalho inclui protótipos das seguintes políticas e normas de segurança da informação::

- Política Geral de Segurança da Informação;
- Política de Uso Aceitável (PUA) para os recursos de TI;
- Plano de resposta a incidentes de segurança da informação;
- Plano de comunicação de incidentes;
- Plano de testes ao PRI;
- Plano de divulgação interna e forma do PRI.

Instruções de Trabalho

Conjunto de instruções detalhadas, a serem seguidas para realizar uma tarefa específica relacionada com procedimentos de segurança da informação, e que devem ser adicionadas e melhoradas de forma contínua.

Entre outras opções possíveis, este trabalho inclui os seguintes playbooks:

- Playbook para incidente de Phishing;
- Playbook para incidente de Acesso Não Autorizado;
- Playbook para incidente de Ransomware.

TESTES, ANÁLISE E REVISÃO À POLÍTICA

A Política Geral de Segurança da Informação do Município ABC deve ser testada e revista anualmente, ou sempre que ocorram alterações significativas na legislação e regulamentação aplicáveis, estratégias de alto nível ou nos sistemas de informação, e alterações na perceção de níveis de risco.

Todas as alterações nesta política serão submetidas à aprovação da Câmara Municipal do Município ABC e devem ser publicadas e comunicadas a todos as entidades cuja presente política é aplicável.

C O N C O R D Â N C I A

Todos os colaboradores, internos ou externo, são obrigados a cumprir as diretrizes estabelecidas pela Política Geral de Segurança da Informação do Município ABC e tem a responsabilidade individual de compreender, conhecer e seguir as indicações para garantir a utilização adequada e a proteção das informações do Município ABC.

O incumprimento da Política Geral de Segurança da Informação pode resultar em processos disciplinares, para além de outras possíveis consequências legais, tanto de natureza civil quanto penal.

Caso existam exceções a esta política, estas devem ser justificadas previamente através de um processo formal de aceitação de risco. Todas as exceções às políticas de segurança da informação devem ser autorizadas e registadas formalmente, além de serem monitorizadas continuamente.

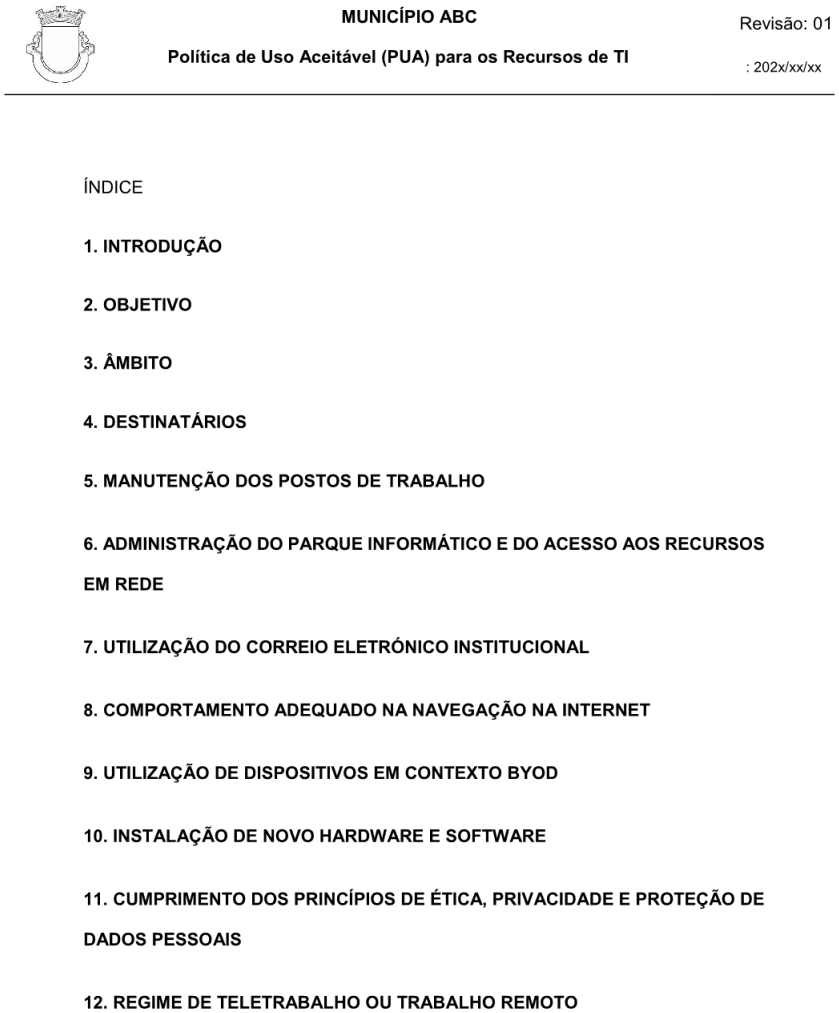
Em caso de dúvidas sobre o âmbito e/ou a aplicação desta política, os colaboradores devem-se dirigir ao Presidente da Câmara Municipal ou a quem lhe for delegada esta competência, de modo a obter os devidos esclarecimentos.

No âmbito das políticas de segurança da informação são implementadas medidas gerais para monitorizar comunicações internas ou externas, bem como padrões de utilização de informação ou sistemas, sempre em conformidade com as leis de proteção da privacidade individual.

Política de Uso Aceitável (PUA) para os recursos de TI

PROPOSTA DE ESTRUTURA E DE LAYOUT

A figura seguinte, apresenta uma Proposta de Estrutura e de Layout, para criação de uma Política de Uso Aceitável (PUA) para os recursos de TI, a utilizar num Município de Pequena e Média Dimensão. Esta proposta tem como base de trabalho, as disposições da norma ISO/IEC 27001 e ISO/IEC 27002 e o conjunto de manuais de boas práticas, no âmbito da Segurança das Redes e Sistemas de Informação, que tem sido disponibilizados pelo CNCS.



MUNICÍPIO ABC Revisão: 01

Política de Uso Aceitável (PUA) para os Recursos de TI : 202x/xx/xx

ÍNDICE

Figura 48: Proposta de Estrutura da PUA

1. INTRODUÇÃO

A presente Política de Uso Aceitável, destina-se a proteger os sistemas e serviços do Município ABC, de modo a garantir disponibilidade, confidencialidade e integridade dos sistemas de informação.

2. OBJETIVO

O objetivo deste documento é definir a utilização responsável dos serviços, recursos eletrónicos e infraestrutura de comunicações do Município ABC.

3. ÂMBITO

O âmbito deste documento visa a definição de papeis e responsabilidades, e procedimentos a adotar nas seguintes temáticas:

- Manutenção dos postos de trabalho e ambiente de trabalho;
- Administração do parque informático e do acesso aos recursos em rede;
- Correta utilização do correio eletrónico para uso profissional;
- Comportamento adequado na navegação na Internet;
- Utilização de dispositivos em contexto BYOD;
- Instalação de novo hardware e software;
- Trabalho remoto ou teletrabalho;
- Cumprimentos dos princípios de ética, privacidade e proteção de dados pessoais (RGPD);

4. DESTINATÁRIOS

Os destinatários desta Política, são as pessoas que utilizam as infraestruturas e os serviços informáticos e tecnológicos necessários ao normal funcionamento do Município ABC, e referenciados nesta política, com a seguinte designação:

- Responsável pelo Setor de TI - funcionário designado pelo Presidente da Câmara Municipal, para a direção e coordenação do Setor de Tecnologias de Informação;
- Responsável pela Segurança de TI- funcionário designado pelo Presidente da Câmara Municipal, como responsável por garantir a segurança dos sistemas, dados e redes da autarquia;
- Utilizador - qualquer funcionário com vínculo contratual ao Município ABC, incluindo prestadores de serviços que, direta ou indiretamente utilizem os sistemas de comunicação e informação do Município ABC, para o desenvolvimento das suas atividades profissionais;
- Responsável pelo tratamento de dados – todo os utilizadores referidos no ponto anterior, e que efetuam tratamento de dados pessoais;
- Encarregado da proteção de dados (DPO) - funcionário designado pelo Presidente da Câmara Municipal para monitorizar a aplicação da regulamentação de proteção de dados e garantir que a organização esteja em conformidade com as leis de proteção de dados.

5. MANUTENÇÃO DOS POSTOS DE TRABALHO

1. O responsável pelo Setor de TI, deve garantir a implementação dos seguintes controlos de deteção e prevenção, para proteger os dados e os recursos de tratamento contra código malicioso (malware):
    - Deve ser instalado software antivírus e software anti-spam em todas as estações de trabalho e servidores que compõem a rede e sistema de informação;
    - O software antivírus e o software anti-spam devem ser sempre devidamente licenciados e mantidos atualizados;
    - A atualização do antivírus e do anti-spam deve ser, preferencialmente, automática;
    - Garantir a verificação regular de presença de código malicioso em:
        - Dados, sistema operativo instalado, pacotes de software e aplicações;
        - Dispositivos de armazenamento removíveis;
        - E-mails e anexos recebidos de fontes externas e internas;
2. O responsável pelo Setor de TI, deve ainda assegurar o seguinte:
    - As portas USB das estações de trabalho que não são necessárias, devem estar bloqueadas;
    - As portas USB que sejam necessárias devem ter políticas implementadas para impedir o acesso e abertura de ficheiros que possam executar programas potencialmente nocivos.
3. O responsável pela segurança, deve sensibilizar os utilizadores para importância da deteção atempada de incidentes de segurança e para a necessidade de o informar, sempre que for detetado código malicioso.
4. O utilizador tem de adotar comportamentos que evitem a introdução de código malicioso, pelo que deve colocar em prática as seguintes ações preventivas:
    - Comunicar de imediato qualquer alerta apresentado pelo sistema antivírus;
    - Evitar utilizar dispositivos de armazenamento removíveis;

- Em caso de comportamento suspeito do sistema, o utilizador deve parar imediatamente qualquer processamento em curso, desligar o sistema potencialmente infetado da rede e notificar o responsável pela segurança.

6. ADMINISTRAÇÃO DO PARQUE INFORMÁTICO E DO ACESSO AOS RECURSOS EM REDE

1. O responsável pelo Setor de TI deve definir políticas e procedimentos para atribuição de privilégios de acesso e utilização do sistema, de modo a garantir que o acesso aos recursos de tratamento dos dados funcionários é efetuado apenas por utilizadores devidamente autorizados.
2. O responsável pelo Setor de TI efetua os seguintes procedimentos para a criação de contas de utilizador do sistema (procedimento de registo - pedido de autorização formal para acessos aos sistemas de informação do Município):
    - O acesso ao sistema só pode ser concedido a quem tiver concluído, com sucesso, o procedimento de registo;
    - Os pedidos de criação ou modificação de uma conta de utilizador, deve ser efetuado através de formulários próprios, devidamente preenchidos e assinados;
    - Devem existir igualmente regras específicas para contas de utilizadores genéricos (por exemplo, webservices);
    - Após aprovação da autorização de acesso, deve ser criada uma nova conta individual para o utilizador e uma palavra-passe inicial (a qual deve também obedecer às regras definidas para as palavra-passe) que lhe permitirá aceder às aplicações, serviços e sistemas para as quais foi autorizado;
    - Não devem ser permitidas contas partilhadas;
3. O responsável pelo Setor de TI tem de dispor de uma lista atualizada de todos os funcionários autorizados a utilizar os sistemas informáticos e o tipo de permissão de acesso. Esta listagem, devidamente atualizada, deverá ser disponibilizada ao encarregado da proteção dos dados, para fins de controlo interno e verificação de conformidade.
4. O responsável pelo Setor de TI deve definir os perfis de utilizador. O acesso às vários funções dos sistemas, aplicações e serviços, deve ser refletido em privilégios de acesso (perfis) diferenciados, em função da necessidade de conhecer e da segregação de funções, sempre de acordo com o princípio do menor privilégio (isto é, cada utilizador deve possuir apenas os privilégios

necessários para realizar a respetiva função na autarquia). Os perfis devem ser devidamente especificados e explicados ao utilizador.

5. O responsável pelo Setor de TI deve definir definir procedimentos para que as credenciais de autenticação (palavra-passe) sejam únicas e intransmissíveis. No caso de autenticação ser efetuada por user/palavra-passe, deve seguir os seguintes procedimentos:

    - No primeiro acesso ao sistema, deverá ser solicitado ao utilizador a alteração da palavra-passe inicial, e assim o utilizador escolhe a sua própria palavra-passe, a qual deve ser única, de fácil de memorização (mas difícil de adivinhar), não repetida e apenas conhecida e memorizada pelo próprio;
    - A palavra-passe deve ter no mínimo 9 caracteres e ser complexa, ou seja, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a..z), letras maiúsculas (A..Z), números (0..9) e caracteres especiais (˜! @ # $ % ^& * () _ + | ‘- = {} []:"; ’<>?,. /);
    - Em alternativa, a palavra-passe poderá ser constituída por frases ou excertos de texto longo, sem carater de “espaço”;
    - A palavra-passe deve ser alterada, no máximo, a cada 180 dias para perfis de utilizador e 90 dias para perfis de administradores de sistemas e bases de dados, ou quando for comprometida ou se suspeite que venha a ser comprometida;
    - O sistema deve ser configurado para alertar os utilizadores de que devem alterar as respetivas palavras-passe, com uma antecedência adequada (máxima de 30 dias);
    - A reutilização de palavras-passe anteriores deverá ser evitada, recomendando-se que não seja igual às últimas 4 palavras-passe.

6. O responsável pelo Setor de TI deve seguir os seguintes procedimentos, para bloqueio de contas dos utilizadores:

    - As contas dos utilizadores deverão ser automaticamente bloqueadas após 3 tentativas de autenticação sem sucesso e bloqueadas manualmente se se suspeitar que a conta está a ser usada incorretamente;
    - O encarregado da proteção de dados deve ser alertado para as situações de bloqueio acima referidas através, por exemplo, de relatórios periódicos, de modo a poder detetar eventuais problemas;
    - As contas que já não são necessárias devem ser bloqueadas, inativadas ou eliminadas;

- Devem ser definidas regras específicas para as situações de ausência prolongada de utilizadores (por exemplo, licenças, férias, baixas prolongadas, mudança de funções, entre outros), bem como procedimentos internos de reporte e de atualização destas situações, entre as várias unidades orgânicas.

7. O responsável pelo Setor de TI deve seguir os seguintes procedimentos, no que concerne aos bloqueios automáticos de uma estação de trabalho:

   - O bloqueio automático do ecrã da estação de trabalho deve ser ativado, preferencialmente, após 5 minutos de inatividade, podendo ser desbloqueado apenas com credenciais de acesso;
   - No final de cada ciclo de trabalho do utilizador, a respetiva sessão deve ser encerrada;
   - Deve ser previsto o encerramento automático da sessão de trabalho do utilizador em caso de inatividade por tempo superior a 3 horas, bem como o encerramento automático da estação de trabalho em caso de inatividade superior a 5 horas (excecionam-se necessidades de sessões ativas para efeitos de manutenção e administração de sistemas).

7. UTILIZAÇÃO DO CORREIO ELETRÓNICO INSTITUCIONAL

1. O utilizador tem de ter a noção de que a caixa de correio eletrónico que lhe foi atribuída é considerada institucional. Deve, por isso, ser utilizada para transmissão oficial de informações ou outras trocas de informação no âmbito da atividade no Município ABC;
2. O Município ABC nunca solicita, por email, telefone ou qualquer outro meio, as credenciais de autenticação (password);
3. A caixa de correio eletrónico referida no ponto 1 não pode ser utilizada para fins comerciais ou qualquer outro fim que ponha em causa o nome e imagem do Município ABC;
4. A caixa de correio eletrónico atribuída possui uma capacidade limitada, pelo que deverá ser efetuada uma manutenção periódica de arquivo das mensagens, de modo a garantir a operacionalidade permanente da receção de mensagens institucionais;
5. Não devem ser enviadas mensagens para um elevado número de destinatários exteriores;
6. A abertura de mensagens e de anexos provenientes de endereços de origem desconhecida deve ser evitada, dado que este é um dos meios mais utilizados para a distribuição de vírus, “malware” e “phishing”;
7. O serviço de correio eletrónico do Município ABC não deve ser utilizado para distribuição massiva de mensagens (SPAM).

8. COMPORTAMENTO ADEQUADO NA NAVEGAÇÃO NA INTERNET

1. O Município ABC disponibiliza acesso à Internet a todos os utilizadores autenticados e subentende-se que a sua utilização deverá ser limitada à atividade oficial da autarquia. Porém, é admitida a possibilidade de utilização da internet para fins pessoais.
2. O acesso não poderá ser utilizado para ganhos financeiros pessoais, como venda de serviços ou produtos, ou outras vantagens patrimoniais.
3. É proibida a visita a sites que exibam conteúdos de natureza pornográfica, ou que contenham material que possa ser considerado ofensivo ou ilícito. Sempre que um utilizador for surpreendido, acidentalmente, com páginas web de conteúdos suspeitos, deve informar de imediato o Responsável pelo Setor de TI.
4. É expressamente proibido:
    - O acesso a servidores sem autorização;
    - Deteção de serviços em servidores ("Port Scan");
    - Alteração de endereços IP (IP Spoofing);
    - A utilização de softwares peer-to-peer (P2P), como por exemplo: Kazaa, BitTorrent, Emule, etc.
5. O utilizador deve estar atento aos Direitos de Autor dos conteúdos que descarregar da Internet.
6. O utilizador nunca deverá indicar o seu endereço de correio eletrónico, sem motivo de força maior, num website. Ao fornecer o seu endereço, ao preencher pesquisas ou outros questionários corre o risco de receber mensagens impróprias, e sem qualquer interesse.

9. UTILIZAÇÃO DE DISPOSITIVOS EM CONTEXTO BYOD

Tendo em consideração a análise dos riscos e benefícios associados ao uso de dispositivos pessoais no contexto da atividade do Município ABC, decidiu-se não permitir que os funcionários utilizem os seus dispositivos pessoais para fins profissionais.

A decisão acima apresentada baseia-se nas seguintes considerações, fundamentais para garantir a segurança e a integridade da atividade da autarquia:

- Sem controlo total sobre os dispositivos pessoais, não é possível garantir que as medidas de segurança necessárias estão aplicadas de forma adequada;
- A autarquia está sujeita a regulamentos e normas, que implicam a adoção de controlos sobre o acesso e a proteção de dados. A utilização de dispositivos pessoais dificulta o cumprimento dessas obrigações.

10. INSTALAÇÃO DE NOVO HARDWARE E SOFTWARE

Os responsável pelo Setor de TI deve seguir os seguintes procedimentos, quanto à instalação de novo hardware e software:

- A configuração local de hardware e software do sistema não deve ser alterada sem autorização prévia;
- Devem ser definidos procedimentos internos, para serem seguidos sempre que se solicitem alterações à configuração do sistema e que permitam o controlo dessas alterações;
- Apenas devem ser instalados componentes de hardware e software autorizados;
- Apenas os componentes de hardware e os dispositivos periféricos autorizados podem ser ligados ao sistema;
- Alterações à configuração local de hardware e software do sistema devem ser comunicadas ao encarregado da proteção de dados.

11. CUMPRIMENTO DOS PRINCÍPIOS DE ÉTICA, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

1. O responsável pelo tratamento de dados tem de assegurar a garantia dos direitos do titular dos dados, nomeadamente:
    - Direito de informação;
    - Direito de acesso aos respetivos dados pessoais;
    - Direito de retificação de dados inexatos;
    - Direito ao apagamento (“direito a ser esquecido");
    - Direito à limitação do tratamento;
    - Direito de portabilidade de dados;
    - Direito de oposição.
2. No âmbito dos direitos referidos anteriormente, o responsável pelo tratamento de dados tem de assegurar o seguinte:
    - A autenticidade da identificação do titular para o exercício dos seus direitos, não divulgando dados pessoais a terceiros não autorizados;
    - A existência de documentação de todos os procedimentos de tramitação dos pedidos e registo em logs das operações que forem realizadas no sistema na sequência de pedidos de acesso, retificação, eliminação ou limitação;
    - O desenvolvimento de políticas organizativas e técnicas que permitam uma transmissão segura dos dados pessoais, de modo a que quando houver portabilidade dos dados (principalmente entre dois responsáveis pelo tratamento, mas também através do titular) estes sejam transmitidos em segurança e não sejam acedidos por terceiros não autorizados.
3. O responsável pelo tratamento de dados, de modo a assegurar uma proteção adequada dos dados pessoais, tem de incluir nas políticas de segurança procedimentos para a respetiva classificação, priorização e monitorização, de acordo com os seguintes procedimentos:
    - Os dados pessoais devem ser classificados de acordo com os critérios de sensibilidade e criticidade pré-definidos;

- Deve ser definida uma priorização para a proteção dos dados pessoais, atribuindo-se prioridade aos considerados mais críticos;
- Devem ser mantidos seguros os registos de atividades dos utilizadores (logs);
- Os serviços de apoio ao utilizador dos sistemas de informação, devem estar preparados para responder a questões relacionadas com a proteção dos dados pessoais;
- Devem ser realizadas verificações e avaliações periódicas aos mecanismos de controlo e procedimentos de segurança implementados;
- Deve ser assegurada a monitorização das redes e sistemas de informação associados. Esta atividade pode ser assegurada por uma terceira entidade tecnicamente competente para o efeito.

12. REGIME DE TELETRABALHO OU TRABALHO REMOTO

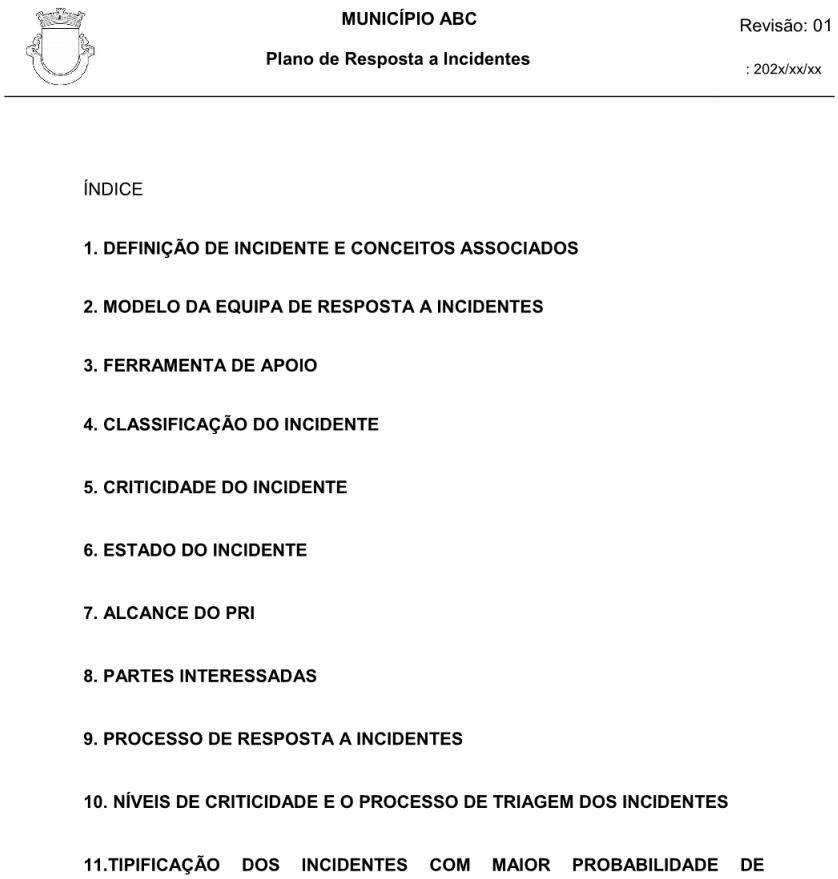
1. O responsável pelo Setor de TI, no que concerne aos trabalhadores com autorização formal para desempenho de funções em regime de teletrabalho ou trabalho remoto, tem de assegurar o seguinte:
    - Disponibilizar equipamentos devidamente preparados de acordo com as normas descritas na presente política;
    - Disponibilizar nesses equipamentos software de proteção malware, devidamente atualizados, e software de proteção avançada de endpoint, que proteja o sistema contra ameaças mais complexas;
    - Acesso à rede do Município ABC efetuado através de pontos de acesso remoto aprovados e que são controlados pelo Setor de TI, utilizando tecnologia VPN.
2. O utilizador com autorização formal para desempenho de funções em regime de teletrabalho ou trabalho remoto tem de assegurar o seguinte:
    - Separar os equipamentos informáticos de utilização profissional dos de utilização pessoal;
    - Garantir que faz logout sempre que termina uma sessão remota, em vez de fechar.
    - Não partilhar equipamentos informáticos do Município ABC com familiares, amigos e outros. Nunca partilhar senhas ou quaisquer outros dispositivos ou parâmetros de acesso.
    - Alterar a password default do router de casa para uma password complexa;
    - Alterar o nome da rede doméstica;
    - Quando possível, desabilitar o acesso remoto dos outros dispositivos da rede doméstica.
    - Assegurar que o router está atualizado;
    - Ativar firewall nos dispositivos da rede doméstica;
    - Dar preferência a uma ligação com fio;
    - No caso de ligação sem fio, usar uma ligação encriptada, com uma password complexa.

- Não deve alterar configurações do sistema operativo ou de aplicações sem permissão ou assistência do Setor de TI.
- O equipamento informático (hardware) não pode ser alterado sem permissão ou assistência do Setor de TI.

B.3 PLANO DE RESPOSTA A INCIDENTES

Plano de Resposta a Incidentes - Município ABC

A figura seguinte, apresenta uma Proposta de Estrutura e de Layout, para criação de um Pano de Resposta a Incidentes, a utilizar num Município de Pequena e Média Dimensão. Esta proposta tem como base de trabalho, as disposições da norma ISO/IEC 27035.



MUNICÍPIO ABC

Plano de Resposta a Incidentes

Revisão: 01

: 202x/xx/xx

ÍNDICE

Figura 49: Proposta de Estrutura do PRI

1. DEFINIÇÃO DE INCIDENTE E CONCEITOS ASSOCIADOS

A definição de incidente dentro de qualquer empresa ou organização, é importante para uma resposta eficaz, eficiente e consistente a eventos de segurança. Esta definição fornece uma base sólida para a identificação, classificação e resposta adequada aos incidentes, e desta forma ajudar a proteger os ativos e a imagem da organização.

Para isso, o Município ABC segue os critérios e caraterísticas indicadas na ISO 27035 para a identificação de um incidente. Esses critérios e caraterísticas são o Tipo de incidente, Severidade do incidente, Impacto do incidente e Nível de risco do incidente, os quais tem a seguinte definição:

- Tipo de incidente: Com base na classificação de eventos, os incidentes podem ser categorizados em tipos específicos. Por exemplo, incidentes de acesso não autorizado, incidentes de violação de dados, incidentes de malware, incidentes de ameaça interna, incidentes de negação de serviço ou incidentes de comprometimento do sistema;
- Severidade do incidente: Os incidentes podem ser avaliados com base em níveis de gravidade para determinar seu impacto na organização. Os níveis de gravidade podem incluir baixo, médio, alto ou crítico, dependendo do potencial de dano ou prejuízo causado pelo incidente;
- Impacto do Incidente: O impacto do incidente deve ser avaliado, considerando fatores como sensibilidade dos dados, alcance dos sistemas comprometidos, perda financeira, danos à reputação, implicações regulatórias ou prejuízo aos direitos de privacidade das pessoas;
- Nível de Risco do Incidente: Avaliar o nível de risco associado ao incidente ajuda a determinar o potencial de exploração adicional, a probabilidade de perda de dados ou acesso não autorizado e as obrigações de conformidade da organização.

De acordo com estes conceitos, o Município ABC entende que um incidente pode ser um único ou uma série de eventos, sejam eles, ataques de cibersegurança, desastres naturais, bem como falhas de energia ou outros incidentes indesejados ou inesperados, que tenham uma probabilidade significativa de comprometer a atividade da Autarquia e ameaçar a segurança da organização.

O Município ABC opta pelo modelo de internalização do CSIRT, com algumas adaptações, dedicado à proteção proativa e reativa contra ameaças cibernéticas, de acordo com o modelo NIST SP 800-61, para a gestão de incidentes.

O modelo NIST SP 800-61 orienta a equipa CSIRT nas fases do ciclo de vida da gestão de incidentes, desde a preparação até a atividade pós-incidente. Segue as diretrizes do NIST SP 800-61 para estabelecer políticas, processos e procedimentos de resposta a incidentes consistentes, eficientes e alinhados com as melhores práticas do setor.

Modelo Interno Centralizado para a estruturação da equipa CSIRT

Todas as funções e responsabilidades relacionadas com a resposta a incidentes de segurança estão centralizadas numa única equipa. De referir que, normalmente e neste modelo, a equipa estaria a full-time a funcionar como CSIRT, mas no caso do Município ABC, tal não é possível. Assim sendo, a equipa apenas trabalhará como CSIRT quando assim o exigir. Este modelo permite uma coordenação ágil, comunicação eficiente e alinhamento estratégico no combate a ameaças cibernéticas.

A equipa CSIRT possui papéis e responsabilidades claramente definidos, incluindo a deteção e análise de incidentes, a coordenação das atividades de resposta, a comunicação com as partes interessadas internas e externas e a implementação de medidas de mitigação e recuperação.

A posição do CSIRT, relativamente ao esquema de departamentos da organização é dentro da unidade orgânica de IT. Deste modo, funciona como um subunidade dentro daquele serviço, podendo, em casos pontuais, recorrer ao outsourcing, para apoio nas suas funções, quando necessário.

Em termos de autoridade perante o Município ABC, a equipa CSIRT tem uma autoridade partilhada, fornecendo suporte na tomada de decisões, sendo estas efetuadas pelo Presidente da Câmara Municipal.

A equipa CSIRT é constituída pelos seguintes elementos:

EQUIPA	CONTATOS	ATIVIDADES A DESEMPENHAR
HELP DESK (2 PESSOAS)	E-mail: suporte@Município ABC.pt	1. Ponto central de contato para receber suspeitas de incidentes, ou mesmo, incidentes confirmados. 2. Após uma primeira análise dos fatos apresentados, o suporte irá fazer a triagem e abrir um incidente.
INCIDENT ANALYST (1 PESSOA)	E-mail: incidentanalyst@Município ABC.pt	1. Quando notificado do incidente pelo helpdesk, tem de efetuar a investigação dos factos e determinar a natureza e o domínio do incidente. 2. Realizar uma análise ao incidente e dados relacionados. 3. Realizar análise forense para identificar a causa e os impactos 4. Trabalhar com as equipas necessárias para determinar a extensão do incidente. 5. Efetuar a mitigação do incidente e respetiva resolução. 6. Tomar medidas para prevenir futuros incidentes. 7. Monitorizar os sistemas nos próximos dias em conjunto com a equipa.
INCIDENT MANAGER (1 PESSOA)	E-mail: incidentmanager@Município ABC.pt	1. Coordenar o incidente numa perspetiva de processo. 2. Definir tarefas e monitorizar a evolução. 3. Facilitar a comunicação e colaboração entre membros de equipa. 4. Efetuar a comunicação com a gestão, stakeholders e terceiros.

Figura 50: Composição da equipa CSIRT

3. FERRAMENTA DE APOIO

A ferramenta a utilizar pela equipa CSIRT do Município ABC para gerir os incidentes é o GLPI (Gestionnaire Libre de Parc Informatique), onde é possível registar, gerir os incidentes e automatizar as respostas. Com esta ferramenta, é possível consultar informações detalhadas sobre cada incidente, tais como, descrição, categoria, prioridade e status atual. Desta forma permite uma visão completa e organizada dos incidents ativos, o que facilita a priorização e alocação de recursos adequados.

Para registo de incidentes, a equipa do IT Service Desk, utiliza os critérios abaixo indicados, para classificação do incidente, atribuição de criticidade do incidente e caraterização da situação atual do incidente.

4. CLASSIFICAÇÃO DO INCIDENTE

A cada incidente deverá ser atribuída umas das seguintes classificações:

- Conteúdo abusivo: spam, informação enganosa, fraude, etc;
- Código malicioso: bot, worm, vírus, trojan, spyware, scripts;
- Prospeção por informações: varredura, sniffing, engenharia social;
- Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;
- Intrusão: Acesso lógico indesejável, comprometimento da conta do utilizador, comprometimento da aplicação;
- Indisponibilidade de serviço ou informação: negação de Serviço, sabotagem;
- Segurança da informação: acesso não autorizado à informação, modificação não autorizada da informação;
- Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não autorizada;
- Outros: incidente não categorizado.

5. CRITICIDADE DO INCIDENTE

A cada incidente terá de ser atribuído um nível criticidade, de acordo com a lista seguinte:

- Alto (Impacto Grave) Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;
- Médio (Impacto Significativo) Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à instituição;
- Baixo (Impacto Mínimo) Possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

6. ESTADO DO INCIDENTE

Um incidente terá um dos seguintes estados:

- Aberto: Neste momento foi realizado apenas o registo das informações;
- Processamento: Quando o incidente é atribuído a um técnico e está em andamento;
- Pendente: É necessário confirmar informação antes de prosseguir. Tentativas de contacto devem ser realizadas e registadas;
- Pendente de Terceiros (Transferido): Ocorre quando uma equipa externa assumiu o incidente de forma a apoiar a organização em questão;
- Resolvido: Indica que o procedimento técnico foi aplicado e aparentemente o incidente foi resolvido;
- Fechado: Quando a solução do incidente foi confirmada. O encerramento pode ocorrer automaticamente ou por contacto.

7. ALCANCE DO PRI

O PRI é implementado em toda as unidades orgânicas da Autarquia. O PRI não será extensível a parcerias externas, como fornecedores de serviços, entre outros.

O PRI é aplicável a todos os sistemas e ativos, incluindo, servidores, redes, aplicativos, dispositivos, informações confidenciais, entre outros.

No presente PRI são considerados vários tipos de incidentes, o que pode ir, desde ataques de cibersegurança, como malware e phishing, a desastres naturais, bem como falhas de energia ou outros incidentes. Cada incidente será objeto de um processo de triagem, classificação e atribuição de um nível de criticidade.

8. PARTES INTERESSADAS

No Quadro abaixo são identificadas as partes interessadas no âmbito do PRI do Município ABC:

DEPARTAMENTO	PAPEL PRIMÁRIO	CONTATOS	DESCRIÇÃO
SERVIÇOS PARTILHADOS	Relações Públicas (1 Pessoa)	E-Mail: rp@Município ABC.pt Tel: 9XXXXXXXX	Encarregado da comunicação interna e externa durante um incidente. É responsável por comunicar as atualizações do incidente aos funcionários, clientes, parceiros de negócio, e outras partes interessadas relevantes.
	Financeiro (1 pessoa)	E-Mail: financeiro@Município ABC.pt Tel: 9XXXXXXXX	O departamento financeiro é responsável por avaliar o impacto financeiro dos incidentes de segurança. Colaboram com outras partes interessadas para garantir que os recursos financeiros necessários estejam disponíveis para tratar o incidente de segurança.
	Compras (1 pessoa)	E-Mail: compras@Município ABC.pt Tel: 9XXXXXXXX	É responsável por contactar os fornecedores, caso seja necessário a compra de hardware ou de software.
TI	Técnico de redes e telecomunicações (1 pessoa)	E-Mail: redes@Município ABC.pt Tel: 9XXXXXXXX	Faz a monitorização das redes, análise de tráfego e logs e suporte técnico durante a resposta a incidentes.
	Responsável de Segurança (1 pessoa)	E-Mail: seguranca@Município ABC.pt Tel: 9XXXXXXXX	Responsável pela deteção, análise e resposta a incidentes de segurança. Coordenam a investigação, implementam medidas corretivas e fornecem orientação sobre melhores práticas de segurança.
	DPO (1 pessoa)	E-Mail: dpo@Município ABC.pt Tel: 9XXXXXXXX	Responsável por garantir que a organização cumpra as leis e regulamentos de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR).
	Helpdesk (2 pessoas)	E-Mail: helpdesk@Município ABC.pt; Tel: 2XXXXXXXX	O Helpdesk serve como ponto central de contacto para o reportar suspeitas de incidentes, ou mesmo, incidentes confirmados.
	Responsável TI (1 pessoa)	E-Mail: ti@Município ABC.pt Tel: 9XXXXXXXX	Tomar decisões e fazer a comunicação dos acontecimentos com o resto dos departamentos. **(Ponto de Contato)**
PRESIDENTE DA CM	Líder do órgão executivo	E-Mail: presidente@Município ABC.pt Tel: 9XXXXXXXX	Realizar decisões administrativas que o líder da equipa TI não pode tomar, tais como, adjudicar compras de hardware e software, entre outras.

Figura 51: Lista dos contatos das partes interessadas

9. PROCESSO DE RESPOSTA A INCIDENTES

O processo de resposta a incidentes de segurança informática, é composto por várias fases necessárias para a resolução de um incidente.

Tendo em consideração a existência de diversos tipos de incidentes de segurança, com resoluções também elas diversas, surge a necessidade de dispor de um único plano de resposta para todos os incidentes que venham a ocorrer.

Neste sentido, é idealizado um processo de alto nível, com o objetivo de consistir numa check list ao processo como um todo, sendo, no entanto, necessário, criar procedimentos específicos e detalhados para cada tipo de incidente conhecido (os denominados playbooks), de forma a proporcionar uma resposta mais eficaz e rápida. De acordo com os processos apresentados nas diversas frameworks para SIR, tal como, ISO/IEC 27035, SANS, NIST 800-61, ENISA, ISACA, etc, e com as devidas adaptações, apresenta-se na imagem seguinte as várias fases do processo de resposta a incidentes:

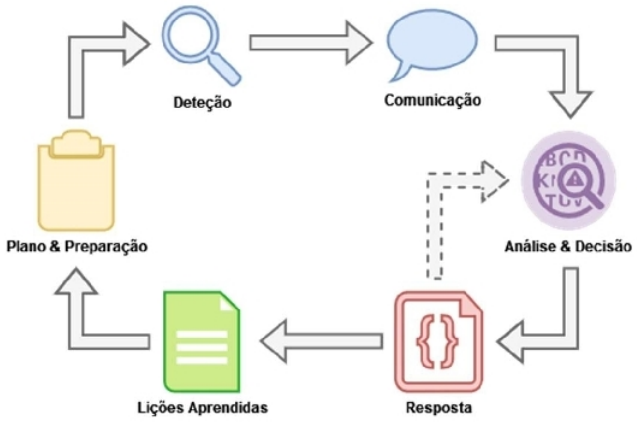


Figura 52: Processo de resposta a incidentes de segurança

O processo definido é composto por 6 fases fundamentais para a resolução de incidentes, onde cada fase contém um conjunto de ações a realizar, diferentes, ou não, dependendo do incidente em causa.

Trata-se de um processo cíclico, que deve estar em constante atualização e evolução, devido à constante alteração e inovação das ameaças, para assim manter, ou até aumentar a capacidade de resposta de todos os intervenientes.

Cada uma das fases tem o seguinte objetivo:

- Plano e Preparação - fase cuja finalidade é garantir a construção, e constante atualização do processo existente, a sua divulgação e formação dos recursos humanos pertencentes ao Município ABC, tal como, garantir que todos os intervenientes do processo se encontram esclarecidos e capazes de executar as suas tarefas, e por fim, realizar testes regulares, ou simulacros, da ocorrência de incidentes, com o intuito de treinar, melhorar e mitigar falhas no processo.
- Deteção - fase responsável pela identificação de um evento como incidente, seja por via de equipas de monitorização ou por automatização deste procedimento, capaz de emitir alertas, caso seja verificado algum evento suspeito.
- Comunicação - fase da transmissão da informação sobre o potencial incidente, aos pontos de contacto e da forma correta, com o objetivo de ser iniciado o procedimento de avaliação do evento suspeito o mais direta e rapidamente possível.
- Avaliação e Decisão - fase responsável pela análise do potencial incidente, e, em caso de confirmação, tem como tarefa a identificação do incidente, assim como, a avaliação do impacto do incidente, validando o estado e condições dos ativos afetados, recolhendo toda a informação possível, de forma a possibilitar uma correta decisão sobre qual a resposta a realizar. Com a informação recolhida é esperado, nesta fase, a identificação do tipo de incidente e o seu grau de criticidade para a organização.
- Resposta - fase técnica, responsável por lidar com o incidente, de forma mitigar os seus impactos na organização. Esta fase, pode ser vista como a possível junção de três tipos de ações, sendo estas a contenção, mitigação e recuperação, tendo como objetivo a resolução das vulnerabilidades encontradas. Onde a ação de contenção, compreende todas as tarefas de contenção dos impactos causado por um determinado incidente, a ação de mitigação, compreende todas as tarefas relacionadas a resolução das vulnerabilidades detetadas com a ocorrência de um determinado incidente, por exemplo atualização dos softwares utilizados, e por fim, temos a ação de recuperação, que compreende todas as ações de recuperação dos serviços e sistemas afetados durante um ataque detetado. No entanto, trata-se de uma fase difícil de definir, por apresentar múltiplas conjugações de ações a executar para os incidentes conhecidos, podendo ser todas necessárias, como apenas uma das ações indicadas.
- Lições Aprendidas - fase da absorção e aprendizagem dos conhecimentos obtidos com o incidente detetado e resolvido, realizando melhorias à documentação de apoio à resposta de incidentes existente, atualizando ou criando, por exemplo dos playbooks utilizados na resolução. Recomenda-se nesta fase a partilha de informação com comunidade, de forma a apoiar outras organizações que possam sofrer com os mesmos incidentes, ou similares, assim como,

o aproveitamento dos conhecimentos adquiridos para atualizar o PRI com o máximo de regularidade possível.

10. NÍVEIS DE CRITICIDADE E O PROCESSO DE TRIAGEM DOS INCIDENTES

Neste âmbito, estão definidos os níveis de severidade adotados pelo Município ABC, bem como, o processo de triagem dos incidentes. No próximo parágrafo, são descritas as diretrizes genéricas relacionadas com a definição dos níveis de criticidade dos incidentes, com o objetivo de atribuir um valor numérico aos incidentes que venham a ocorrer, de maneira a refletir o impacto e gravidade, sendo um apoio na definição de prioridades e na alocação de recursos conforme a importância e urgência de cada incidente.

As diretrizes seguidas são as seguintes:

- Identificação dos critérios a utilizar na avaliação da severidade dos incidentes de segurança, tendo em linha de conta, o impacto causado aos ativos e no funcionamento da autarquia, a sensibilidade dos dados afetados, exposição, legislação aplicável, entre outros.
- Instituição de uma escala quantitativa, que inclua os níveis de severidade representativos da gravidade dos incidentes. Esta escala deve apenas conter os níveis essenciais, de forma a facilitar o processo de triagem.
- Definição e atribuição dos critérios específicos de cada nível de severidade.
- Elaboração de documentação clara e acessível, de modo a garantir que todos os envolvidos no processo de resposta a incidentes possam compreender e aplicar consistentemente as informações nas suas tarefas.
- Avaliação e atualização contínua dos critérios utilizados, a fim de acompanhar as mudanças na autarquia e a evolução das ameaças.

Com base nas diretrizes, acima apresentadas, são definidos os seguintes critérios macro de avaliação de incidentes:

- Escala de criticidade dos incidentes: estabelecida num intervalo de 1 a 3, podendo ser adicionado o nível crítico 4, equivalente à escala qualitativa de baixa, média e alta criticidade. Essa escala deve ser aplicada a cada critério macro identificado.
- Gravidade do Incidente: Valor atribuído pelo Município ABC de acordo com a interpretação que faz do incidente em análise.
- Abrangência do impacto Dentro do Município ABC: Valor atribuído consoante a abrangência de impacto espectável, ou identificada, do incidente.

- Impacto Financeiro: Valor atribuído com base no impacto/dano financeiro esperado ou identificado do incidente. Em relação a este aspecto específico, foram introduzidos dois níveis adicionais, destinados a aumentar o valor de severidade final, com o propósito de ajustar deliberadamente a criticidade dos incidentes ocorridos, de maneira justificada.
- Obrigações Legais e Contratuais: Valor atribuído consoante a possibilidade de incumprimento das obrigações Legais e ou contratuais espectável, ou identificada, do incidente.

A tabela seguinte ilustra o nível de gravidade que poderá ser atribuído a cada incidente:

Nível Quantitativo	Nível Qualitativo	Especificidade
1	Baixo	• Interrupção limitada das operações
2	Médio	• Interrupção parcial da atividade • Acesso a contas e informações de funcionários • Falha de segurança e impacto na reputação • Corrupção de ativos humanos
3	Alto	• Interrupção significativa da atividade • Acesso aos sistemas e infraestrutura • Falha na integridade e disponibilidade dos bancos de dados • Infeção de sistemas e comprometimento de dados

Figura 53: Níveis de gravidade dos incidentes

A tabela seguinte ilustra os diferentes níveis de abrangência do impato que poderá ser atribuído a cada incidente:

Nível Quantitativo	Nível Qualitativo	Especificidade
1	Localizado	• Afeta uma área específica
2	Misto	• Afeta sistemas específicos ou todos os sistemas • Afeta contas de administrativas • Afeta sistemas que utilizam bancos de dados vulneráveis
3	Global	• Afeta todos os servidores e sistemas • Atinge todos os clientes afetados • Afeta ativos humanos • Afeta significativamente a organização

Figura 54: Níveis de abrangência dos incidentes

A tabela seguinte ilustra o nível dos impato/dano financeiro esperado ou identificado e que poderá ser atribuído a cada incidente:

A tabela seguinte ilustra os diferentes níveis a atribuir a cada incidente, conforme a possibilidade/probabilidade de incumprimento das obrigações Legais e ou regulamentares.

Para obter um valor final de criticidade global, do incidente, é alocado um peso percentual a cada critério macro existente, para refletir as prioridades do Município ABC, em relação à segurança da informação, conforme tabela seguinte:

Nível Quantitativo	Nível Qualitativo	Especificidade
1	Baixo	• Interrupção limitada das operações
2	Médio	• Interrupção parcial da atividade • Acesso a contas e informações de funcionários • Falha de segurança e impacto na reputação • Corrupção de ativos humanos
3	Alto	• Interrupção significativa da atividade • Acesso aos sistemas e infraestrutura • Falha na integridade e disponibilidade dos bancos de dados • Infeção de sistemas e comprometimento de dados

Figura 55: Níveis de impato/dano financeiro

Nível Quantitativo	Nível Qualitativo	Especificidade
1	Localizado	• Afeta uma área específica
2	Misto	• Afeta sistemas específicos ou todos os sistemas • Afeta contas de administrativas • Afeta sistemas que utilizam bancos de dados vulneráveis
3	Global	• Afeta todos os servidores e sistemas • Atinge todos os clientes afetados • Afeta ativos humanos • Afeta significativamente a organização

Figura 56: Níveis relativos ao cumprimento de obrigações legais ou regulamentares

Critério	*Peso*
Gravidade do Incidente	15 %
Abrangência do Impacto	20 %
Impacto Financeiro	25 %
Obrigações Legais e Contratuais	40 %

Figura 57: Tabela de peso percentual dos critérios

A atribuição do valor final de nível de severidade, é efetuado de acordo com o método de arredondamento apresentado na tabela seguinte:

Nível de Severidade (Decimal)	*Nível Final*
Entre 1 e 1,49	1
Entre 1.5 e 2,49	2
>= 2.5	3

Figura 58: Apuramento do nível de severidade

11. TIPIFICAÇÃO DOS INCIDENTES COM MAIOR PROBABILIDADE DE OCORRÊNCIA

Com o objetivo de tipificar, numa primeira fase, alguns dos incidentes de segurança informática com maior probabilidade de ocorrência no Município ABC devido às suas áreas de atuação, foram identificados e categorizados os incidentes abaixo apresentados.

- Phishing, incidente onde existe a tentativa ludibriar os utilizadores a divulgarem informações confidenciais, como credenciais, por via de correio eletrónico, páginas web falsas, mensagens de texto ou comunicação telefónica. Com o objetivo de obter acesso não autorizado a contas ou informação sensível.
- Acesso não autorizado, incidente onde os sistemas, serviços ou dados confidenciais da organização são acedidos de forma indevida. Esta prática pode incluir tentativa de login não autorizada, utilização de credenciais roubadas ou comprometidas, violação de políticas de acesso, entre outros.
- Ataque de Negação de Serviço ou DDoS, incidente onde os sistemas e/ou serviços são sobrecarregados, com o objetivo de os tornar inacessíveis aos utilizadores.
- Perda ou Roubo de Dados, incidente onde os dados confidenciais são perdidos, roubados ou divulgados de forma não autorizada, devido a falhas de segurança de sistemas, redes ou serviços, perda ou roubo de dispositivos, entre outros.
- Malware, incidente relacionado a softwares maliciosos, como vírus, worms, trojans, ransomware e spyware. Com o objetivo de comprometer sistemas, redes ou serviços, roubo de dados confidenciais, interrupção de serviços, dano de repotação, entre outros.
- Exploração de Vulnerabilidades, incidente onde vulnerabilidades, conhecidas ou desconhecidas, nos sistemas, aplicações ou redes são exploradas de forma maliciosa, com o objetivo de obter acesso não autorizado, execução remota de código, negação de serviço, escalonamento de privilégios, entre outros.
- Violação de Políticas de Segurança, incidente onde as políticas e diretrizes de segurança da organização são violadas pelo uso inadequado de sistemas, partilha de informação confidencial, instalação de software não autorizado, entre outros.

No âmbito do processo de comunicação dos incidentes, tem de ser seguido o Plano de comunicação de incidentes por parte da comunidade, o qual contêm regras definidas para a comunicação de incidentes.

12. PLANO DE COMUNICAÇÃO DE INCIDENTES POR PARTE DA COMUNIDADE DO MUNICÍPIO ABC

O Município ABC assume a importância de envolver a comunidade no processo de comunicação de incidentes. Este documento pretende definir um processo com as diretrizes relativamente a essa comunicação, a utilizar por parte da comunidade do Município ABC. Entende-se como comunidade do Município ABC, a comunidade local, nomeadamente, os funcionários, pessoas que vivem ou trabalham na área geográfica próxima à autarquia, munícipes e técnicos, a comunidade de parceiros e fornecedores e a comunidade online, a qual inclui, por exemplo, os utilizadores dos Serviços Online da autarquia. Canais de comunicação para relatar incidentes:

- Número de telefone dedicado: 2XX XXX XXX
- Endereço de e-mail específico: xxx@municipioABC.pt
- Formulário online disponível em...

Os referidos canais de comunicação serão divulgados no âmbito de campanhas de sensibilização a realizar anualmente, através de cartazes e flyres, e através de canais de comunicação interna, nomeadamente, na intranet do Município ABC. Nessa divulgação será explicado o procedimento de reporte de incidente, que se pretende que seja simples e acessível a todos, sendo necessário indicar apenas as seguintes informações:

- Nome;
- Contato;
- Local de origem do incidente;
- Descrição objetiva do incidente;
- Data da ocorrência;
- Hora da ocorrência.

Será dada indicação de que as informações pessoais serão tratas com confidencialidade, sendo posteriormente devolvido feedback sobre as medidas tomadas em relação aos incidentes relatados.

13. CRITÉRIOS DE ATIVAÇÃO DO BCP E DO DRP

Nos critérios de ativação do Business Continuity Plan (BCP) e do (Disaster Recovery Plan (DRP), apresentados nas figuras n.º 59 e n.º 60 seguintes, foram consideradas várias tipologias de incidentes, e são apresentados critérios que definem, para cada tipo de incidente, o nível de gravidade, o impacto nas operações, a extensão do incidente e o potencial de danos.

De modo a definir em que situações concretas são ativados os planos BCP e/ou DRP, foram introduzidas as duas variáveis: impato financeiro e duração do incidente. Assim, de acordo com o montante do impato financeiro ou tempo de duração do incidente proceder-se ou não, à a ativação do BCP e/ou DRP.

Os critérios a utilizar para ativação do BCP e DRP, são os seguintes:

- Gravidade do incidente - poderá ser alta, média ou baixa. No caso de alto nível gravidade poderá implicar interrupção total dos serviços online. Em cenário de médio nível de gravidade, implica um comprometimento da segurança e confiança dos clientes. No caso de gravidade baixa existe a possibilidade de uma interrupção limitada das operações;
- Abrangência do impato do incidente em termos geográficos e alcance das operações afetadas – A abrangência poderá ser do tipo Global, quando afeta todos os servidores e sistemas online. Poderá ser um incidente Misto (localizado/global), em que neste cenário pode afetar sistemas específicos ou todos os sistemas. Poderá ser ainda um incidente Localizado, quando é circunscrito a um único local, como por exemplo o escritório central. Por fim, podemos ter um incidente do tipo Regional/Global quando afeta várias localidades da organização.
- Impato financeiro – na tabela seguinte é definido um limiar financeiro, além do qual a ativação do BCP/DRP é obrigatória. O montante definido foi calculado apurando custos diretos, como danos em equipamentos ou interrupção do negócio (recebimentos/fluxo de caixa), ou em estimativas de perdas futuras decorrentes do incidente.
- Danos potenciais – Estes podem ser de nível Alto, aplicável aos cenários de perda de receita, danos à reputação, tempo de inatividade prolongado, violação de privacidade, danos à reputação, extorsão financeira, acesso não autorizado a sistemas críticos, manipulação de configurações, roubo de dados sensíveis, etc. Depois poderão existir danos de nível Médio, que inclui roubo

de credenciais, violação de dados pessoais, acesso não autorizado, em sistemas que não são críticos. Por fim temos o nível Baixo, o qual pode incluir, por exemplo, situações de acesso não autorizado e comprometimento limitado de dados.

- Duração da paragem de operações e ativação de BCP ou DRP – Como em alguns tipos de incidentes podem implicar paragens de curta duração, e assim podem ser mitigados rapidamente, pode não ser necessário ativar o BCP ou DRP, apenas pode exigir a ativação se persistirem por um determinado período de tempo. Na tabela seguinte são definidos os limites de tempo para a ativação do BCP e/ou do DRP com base na natureza do incidente.
- Obrigações legais ou contratuais - no Município ABC não existem atualmente obrigações legais ou contratuais que impliquem definir critérios específicos para ativação do BCP ou do DRP e assim este critério não foi incluído na tabela seguinte.

Incidente	Gravidade	Abrangência	Danos potenciais	Impato financeiro / limiar financeiro para ativação	Paragem das operações e prazo limite ativação
Ataque de negação de serviço (DDoS)	Alto	Global	Alto: Perda de receita, danos à reputação, tempo de inatividade prolongado	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 24h úteis, ativa BCP e/ou DRP
Roubo de dados pessoais de munícipes	Médio	Global	Alto: Violação de privacidade, danos à reputação, ações legais	impato financeiro > 2.000€ ativa BCP e/ou DRP	Não aplicável
Ransomware que criptografa dados	Alto	Misto: Localizado /Global	Alto: Perda de dados, extorsão financeira, tempo de inatividade prolongado	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 8h úteis, ativa BCP e/ou DRP
Ataque de phishing bem-sucedido	Médio	Global	Médio: Roubo de credenciais, violação de dados pessoais, acesso não autorizado	impato financeiro > 2.000€ ativa BCP e/ou DRP	Paragem das operações > 48h úteis, ativa BCP e/ou DRP
Exploração de vulnerabilidade conhecida	Baixo	Misto: Localizado /Global	Baixo: Acesso não autorizado, comprometimento limitado de dados, tempo de resposta moderado	impato financeiro > 3.000€ ativa BCP e/ou DRP	Paragem das operações > 24h úteis, ativa BCP e/ou DRP
Comprometimento de contas de administrador	Alto	Misto: Localizado /Global	Alto: Acesso não autorizado a sistemas críticos, manipulação de configurações, roubo de dados sensíveis	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 24h úteis, ativa BCP e/ou DRP
Exfiltração de informações confidenciais	Médio	Global	Médio: Prejuízos financeiros, violação de privacidade, danos de reputação	impato financeiro > 2.000€ ativa BCP e/ou DRP	Não aplicável

Figura 59: Critérios de ativação do BCP e DRP (cont.)

Ativar BCP e/ou DRP

Na tabela acima representada (figuras n.º 59 e n.º 60), foi considerado que segundo determinados critérios será ativado o BCP e/ou DRP.

Neste trabalho académico não foram criados os planos a seguir pela Autarquia, no caso se ser necessário ativar BCP e ou DRP, por estar for dos objetivos deste projeto.

A ativação de um ou outro plano, ou dos dois em simultâneo, vai depender da abrangência dos referidos planos.

O DRP é específico para a recuperação de desastres relacionados com infraestrutura de TI (acionado em situações em que ocorrem falhas ou danos graves nos sistemas de informação, como incêndios, falhas físicas de servidores, ciberataques

Incidente	Gravidade	Abrangência	Danos potenciais	Impato financeiro / limiar financeiro para ativação	Paragem das operações e prazo limite ativação
Ataque de injeção de código (SQL Injection)	Alto	Misto: Localizado /Global	Alto: Acesso não autorizado a informações sensíveis, corrupção de dados, interrupção de serviços	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 48h úteis, ativa BCP e/ou DRP
Ataque de engenharia social	Médio	Global	Médio: Roubo de informações confidenciais, comprometimento de contas, acesso não autorizado	impato financeiro > 2.000€ ativa BCP e/ou DRP	Paragem das operações > 36h úteis, ativa BCP e/ou DRP
Ataque de malware via e-mail (phishing, anexos maliciosos)	Médio	Global	Médio: Roubo de dados, comprometimento da segurança	impato financeiro > 2.000€ ativa BCP e/ou DRP	Paragem das operações > 36h úteis, ativa BCP e/ou DRP
Interrupção do fornecimento de energia elétrica	Alto	Localizado	Alto: Perda de dados, danos em equipamentos, interrupção prolongada	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 24h úteis, ativa BCP e/ou DRP
Inundação nas instalações administrativas	Alto	Localizado	Alto: Danos a equipamentos, custos de recuperação, interrupção prolongada	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 24h úteis, BCP e/ou DRP
Incêndio nas instalações administrativas	Alto	Localizado	Alto: Danos a prédios, perda de equipamentos, interrupção prolongada	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 24h úteis, BCP e/ou DRP
Perda ou Roubo do Dispositivo de TI	Alto	Localizado	Alto: perda de equipamentos, interrupção prolongada	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 36h úteis, ativa BCP e/ou DRP
Desastre natural (terremoto, furacão, etc.)	Alto	Regional /Global	Alto: Danos estruturais, interrupção prolongada, perda de vidas	impato financeiro > 1.000€ ativa BCP e/ou DRP	Paragem das operações > 24h úteis, BCP e/ou DRP

Figura 60: Critérios de ativação do BCP e DRP

destrutivos, entre outros), e é provável que nos tipos de incidentes mais graves, seja necessário ativar este plano.

No entanto, poderá ser necessário ativar apenas o BCP, mesmo num incidente grave. Será sempre dependente da natureza do incidente e das necessidades específicas da empresa. O BCP é geralmente acionado em eventos que causam interrupções operacionais significativas, como falhas de sistemas, indisponibilidade de recursos críticos, desastres naturais ou ataques de cibersegurança graves. O objetivo deste plano é manter as operações da autarquia em produção, mesmo em circunstâncias adversas. O BCP pode envolver ações como realocação de pessoal, ativação de sites

de backup, implementação de sistemas alternativos e comunicação com as partes interessadas relevantes.

Portanto, a decisão de ativar BCP e/ou DRP dependerá da abrangência destes planos, da natureza do incidente, do impacto nos sistemas de informação e das estratégias de recuperação definidas pela empresa. É fundamental que a autarquia tenha estes dois planos bem definidos, testados e atualizados, para conseguir lidar com diferentes cenários de interrupção e garantir a melhor resposta possível e assim dar continuidade à sua operação.

B.4 PLANO DE TESTES AO PRI

O plano seguinte contêm as regras a seguir para a realização de testes ao PRI.

Plano de testes (simulacro) ao PRI do Município ABC

O PRI deve ser testado para garantir que todas as partes interessadas são treinadas/formadas no processo. Testar o plano ajuda a identificar lacunas na capacidade de deteção e resposta. Devem realizar-se testes sempre que ocorram mudanças dos principais intervenientes ou do âmbito do PRI. Recomenda-se a realização dos testes ao plano de uma vez por trimestre. Para além do planeamento indicado no ponto quinto "Planeamento dos Testes", sempre que ocorram alterações nos principais intervenientes no PRI, deverá ser efetuado um exercício/simulacro de 60 minutos para avaliar e garantir que todas as partes interessadas estão treinadas e formadas no PRI.

- Duração - o tempo previsto para o teste/simulacro é de cerca de 60 minutos.
- Objetivos principais do simulacro:
  - Certificar que todas as partes interessadas/envolvidas compreendem o processo e conhecem qual a sua função neste processo;
  - Identificar quaisquer as lacunas na capacidade de detetar, responder e conter um incidente;
  - Identificar problemas/limitações nos processos existentes;
  - Avaliar a prontidão e a capacidade de resposta da equipe de resposta a incidentes;
  - Identificar possíveis lacunas ou melhorias a efetuar no PRI e nos seus procedimentos;
- Âmbito – o teste será conduzido em ambiente controlado, simulando incidentes de segurança. O teste abrangerá algumas áreas funcionais e sistemas críticos do Município ABC.
- Tipo de teste - o teste a efetuar será uma simulação prática de um ou mais incidente de segurança e/ou cibersegurança em ambiente controlado. Serão criados cenários realistas para avaliar a resposta da equipa e comunidade e observar a coordenação, comunicação e execução de ações de resposta. Também poderão ser adotados testes de penetração para avaliar a resistência dos sistemas de TI a ataques reais, identificar de possíveis vulnerabilidades e pontos fracos e assim efetuar a verificação da capacidade do PRI em lidar com ataques reais. As regras de preparação do tipo de teste/simulacro a realizar serão definidas num documento autónomo.

- Planeamento dos testes - o teste de simulação será realizado semestralmente e o teste de penetração será realizado anualmente.
- Análise dos resultados do simulacro – serão documentadas todas as descobertas, lições aprendidas e recomendações de melhorias. Será efetuada uma análise pós-teste para identificar pontos fortes e áreas de melhoria e posteriormente será atualizado o PRI com base nos resultados dos testes e nas recomendações.
- Monitorização e melhoria contínua – regularmente serão efetuadas revisões a este plano para garantir que está atualizado e alinhado com as ameaças mais recentes. Também serão efetuadas ações de formação internas de atualização para a equipa de resposta a incidentes.

A-Regras de preparação do tipo de teste/simulacro a realizar:

- Definição do cenário:
  - Será escolhido um ou mais incidente de segurança e/ou cibersegurança, relevante para a organização, tais como, como um ataque de ransomware ou uma situação de exfiltração de dados.
  - Serão previamente preparados os detalhes do cenário, incluindo informações sobre o tipo de ataque, os sistemas a afetar e as ações do intruso.
- Planeamento do exercício:
  - Serão definidos os objetivos específicos, métricas e indicadores de sucesso do simulacro.
  - Para cada exercício serão previamente identificados os principais participantes, incluindo membros da equipa de cibersegurança, equipa de TI, gabinete de imagem e comunicação e outros setores considerados relevantes.
  - Para cada exercício será designada uma pessoa para coordenar e conduzir o exercício.
- Comunicação:
  - Os participantes serão avisados atempadamente sobre o exercício, onde se incluirá explicação dos objetivos e o âmbito.
  - Será necessário criar um ambiente que seja seguro para a realização do exercício, e que todos os participantes percebam de que se trata de um cenário simulado.

B - Regras para realização do exercício/teste de simulação

- O exercício/simulacro consistirá nas seguintes fases/tarefas:
- Apresentar o cenário do incidente aos participantes.

- Explicar as regras e procedimentos do exercício.
- Desencadear o incidente simulado, e fornecer informações e eventos ao longo do exercício.
- Deve existir participação ativa dos membros da equipa de cibersegurança na deteção, análise e resposta ao incidente.
- Fazer análise forense e recolha de evidências.
- Efetuar mitigação e contenção do incidente.
- Restaurar os sistemas e serviços afetados.
- Efetuar comunicação interna e externa sobre o incidente.
- Avaliar impacto e avaliar e os riscos.
- Documentar todas as ações tomadas durante o exercício.
- Registar os tempos de resposta, eficácia das medidas tomadas e as lições aprendidas.

B.5 PLANO DE DIVULGAÇÃO INTERNA E FORMAÇÃO DO PRI

O plano seguinte contêm as regras definidas para a divulgação interna e formação no âmbito do PRI.

Plano de Divulgação Interna e Formação do PRI

Âmbito - com este plano pretende-se descrever as estratégias e ações necessárias para garantir que todos os funcionários do Município ABC estão cientes da existência do PRI, compreendam os procedimentos e responsabilidades, e para que estejam preparados para responder a incidentes de segurança. O objetivo principal é promover o conhecimento e a adoção efetiva do PRI em toda a autarquia.

Objetivos:

- Garantir que todos os funcionários tenham conhecimento da existência do PRI.
- Fornecer uma compreensão clara dos procedimentos e responsabilidades relacionados ao PRI.
- Promover a importância da segurança cibernética e do papel de cada indivíduo na resposta a incidentes.

Destinatários: todos os funcionários e colaboradores do Município ABC, independentemente do nível hierárquico ou unidade orgânica.

Estratégia de comunicação e formação:

- Enviar um comunicado oficial do Presidente da Câmara Municipal do Município ABC, a divulgar a implementação do PRI, abordar a importância da cibersegurança, e evidenciar os benefícios de ter um PRI e a sua contribuição para a proteção dos ativos da Município ABC;
- Organizar sessões de formação presenciais ou virtuais destinada a todos os funcionários, na qual será apresentada uma visão geral do PRI, incluindo os objetivos, componentes principais e fluxo de resposta a incidentes, bem como, as responsabilidades individuais e coletivas durante um incidente de segurança.
- Elaborar um documento ou guia informativo sobre o PRI, com informações importantes e orientações para os funcionários. Todo o conteúdo de comunicação sobre PRI deverá ser disponibilizado na intranet do Município ABC.
- Regularmente ao longo do ano, efetuar campanhas de consciencialização do PRI e também com foco em tópicos específicos de cibersegurança.

Playbook para incidente de Phishing

INTRODUÇÃO

O presente Playbook para incidente de Phishing, foi criado para funcionar como um guia de apoio na gestão de incidentes e mitigação de ameaças de phishing no Município ABC. O phishing continua a ser uma das táticas mais comuns e eficazes usadas por cibercriminosos para comprometer sistemas de informação e roubar dados sensíveis.

Dado o potencial impacto negativo de um ataque de phishing bem-sucedido, é crucial que as organizações tenham um plano claro e eficiente para responder rapidamente a esses incidentes.

Assim este playbook fornece uma abordagem sistemática para preparar, detetar, investigar, comunicar, avaliar, responder, aprender, no que concerne a incidentes de phishing.

O objetivo que é que seja prático e acionável, e assim permita que diferentes técnicos dentro da organização colaborem de maneira eficaz.

ESTRUTURA

A estrutura de construção de playbooks adotada neste trabalho, contêm um primeiro quadro com o sínteses das várias ações e uma breve descrição das mesmas e, um segundo quadro, com a descrição detalhada do que deverá ser desenvolvido em cada ação.

AÇÕES A REALIZAR NUM INCIDENTE DE PHISHING

Preparação	Deteção	Comunicação	Avaliação	Resposta	Lições Aprendidas
P-Phishing-1 Formar os utilizadores relativamente a ataques de phishing	**D-Phishing-1** Deteção do email por parte dos utilziadores.	**C-Phishing-1** Contacto pelos meios convencionais ao Helpdesk.	**A-Phishing-1** Avaliação de severidade do incidente baixa, média ou alta (1,2 e 3).	**R-Phishing-1** Eliminar o Email	**LA-Phishing-1** Mediante o grau de severidade do incidente, do tempo a que foi detetado recolher lições aprendidas
	D-Phishing-2 Análise automatizada de servidor de emails.	**C-Phishing-2** Criação de Ticket		**R-Phishing-2** Colocar um bloqueio de segurança para emails maliciosos deste tipo que encontrem similaridade com o email malicioso inicial	
				R-Phishing-3 Atualizar a Proxy Web submeter o url malicioso para ser caracterizado	
				R-Phishing-4 Alterar as credenciais do utilizador lesado no serviço em questão	
				R-Phishing-5 Monitorizar as contas lesadas por comportamentos estranhos / inadequados	

Figura 61: Ações a realizar num incidente de Phishing

DESCRIÇÃO DETALHADA DAS AÇÕES A REALIZAR NUM INCIDENTE DE PHISHING

Ações de Planeamento e Preparação	
P-Phishing-1	Formar os utilizadores relativamente a ataques de phishing. Neste sentido conduzir formações acerca de como identificar emails suspeitos, e as melhores práticas para saber lidar com técnicas de phishing. Criar emails de phishing de teste e testar a capacidade de resposta dos trabalhadores regularmente. Munir os funcionários com ferramentas com a capacidade de transformar o conteúdo do email, em texto apenas, e com capacidade de revelar os cabeçalhos dos emails. Para o efeito criar manuais de utilização de caixa de email para melhor deteção.
Ações de Deteção	
D-Phishing-1	Deteção do email por parte do colaborador.
D-Phishing-2	Análise automatizada de servidor de emails.
Ações de Comunicação	
C-Phishing-1	Contacto pelos meios convencionais ao Helpdesk.
C-Phishing-2	Criação de Ticket.
Ações de Análise e Avaliação	
A-Phishing-1	Avaliação de severidade do incidente baixa, média ou alta (1,2 e 3). Em que severidade baixa se aplica quando apenas 1 a 3 contas de email internas foram afetas, média quando 50 ou mais contas de email internas foram afetadas, e alta quando foram afetas contas de email de partes interessadas do Município ABC. A Avaliação de severidade também pode ser feita com base nas repercussões do incidente, ou seja, quando não existem repercussões detetadas trata-se de um evento de severidade baixa, quando existem repercussões em serviços ou sistemas não cruciais média, e para casos em que serviços ou sistemas cruciais sejam afetados, alta.
Ações de Resposta	
R-Phishing-1	Eliminar o Email.
R-Phishing-2	Colocar um bloqueio de segurança para emails maliciosos deste tipo que encontrem similaridade com o email malicioso inicial.
R-Phishing-3	Atualizar a Proxy Web submeter o url malicioso para ser caracterizado.
R-Phishing-4	Alterar as credenciais do utilizador lesado no serviço em questão.
R-Phishing-5	Monitorizar as contas lesadas por comportamentos estranhos / inadequados.
Ações de Documentação das Lições Aprendidas	
LA-Phishing-1	Mediante o grau de severidade do incidente, do tempo a que foi detetado recolher lições aprendidas. Se o grau de severidade é baixo pode significar que as campanhas estão a produzir efeito (especialmente se existem vários utilizadores a detetar previamente o incidente). Caso o grau de severidade seja médio pode significar que as campanhas não estão a fazer o efeito desejado, ou que os testes não são robustos o suficiente. Caso se trate de um grau de severidade alto pode significar que os ataques de phishing estão mais sofisticados pode ser necessário adaptar as campanhas e testes de ataques de phishing nesse sentido.

Figura 62: Descrição detalhada das ações a realizar num incidente de Phishing

B.7 PLAYBOOK PARA INCIDENTE DE ACESSO NÃO AUTORIZADO

Playbook para incidente de Acesso Não Autorizado

INTRODUÇÃO

ESTRUTURA

A estrutura de construção de playbooks adotada neste trabalho, contêm um primeiro quadro com o sínteses das várias ações e uma breve descrição das mesmas e, um segundo quadro, com a descrição detalhada do que deverá ser desenvolvido em cada ação.

AÇÕES A REALIZAR NUM INCIDENTE DE ACESSO NÃO AUTORIZADO

O presente Playbook para incidentes de Acesso Não Autorizado foi criado para funcionar como um guia de apoio na gestão de incidentes e mitigação de ameaças de acesso não autorizado no Município ABC. O acesso não autorizado continua a ser uma das táticas mais comuns e eficazes usadas por cibercriminosos para comprometer sistemas de informação e roubar dados sensíveis.

Dado o potencial impacto negativo de um incidente de acesso não autorizado bem-sucedido, é crucial que as organizações tenham um plano claro e eficiente para responder rapidamente a esses incidentes.

Assim, este Playbook fornece uma abordagem sistemática para preparar, detetar, investigar, comunicar, avaliar, responder e aprender no que concerne a incidentes de acesso não autorizado.

O objetivo é que seja prático e acionável, permitindo que diferentes técnicos dentro da organização colaborem de maneira eficaz.

Preparação	Deteção	Comunicação	Avaliação	Resposta	Lições Aprendidas
P-Acesso-1 Implementar Política de Passwords Forte	**D-Acesso-1** Análise de Log	**C-Acesso-1** Comunicação com o grupo de HelpDesk.	**A-Acesso-1** Conforme o sistema ou serviço comprometido é feita uma avaliação de severidade do incidente.	**R-Acesso-1** Eliminar a conta comprometida em questão e se necessário recriar a conta.	**LA- Acesso -1** Mediante o grau de severidade do incidente, do tempo a que foi detetado recolher lições aprendidas
P-Acesso-2 Utilizar dois fatores de autenticação	**D-Acesso-2** Alertas com base em regras	**C-Acesso-2** Criação de Ticket e efetuar a comunicação direta com o gestor de incidentes.		**R-Acesso-2** Alterar as credenciais de acesso á conta vulnerável	
P-Acesso-3 Práticas de Segurança Física	**D-Acesso-3** Analíticas de comportamento			**R-Acesso-3** Criar regras que espoletem alertas	
P-Acesso-4 Monitorizar atividade dos utilizadores				**R-Acesso-4** Atualizar os modelos responsáveis pelo UEBA	
P-Accesso-5 Aplicação de segurança nos serviços disponibilizados				**R-Acesso-5** Monitorizar as máquinas ou serviços afetados	

Figura 63: Ações a realizar num incidente de Acesso Não Autorizado

DESCRIÇÃO DETALHADA DAS AÇÕES A REALIZAR NUM INCIDENTE DE ACESSO NÃO AUTORIZADO

Ações de Planeamento e Preparação	
P-Acesso-1	Os utilizadores devem ser formados no sentido utilizar passwords seguras: passwords longas, com letras, com números, com caracteres especiais. Mudar as passwords frequentemente, evitar termos generalistas que possam facilitar os ataques de força bruta, evitar partilhar password com mais de um sistema.
P-Acesso-2	Usar sistemas ou implementar sistemas que requeiram dois fatores de autenticação, que tornem mais difíceis os acessos ilegítimos a sistemas. Se necessário treinar e formar os utilizadores.
P-Acesso-3	Treinar e formar os utilizadores para fecharem sempre os seus dispositivos portáteis, e inclusive desligando-os quando não estejam presentes. Evitar escrever passwords em locais visíveis ou de fácil acesso. Ter uma política clara de horário de funcionamento do escritório, mantendo-o fechado sem a presença de pessoal autorizado e restringir o acesso a áreas sensíveis.
P-Acesso-4	Monitorizar a atividade dos utilizadores é importante para manter registo das entradas e saídas de serviços e sistemas para desta forma monitorizar comportamentos fora do comum. Manter uma análise de registos (logs) dos sistemas, criar regras de alertas para avisar os analistas de segurança de várias tentativas de login ou de sistemas sensíveis.
P-Acesso-5	Implementar mecanismos de segurança do endpoint, seja ele um servidor ou computador terminal, de modo a manter a utilização destes equipamentos alinhada com as políticas do Município ABC. Podem aqui ser usados por exemplo "Endpoint Detection and Response" (EDRs).
Ações de Deteção	
D-Acesso-1	A deteção com base em logs pode acontecer a qualquer momento inclusive numa análise forense, ou quando um analista de segurança ou outro técnico, deteta um registo fora do normal.
D-Acesso-2	A detenção com recurso a regras acontece quando uma ferramenta de segurança alerta o analista de segurança de atividades ou padrões de comportamento suspeitos, tais como múltiplas tentativas de login para sistemas sensíveis.
D-Acesso-3	Outra forma de deteção pode ocorrer com recurso a analíticas de comportamento de utilizadores ou eventos, ou seja, quando o comportamento de um utilizador ou sistema sai fora do seu padrão de comportamento normal e pré-estabelecido são difundidos alertas que indicam a atividade anormal que pode revelar-se maliciosa.
Ações de Comunicação	
C-Acesso-1	Comunicação com o grupo de HelpDesk.
C-Acesso-2	É criado um ticket e é enviada uma comunicação direta ao Gestor de Incidentes.
Ações de Análise e Avaliação	
A-Acesso-1	A avaliação da gravidade do incidente deve ser feita pelo gestor de analistas de segurança de nível 2, para que este possa determinar qual o nível de importância do sistema ou máquina comprometida. As permissões dadas à conta ou máquina são determinantes no sentido de fazer uma correta avaliação.
Ações de Resposta	
R-Acesso-1	Eliminar a conta comprometida em questão e recriar a mesma.
R-Acesso-2	Alterar as credenciais de acesso à conta vulnerável. Caso o nível de severidade do incidente seja baixo devem ser alteradas as credenciais de acesso à máquina ou serviço em questão.
R-Acesso-3	Criar regras que espoletem alertas após deteção do incidente. Independentemente da sua severidade as regras que espoletam alertas têm de ser atualizadas para que os analistas de segurança possam ser avisados atempadamente, no caso de outro evento similar.
R-Acesso-4	Devem ser atualizados de forma contínua os modelos responsáveis pelo UEBA (análise de comportamento de utilizadores). No caso de se tratar de um incidente de severidade alta deve-se fazer uma introspetiva ao que aconteceu, para evitar que aconteça novamente.
R-Acesso-5	Monitorizar as máquinas ou serviços afetados.
Ações de Documentação das Lições Aprendidas	
LA-Acesso-1	Mediante o grau de severidade do incidente, do tempo a que foi detetado recolher lições aprendidas e analisar o que falhou: o Foi ignorado algum alerta? o O sistema UEBA não detetou? o Foram colocados modelos UEBA em produção antes de serem testados?

Figura 64: Descrição detalhada das ações a realizar num incidente de Acesso Não Autorizado

B.8 PLAYBOOK PARA INCIDENTE DE RANSOMWARE

Playbook para incidente de Ransomware

INTRODUÇÃO

O presente Playbook para incidentes de Ransomware foi criado para funcionar como um guia de apoio na gestão de incidentes e mitigação de ameaças de ransomware no Município ABC. O ransomware tem sido uma tática comum usada por cibercriminosos para comprometer sistemas de informação e extorquir dinheiro em troca da devolução do acesso a dados críticos das organizações.

Dado o potencial impacto negativo de um ataque de ransomware bem-sucedido, é muito importante que os municípios tenham um plano claro e eficiente para responder rapidamente a esses incidentes.

Assim, este Playbook fornece uma abordagem sistemática para preparar, detetar, investigar, comunicar, avaliar, responder e aprender no que concerne a incidentes de ransomware.

O objetivo é que seja prático e acionável, permitindo que diferentes técnicos dentro da organização colaborem de maneira eficaz.

ESTRUTURA

A estrutura de construção de playbooks adotada neste trabalho, contêm um primeiro quadro com o sínteses das várias ações e uma breve descrição das mesmas e, um segundo quadro, com a descrição detalhada do que deverá ser desenvolvido em cada ação.

AÇÕES A REALIZAR NUM INCIDENTE DE RANSOMWARE

Preparação	Deteção	Comunicação	Avaliação	Resposta	Lições Aprendidas
P-Ransomware-1 Assegurar que todos os sistemas estão atualizados	**D-Ransomware-1** Tentativas de reconhecimento, acesso inicial a máquinas	**C-Acesso-1** Comunicação à equipa de HelpDesk.	**A-Ransomware-1** Avaliar a a fase em que se encontra o ataque de Ransomware	**R-Ransomware-1** Isolar e conter	**LA-Ransomware-1** Fazer atualizações no plano de resposta a incidentes
P-Ransomware-2 Implementar Sistemas de Backup	**D-Ransomware-2** Detetar tentativas de acessos não autorizados a sistemas	**C-Acesso-2** Criação de Ticket e efetuar a comunicação direta com o gestor de incidentes.		**R-Ransomware-2** Preservar. Recolher evidencias	
P-Ransomware-3 Formar os analistas de segurança relativamente a sinais prévios de identificação	**D-Ransomware-3** Deteção de mudanças nos ficheiros registry			**R-Ransomware-3** Restaurar Backups	
P-Ransomware-4 Identificar vulnerabilidades nos recursos	**D-Ransomware-4** Deteção de portos abertos suspeitos				
P-Ransomware-5 Testar e validar	**D-Ransomware-5** Deteção de serviços em execução suspeitos				

Figura 65: Ações a realizar num incidente de Ransomware

DESCRIÇÃO DETALHADA DAS AÇÕES A REALIZAR NUM INCIDENTE DE RANSOMWARE

Ações de Planeamento e Preparação	
P-Ransomware-1	Assegurar que todos os sistemas estão atualizados com as últimas versões de software: antivírus, firewalls e sistemas de deteção de intrusões.Verificar regularmente por atualizações, ou patchs que destinados a mitigar vulnerabilidades.
P-Ransomware-2	Implementar backups e testar sitemas de backups em cenários de desastre, para minimizar o impacto de ataques ransomware.
P-Ransomware-3	Formar os analistas de segurança relativamente a sinais de ransomware, tais como, tráfego de rede incomum, execução de ficheiros anormais e demasiados renomeações de nomes de ficheiros, cifragem de ficheiros efetuada de forma não habitual, portas abertas em máquinas onde estas não são esperadas, etc.
P-Ransomware-4	Manter os analistas de segurança formados relativamente a vulnerabilidades dos sistemas, e dar-lhes formação na maneira de detetar estas vulnerabilidades.
P-Ransomware-5	Regularmente testar e validar a eficácia da resposta a este tipos de incidentes através de cenários, onde sejam identificadas as áreas de melhoria.
Ações de Deteção	
D-Ransomware-1	Numa fase inicial de um ataque ransomware os atacantes usam técnicas categorizadas por Reconhecimento, Desenvolvimento de Recursos, e Acesso Inicial e táticas da framework MITRE ATT&CK.
D-Ransomware-2	Detetar tentativas de acessos não autorizados a sistemas. Detetar escalanomanento de privilégios que sejam suspeitos.
D-Ransomware-3	Deteção de mudanças suspeitas em ficheiros registry.
D-Ransomware-4	Deteção de portos abertos suspeitos.
D-Ransomwara-5	Deteção de serviços em execução suspeitos.
Ações de Comunicação	
C-Ransomware-1	Comunicação à equipa de HelpDesk.
C-Ransomware-2	Criação de Ticket e efetuar comunicação direta com o gestor de incidentes.
Ações de Análise e Avaliação	
A-Ransomware-1	Avaliar a gravidade do incidente, em 5 fases: 1. A rede é comprometida por meio de um email de phishing, exploração ou Worm, de gravidade baixa ou média mediante as contas a afetadas e extensão do incidente. 2. Uma vez dentro da rede, o ransomware estabelece uma conexão com o servidor de comando e controle do atacante para receber instruções, sendo esta fase de gravidade alta. 3. Ainda não detetado, o ransomware continua a preparar para o seu ataque através do roubo credenciais e ganhando acesso a mais contas na rede, sendo esta fase de gravidade alta. 4. O ransomware procura por arquivos para criptografar, tanto no computador local como nas redes às quais ele obteve acesso por meio de movimentação lateral, sendo esta fase de gravidade alta. 5. Os criminosos pretendem cifrar os dados de máquinas ou sistemas locais e da rede, sendo esta fase de gravidade alta.
Ações de Resposta	
R-Ransomware-1	Isolar e conter este tipo de resposta pressupõem isolar os sistemas ou máquinas afetadas da rede para evitar uma maior propagação do ransomware. Nesta resposta ao incidente são desconectadas as máquinas afetadas da internet e é desligado o Wi-FI e bluethooth para minimizar os danos dentro da infraestrutura.
R-Ransomware-2	Preservar evidências. É importante documentar o máximo de informação, como timestamps e outros indicadores de comprometimento. Procurar preserver logs, tráfego de rede e outros dados potenciais para serem utilizados numa análise forense posterior, bem como para relato às autoridades competentes.
R-Ransomware-3	Restaurar Backups.Dever ser assegurado que os backups estão limpos e livres de qualquer ransomware.
Ações de Documentação das Lições Aprendidas	
LA-Ransomware-1	Com base nas lições aprendidas devem ser revistos os controlos de segurança, e se necessário deve ser atualizado o plano de resposta a incidentes.

Figura 66: Descrição detalhada das ações a realizar num incidente de Ransomware

DECLARAÇÃO

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"Plano de implementação de um SGSI, baseado no QNRCS, em municípios de pequena e média dimensão"*, é original e foi realizado por Estudante Pedro Miguel Gonçalves Marques (2220289) sob orientação de Professor Doutor Leonel Filipe Simões Santos (leonel.santos@ipleiria.pt) e coorientação do Professor Especialista Carlos Manuel Gonçalves Antunes (carlos.antunes@ipleiria.pt).

Leiria, Setembro de 2024

Estudante Pedro Miguel Gonçalves Marques