POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Versão e aprovação

Versão:	Aprovado em:	Deliberação:
1	Reunião de Câmara Municipal Ordinária Pública	N.º 522 de 17/09/2025

Índice

Acrónimos

CMB – Câmara Municipal do Barreiro

CNCS – Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

PSI – Política de Segurança de Informação

QNRCS – Quadro Nacional de Referência para a Cibersegurança

RGPD – Regulamento Geral de Proteção de dados

SMTCB – Serviços Municipalizados dos Transportes Coletivos do Barreiro

TI – Tecnologias de Informação

TO – Tecnologias da Operação

1 INTRODUÇÃO

A política de segurança da informação (PSI) é uma estrutura, que define as diretrizes, procedimentos e práticas que a Câmara Municipal do Barreiro (CMB) deve adotar para proteger os seus ativos e recursos de informação contra ameaças e garantir a confidencialidade, integridade e disponibilidade dos dados.

Esta PSI é essencial para minimizar riscos e garantir a conformidade com as regulamentações aplicáveis.

A segurança da informação é de fundamental importância na era digital em que vivemos, abrangendo a proteção de sistemas de informação, redes, dispositivos e dados, contra-ataques, acessos não autorizados, danos ou qualquer outra ameaça cibernética e operacional que possa comprometer a confidencialidade, integridade e disponibilidade das informações e sistemas.

Quando aplicada a um organismo público do Estado, a segurança da informação ganha ainda mais relevância, uma vez que essas instituições são responsáveis por gerir uma quantidade significativa de informações sensíveis e críticas. A seguir, destacam-se alguns pontos essenciais sobre a importância da segurança da informação em organismos públicos:

- Proteção de informações sensíveis: Os organismos públicos do Estado lidam com uma vasta gama de informações sensíveis, incluindo dados pessoais de cidadãos, informações financeiras, documentos governamentais, segredos diplomáticos e dados estratégicos. A segurança da informação é crucial para proteger essas informações contra acessos não autorizados, extração ou manipulações indevidas, garantindo a sua confidencialidade e integridade.
- Salvaguarda da soberania nacional: O estado é responsável pela defesa da soberania nacional, e a segurança da informação é fundamental para proteger os sistemas de defesa, inteligência e infraestrutura crítica contra ameaças cibernéticas que possam visar o enfraquecimento do país ou a obtenção de informações estratégicas.
- Continuidade dos serviços governamentais: Os organismos públicos fornecem serviços essenciais aos cidadãos, como saúde, educação, segurança pública, proteção social e muito mais. A segurança da informação é fundamental para assegurar que esses serviços permaneçam operacionais e ininterruptos, evitando ataques que possam comprometer o funcionamento das instituições e a qualidade da prestação de serviços aos cidadãos.

- Transparência e responsabilidade: A segurança da informação está igualmente ligada à transparência e à responsabilidade do Estado. Garantir a integridade dos dados públicos, protegendo-os contra adulterações, é essencial para manter a confiança dos cidadãos nas instituições governamentais, assegurando que as informações oficiais sejam precisas e confiáveis.
- Defesa contra ataques cibernéticos sofisticados: Os organismos públicos do estado podem ser alvos de ataques cibernéticos sofisticados, incluindo ataques de nações estrangeiras, grupos de hackers e cibercriminosos. A segurança da informação deve ser capaz de detetar e responder a essas ameaças de forma proativa, garantindo a proteção dos sistemas e das informações do governo.

Em suma, a segurança da informação é essencial para proteger as informações, serviços e infraestruturas governamentais, salvaguardar a soberania nacional, promover a transparência e a responsabilidade, além de manter a confiança dos cidadãos nas instituições públicas do Estado.

2 POLÍTICA DE INFORMAÇÃO

2.1 Princípios

A PSI da CMB e dos Serviços Municipalizados e empresas municipais (SMTCB), tem como objetivo estabelecer diretrizes, procedimentos e medidas para proteger as informações, os sistemas de tecnologia da informação (TI) e os sistemas de tecnologia da operação (TO) contra ameaças cibernéticas e garantir a integridade, confidencialidade e disponibilidade dos dados da autarquia.

2.2 Objetivos

Alguns dos principais objetivos de uma política de segurança de informação são:

- Proteger a infraestrutura crítica: A autarquia possui infraestruturas de serviços essenciais, como abastecimento de água potável, e os SMTCB como operadores de transporte público rodoviário que são vitais para o funcionamento da sociedade. A política de segurança de informação visa proteger essas infraestruturas contra-ataques cibernéticos que possam causar disrupções significativas e danos à sociedade.
- Fortalecer a defesa nacional e a segurança interna: A política visa proteger os sistemas de defesa e inteligência contra ameaças cibernéticas que possam comprometer informações estratégicas ou enfraquecer a segurança nacional.

- Conformidade com leis e regulamentações: A política procura garantir que o organismo do Estado esteja em conformidade com as leis e regulamentações relacionadas à proteção de dados e segurança da informação.
- Sensibilização e formação: A política deve incluir medidas para aumentar a sensibilização e consciencialização dos funcionários sobre boas práticas de segurança, promovendo formação regular e ações educativas para evitar erros humanos e comportamentos de risco.
- Resposta a incidentes: A política deve incluir um plano abrangente de resposta a incidentes de segurança, detalhando procedimentos claros e padronizados a serem adotados em caso de violações de segurança ou ataques cibernéticos. Esse plano deve garantir uma atuação rápida e eficaz para mitigar danos, identificar vulnerabilidades e restabelecer a normalidade de forma segura.

2.3 Âmbito

Esta política abrange todos os colaboradores de todas as áreas e em todas as posições hierarquias, contratados, estagiários e fornecedores na cadeia de abastecimento que tenham acesso aos sistemas e informações da CMB e SMTCB, independentemente da localização física ou tecnológica. A PSI aplica-se a todas as formas de informação, incluindo dados em papel, eletrónicos, sistemas de TI e TO, e-mails, dispositivos móveis e qualquer outra forma de armazenamento e processamento de dados utilizada na autarquia.

2.4 Responsabilidades e compromisso da Câmara

A definição de responsabilidades na política de segurança da informação é fundamental para garantir a efetiva implementação e gestão das medidas de segurança.

A governação da Câmara Municipal do Barreiro engloba a presidência, vereadores, chefias intermédias de 1º, 2º e 3º nível, secretários, etc. e tem a responsabilidade de demonstrar um compromisso firme com a segurança da informação. Para além de aprovar a política de segurança da informação, fornecem os recursos adequados para a sua implementação e para estabelecer uma cultura organizacional que valorize a segurança da informação.

Na estrutura organizativa da CMB também está assegurada a função de Responsável de Segurança, que tem a responsabilidade por desenvolver, implementar e monitorizar a política de segurança da informação, coordenar a equipa de segurança, garantir que as medidas de segurança sejam adequadamente aplicadas em toda a organização e assegurar o contacto com o Centro Nacional de Cibsesegurança.

Desta forma, a Câmara Municipal do Barreiro, compromete-se a:

a) Garantir a segurança da informação que titula, assim como de todos os recursos a ela associados, sejam eles processuais, tecnológicos ou humanos;
b) Assegurar o estabelecimento e a prossecução dos princípios descritos nesta política, bem como a sua aprovação, publicação, comunicação a todos os colaboradores e entidades externas relevantes;
c) Garantir os recursos necessários para a operacionalização dos processos e atividades de gestão da segurança da informação;
d) Assegurar a definição, implementação e revisão da estratégia de gestão de segurança da informação e garantir o correto alinhamento com as políticas, objetivos e compromissos da Câmara;
e) Assegurar que o Sistema de Gestão de Segurança da Informação atinge os resultados pretendidos, mediante processos de monitorização constante e auditorias internas regulares.
f) Promover, de forma estruturada e sistemática, a melhoria contínua do Sistema de Gestão de Segurança da Informação da Câmara.

3 DOMÍNIOS DA SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação estabelece os princípios e orientações estratégicas que refletem a forma como a Câmara protege e gere a informação, assegurando a sua confidencialidade, integridade e disponibilidade.

Este documento define ainda os mecanismos de governação aplicáveis aos principais domínios da segurança da informação, servindo como referência para colaboradores, fornecedores e demais partes interessadas.

3.1 Gestão de Identidades e Acessos

A gestão de identidades e acessos da CMB e SMTCB tem como objetivo garantir que os utilizadores tenham acesso adequado e mínimos indispensáveis (princípio de privilégios mínimos) aos recursos de TI e TO para desempenhar as suas funções, enquanto protege os ativos de informação contra acessos não autorizados e garante a conformidade com as normas e regulamentações relevantes.

3.2 Classificação da Informação

A política de classificação de informação da CMB e SMTCB tem como objetivo estabelecer diretrizes para a correta classificação das informações, garantindo a proteção adequada das informações sensíveis, confidenciais e estratégicas sob a responsabilidade do organismo. A classificação adequada das informações permite uma

gestão eficaz dos riscos de segurança da informação, bem como a proteção dos direitos de privacidade e segurança do município e dos cidadãos.

3.3 Proteção de Dados e Privacidade

A política de proteção de dados e privacidade da CMB e SMTCB tem como objetivo garantir a proteção adequada dos dados pessoais e a privacidade dos cidadãos e demais titulares de dados com os quais o organismo interage. Esta política é fundamentada nas leis e regulamentos aplicáveis, incluindo o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia.

Esta política abrange todos os dados pessoais recolhidos, processados e armazenados pela CMB e SMTCB no exercício das suas funções e missões. Isso incluí dados de colaboradores, cidadãos, fornecedores na cadeia de abastecimento e quaisquer outras partes com as quais o organismo interaja.

3.4 Segurança da Rede e Sistemas

A segurança da rede e sistemas tem como objetivo proteger a infraestrutura de TI e TO e sistemas contra ameaças cibernéticas, garantindo a disponibilidade, integridade e confidencialidade dos dados. Esta política é baseada nas normas internacionais reconhecidas e normas nacionais como o Quadro Nacional de Referência para a cibersegurança (QNRCS), bem como nas melhores práticas do setor.

Esta política abrange toda a infraestrutura de rede e sistemas da Câmara Municipal do Barreiro, incluindo redes internas e externas, servidores, dispositivos de armazenamento, equipamentos de rede, sistemas operativos e aplicações utilizadas pela autarquia nas suas variadas atividades e setores.

3.5 Relação com os fornecedores

Os fornecedores que prestam serviços ou fornecem bens à Câmara Municipal do Barreiro são avaliados de forma sistemática e criteriosa, com o objetivo de assegurar que as relações contratuais estabelecidas contribuem para a proteção da informação, a continuidade das operações e o acesso a matérias e serviços adequados às necessidades do negócio.

Deste modo, reconhece-se que os fornecedores, pela sua posição na cadeia de abastecimento, podem representar potenciais riscos para a segurança da informação e para a continuidade das operações, pelo que a sua avaliação e monitorização contínuas são fundamentais para mitigar vulnerabilidades e reforçar a resiliência da Câmara Municipal do Barreiro.

3.6 Deteção atempada e Gestão de Incidentes

A política de deteção e gestão de incidentes de segurança tem como objetivo estabelecer um processo eficiente e coordenado para monitorização, deteção, resposta, recuperação, investigação e mitigação de incidentes de segurança da informação. Esta política está ainda em conformidade com o Quadro Nacional de Referência para a Cibersegurança (QNRCS) do Centro Nacional de Cibersegurança (CNCS), tem como base as melhores práticas do setor e cumpre com todos os requisitos exigidos pela legislação nacional nesta matéria.

3.7 Segurança Física e Ambiental

A segurança física é essencial para proteger os ativos tangíveis do Município, incluindo pessoas, instalações e equipamentos, contra ameaças físicas. Esta seção define as medidas e procedimentos necessários para garantir a proteção física dos recursos da empresa.

Esta política aplica-se a todas as instalações, equipamentos e colaboradores da CMB e SMTCB. Inclui medidas de controlo de acesso, proteção de equipamentos, segurança das instalações, ambientes seguros, procedimentos de emergência e manutenção de sistemas de segurança.

3.8 Resiliência e Continuidade das Operações

Resiliência é a capacidade de recuperação e adaptação a mudanças, adversidades, crises ou choques sem perder a sua estrutura fundamental e manter o seu funcionamento normal ou próximo do normal. A resiliência é uma característica crítica para proteger ativos, dados e operações em ambientes, onde ameaças cibernéticas e eventos inesperados podem ocorrer a qualquer momento.

No contexto da cibersegurança, a Câmara dispõe de mecanismos que lhe permite manter a sua operação normal ou recuperar rapidamente após a ocorrência de um ataque cibernético, de uma falha de hardware ou de qualquer outro evento suscetível de provocar interrupções ou perda de dados. Para tal, estão implementados planos de continuidade de negócio e de recuperação de desastres que garantem a resiliência dos serviços essenciais. A continuidade da Segurança da Informação é assim assegurada através de medidas preventivas e de recuperação, integradas na estratégia global de continuidade da Câmara.

4 SENSIBILIZAÇÃO E FORMAÇÃO

A segurança da informação é um pilar fundamental para a proteção dos ativos digitais e a continuidade dos serviços da CMB e dos SMTCB. Para garantir a eficácia das medidas de segurança implementadas, todos os colaboradores estão devidamente informados e conscientes dos riscos associados à segurança da informação, bem como das melhores práticas para mitigá-los. A formação e a sensibilização contínuas são cruciais para criar uma cultura de segurança robusta e proativa, onde cada indivíduo compreende o seu papel e responsabilidade na proteção dos dados e sistemas da organização.

É ainda assegurado que todos os colaboradores e partes interessadas da CMB e dos SMTCB, de forma periódica, recebem formação e participam em ações de sensibilização.

5 CONFORMIDADE LEGAL

O Sistema de Gestão de Segurança da Informação da Câmara Municipal do Barreiro encontra-se estruturado de forma a assegurar o cumprimento das obrigações legais, regulamentares e normativas aplicáveis, garantindo que a proteção da informação é realizada em conformidade com as melhores práticas nacionais e internacionais.

Neste âmbito, são observadas as disposições emanadas por entidades e referenciais relevantes, nomeadamente:

a) Centro Nacional de Cibersegurança (CNCS) e o Quadro Nacional de Referência para a Cibersegurança (QNRCS);
b) Comissão Nacional de Proteção de Dados (CNPD) e legislação nacional em matéria de proteção de dados;
c) Resolução do Conselho de Ministros n.º 41/2018, que aprova a Estratégia Nacional de Segurança do Ciberespaço;
d) Lei n.º 46/2018, relativa à segurança do ciberespaço;
e) Decreto-Lei n.º 65/2021, que estabelece os requisitos de segurança das redes e sistemas de informação e, por outro lado, as regras para a notificação de incidentes ao CNCS;
f) Referenciais internacionais de gestão e boas práticas, nomeadamente as normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005.

Adicionalmente, o SGSI considera as diretivas e regulamentações europeias relevantes, em particular a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 (NIS2), que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança na União Europeia.

O compromisso com a conformidade legal e normativa assegura não apenas a mitigação de riscos de sanções, mas sobretudo a criação de um ambiente de confiança, resiliência e alinhamento com os requisitos exigidos para a gestão segura da informação no setor público.

6 REVISÃO, ATUALIZAÇÃO E COMUNICAÇÃO

Esta política é revista periodicamente para garantir que continua a atender às necessidades de segurança de informação da CMB e SMTCB e se encontra em conformidade com as leis e regulamentações relevantes. Esta responsabilidade recai sobre o Responsável de Segurança da CMB em estreita ligação aos Órgãos Executivas.

7 DISPOSIÇÕES FINAIS

O cumprimento desta política é obrigatório para todos os utilizadores, funcionários, colaboradores e partes interessadas da CMB e SMTCB. O não cumprimento desta política pode resultar em ações disciplinares, conforme previsto nas políticas internas da organização.

8 ENTRADA EM VIGOR

A política de segurança da informação entra em vigor na data do despacho do senhor Presidente da Câmara Municipal do Barreiro.