Política da Segurança da Informação

USO PÚBLICO

Classificação Documento:	**Uso Público**
Referência Documento:	**A05.4/CMM**
Versão:	**1**
Data:	**02/12/2024**
Autor Documento:	**DSI**
Dono Documento:	**CMM**

Histórico de Revisão

Versão	Data	Autor Revisão	Sumário de Alterações

Distribuição

Nome	Título
DSI	Departamento de Sistemas de Informação

Aprovação

CARLOS MANUEL AMORIM DA MOUTA

Assinado de forma digital por CARLOS MANUEL AMORIM DA MOUTA
Dados: 2025.01.10 19:26:21 Z

USO PÚBLICO

Índice

Lista de Tabelas

USO PÚBLICO

1 Introdução

Este documento define a política de segurança da informação do Departamento Sistemas de Informação (DSI) da Câmara Municipal de Matosinhos.

Como uma administração pública moderna e voltada para o futuro, a Câmara Municipal de Matosinhos reconhece nos níveis seniores a necessidade de garantir que as suas atividades e serviços operem sem problemas e sem interrupções para o benefício dos seus munícipes, colaboradores e outras partes interessadas.

A fim de fornecer este nível de operação contínua, a Câmara Municipal de Matosinhos implementou um Sistema de Gestão da Segurança da Informação (SGSI) em linha com a Norma Internacional para Segurança da Informação, ISO / IEC 27001:2022. Esta norma define os requisitos para um SGSI com base em melhores práticas reconhecidas internacionalmente.

A operação do SGSI traz muitos benefícios para a atividade da Câmara Municipal de Matosinhos, incluindo:

- Garantir o fornecimento de bens e serviços aos munícipes de forma eficaz e segura;
- Conformidade com os requisitos legais e regulamentares.

A Câmara Municipal de Matosinhos decidiu obter certificação completa para ISO / IEC 27001:2022 no DSI para que a adoção efetiva das melhores práticas de segurança da informação possa ser validada por um terceiro independente, um Organismo de Certificação Registado (RCB).

Esta política aplica-se a todos os sistemas, pessoas e processos que constituem os sistemas de informação do DSI da Câmara Municipal de Matosinhos, incluindo diretores, colaboradores, fornecedores e outros terceiros que tenham acesso aos sistemas da Câmara Municipal de Matosinhos, tendo sempre por base os três pilares fundamentais da ISO 27001:2022: a confidencialidade, integridade e disponibilidade da informação.

Os seguintes documentos de apoio são relevantes para esta política de segurança da informação e fornecem informações adicionais sobre como é aplicada:

04- Contexto da Organização

CMM_SGSI-04-Contexto Segurança Informação, Requisitos e Âmbito

05- Liderança

CMM_SGSI- ANEXO - Carta de Suporte do Executivo – SGSI
CMM_SGSI-05-1 Liderança e Compromisso Manual SGSI
CMM_SGSI-05-2 Política da Segurança da Informação
CMM_SGSI-05-3 Funções Responsabilidades e Autoridade da Segurança da Informação

06- Planeamento

CMM_SGSI-06-1.3 Plano de Tratamento do Risco
CMM_SGSI-06-1.3 d) SOA
CMM_SGSI-DOC-06-1 Objetivos e Plano da Segurança da Informação
CMM_SGSI-DOC-06-1.2 Processo Avaliação e Tratamento do Risco
CMM_SGSI-DOC-06-2 Objetivos Segurança Informação

USO PÚBLICO

CMM-SGSI-SOA - ISO27K1_22

07- Suporte

CMM_SGSI-07-1 e 2 Procedimento Desenvolvimento Competências Segurança da Informação_v1.0

CMM_SGSI-07-2_d) Registo Formação e Ações de Sensibilização SGSI DSI

CMM_SGSI-07-3 e 4 Programa de Comunicação de Segurança da Informação

CMM_SGSI-07-5 Procedimento de Controlo de Informações Documentadas

08- Operação

CMM_SGSI-08.1- Planeamento Operacional e Controlo

CMM_SGSI-08.2- Relatório Avaliação Riscos Baseado Ativos

CMM_SGSI-08.2-Inventario de Ativos

CMM_SGSI-08.3- Plano Tratamento Riscos

09- Avaliação de Performance

CMM-SGSI-09-2.1 Planeamento de Auditoria Interna

CMM-SGSI-09-2.2 c) Relatório de Auditoria Interna

CMM-SGSI-09-2.2 Programa de Auditoria Interna

CMM-SGSI-FORM-09-2.2 Plano de Ação do Relatório de Auditoria Interna

CMM-SGSI-FORM-09-2.2 Agendamento Plano de Auditoria Interna

CMM-SGSI-09-3 Processo de Monitorização, Medição, Análise e Avaliação

CMM-SGSI-FORM-09-3.1 a) Agenda da Reunião de Revisão pela Gestão

CMM-SGSI-09-3.1 Procedimento para Avaliações de Gestão Programadas

CMM-SGSI-FORM-09-3.2-Revisão pela Gestão

CMM-SGSI-Indicadores Revisão pela Gestão

10- Melhoria

CMM_SGSI-10-1 Procedimento Gestão da Não Conformidade

A05- Controlos Organizacionais

A05 - Templates - Controlos Organizacionais

CMM-SGSI-A05.35 Plano de Auditoria Interna

CMM-SGSI-A05.37 IT_Contatos Assistência Plataformas Software

CMM-SGSI-A05.37 IT Destruição de Discos

CMM-SGSI-A05.37 IT_Fuxograma Pedidos Acessos Internos

CMM-SGSI-A05_11 - Offboarding Processo

CMM-SGSI-A05_14 Procedimento de Transferência de Informação

CMM-SGSI-A05_37 IT_AUTORIZACAO RECOLHA DE DADOS PESSOAIS DATA CENTER

CMM-SGSI-A05_37 IT_FICHA REGISTO DE ACESSO EXTERNO AO DATA CENTER

CMM-SGSI-A05-1 Ficha Resumo de Segurança da Informação

CMM-SGSI-A05-2 Política de Software

CMM-SGSI-A05-3 Diretrizes para a Segregação de Deveres

CMM-SGSI-A05-4 e 10 Política de Uso aceitável

CMM-SGSI-A05-5 Contactos Autoridades

CMM-SGSI-A05-6 Contactos Grupos interesse

CMM-SGSI-A05-7 Política Threat Intelligence

CMM-SGSI-A05-8 Diretrizes Seg Informação Gestão Projetos

CMM-SGSI-A05-9 Inventario de Ativos

CMM-SGSI-A05-10 Política de Dispositivos Moveis e 7_9_BYOD

CMM-SGSI-A05-10 Política de Utilização Aceitável da Internet

CMM-SGSI-A05-10 Procedimento de Manuseamento e Gestão de Mídias Amovíveis

CMM-SGSI-A05-10 Procedimento de transferência de Mídia física

CMM-SGSI-A05-10 Procedimento de Manuseamento de Ativos

CMM-SGSI-A05_11 IT_Return of Assets - Offboarding Processo

USO PÚBLICO

CMM-SGSI-A05-12 Procedimento de Classificação de Informação
CMM-SGSI-A05-13 Procedimento de Etiquetagem Ativos de Informação
CMM-SGSI-A05-15 e 18 Processo de Gestão de Acesso ao Utilizador
CMM-SGSI-A05-15 Política de Controlo de Acessos
CMM-SGSI-A05-19 Acordo de Segurança de Informação de Fornecedores
CMM-SGSI-A05-19 Política Segurança Informação Relações com Fornecedores
CMM_SGSI-A05.22 Processo Avaliacao Seguranca da Informacao de Fornecedores
CMM-SGSI-A05-23 Política Computação Cloud
CMM-SGSI-A05-24 Procedimento Avaliação de Eventos
CMM-SGSI-A05-25 Procedimento de Resposta a Incidentes
CMM-SGSI-A05-30 Plano de Continuidade - APP-em-SRV
CMM-SGSI-A05-30 Plano de Continuidade - DataCenter_DR
CMM-SGSI-A05-30 Plano de Continuidade - Reposicao_SRV
CMM-SGSI-A05-30 Plano de Continuidade - Switch_CORE
CMM-SGSI-A05-30 Plano de Teste Direção Redes 2023-06-26
CMM-SGSI-A05-30 Política de Gestão de Disponibilidade
CMM-SGSI-A05-30 Relatório de Teste Direção Redes 2023-06-25
CMM-SGSI-A05-31 Procedimento de Requisitos Legais Regulamentares e Contratuais
CMM-SGSI-A05-31 Requisitos Legais, Regulamentares e Contratuais
CMM-SGSI-A05-32 Política de Conformidade IP e Copyrigth
CMM-SGSI-A05-33 Política de Retenção e Proteção de Arquivos
CMM-SGSI-A05-34 Política de Privacidade e Proteção de Dados Pessoais
CMM-SGSI-A05-37 IT_Fuxograma Pedidos Acesso VPN
CMM-SGSI-A05-37 IT_Processo Salvaguarda da Informação
CMM-SGSI-A05-37 IT_Software Sugerido pelo DSI
CMM-SGSI-A05-37 IT_Suporte Informático

A06- Controlos Recursos Humanos

CMM-SGSI-A06-3 Awareness e Formação
CMM-SGSI-A06-5_Responsabilidades após Cessação Contrato
CMM-SGSI-A06-6_ Acordos de Confidencialidade
CMM-SGSI-A06-7 Política de Teletrabalho
CMM-SGSI-A06-8 Notificação de Eventos

A07- Controlos Físicos

CMM-SGSI-A07_1_4_e_5 Segurança Física Padrões de Design
CMM-SGSI-A07_2 Política de Segurança Física
CMM-SGSI-A07_3 Procedimento de Acesso ao Datacenter
CMM-SGSI-A07_6 Procedimento de funcionamento em Áreas Segura
CMM-SGSI-A07_7 Política de Secretaria Limpa e Ecrã Limpo
CMM-SGSI-A07_9 Procedimento para Tirar Ativos Fora da CMM
CMM-SGSI-A07_13 Cronograma de Manutenção dos Equipamentos-Formulário

A08- Controlos Tecnológicos

CMM-SGSI-A08_12 Cronograma de Acordos de Confidencialidade
CMM-SGSI-A08_12 Política de Mensagens Eletrónicas
CMM-SGSI-A08_20 Política de segurança de Rede
CMM-SGSI-A08_21 Acordo Serviços de Redes_ATUAL
CMM-SGSI-A08_24 Política de Criptografia
CMM-SGSI-A08_27 Princípios Segurança para Engenharia Sistemas
CMM-SGSI-A08_33 Testes de aceitação List
CMM-SGSI-A08-6 Plano de Capacidade
CMM-SGSI-A08-7 Política Anti-Malware

USO PÚBLICO

CMM-SGSI-A08-13 Política de Backup
CMM-SGSI-A08-15 Procedimento Monitorização Utilização Sistema (Logging)
CMM-SGSI-A08-26 Política Gestão de Vulnerabilidades Técnicas
CMM-SGSI-A08-26 Procedimento Avaliação Vulnerabilidade
CMM-SGSI-FORM-Cronograma e checklist de instalação de atualizações

Os detalhes do número da versão mais recente de cada um desses documentos estão disponíveis no Registo de Documentação do SGSI na plataforma AGIR.

Política de Segurança da Informação

1.1 Requisitos de segurança da informação

Uma definição clara dos requisitos da Segurança da Informação dentro do Departamento Sistemas de Informação (DSI) da Câmara Municipal de Matosinhos será acordada e mantida com os clientes internos para que todas as atividades do SGSI sejam focadas no cumprimento destes requisitos. Requisitos estatutários, regulamentares e contratuais serão também documentados e serão inseridos no processo de planeamento. Requisitos específicos relativos à segurança de sistemas ou serviços novos ou alterados, serão registados como parte do estágio de design de cada projeto.

É um princípio fundamental do Sistema de Gestão da Segurança da Informação do DSI da Câmara Municipal de Matosinhos que os controlos implementados sejam orientados pelas necessidades das atividades e serviços e isso será regularmente comunicado a todos os colaboradores por meio de reuniões de equipa e documentos informativos.

1.2 Estrutura para definir os objetivos

Será utilizado um ciclo regular para o estabelecimento de objetivos para a Segurança da Informação, por forma a planear e garantir o financiamento necessário para as atividades de melhoria identificadas. Estes objetivos serão baseados numa compreensão clara dos requisitos da entidade, resultantes do processo de análise crítica pela Presidência, durante o qual as necessidades das partes interessadas relevantes podem ser obtidas.

Os objetivos da Segurança da Informação serão documentados por um período de tempo acordado (1 ano), juntamente com os detalhes de como serão alcançados. Os objetivos serão avaliados e monitorizados como parte das análises críticas pela direção, para garantir que permanecem válidos. Se forem necessárias alterações, as mesmas serão geridas através do processo de gestão de alterações.

De acordo com a ISO / IEC 27001:2022, os controlos de referência detalhados no Anexo A da norma, serão adotados quando apropriados para a Câmara Municipal de Matosinhos. Estes serão revistos regularmente à luz do resultado das avaliações do risco e de acordo com os planos de tratamento do risco da segurança da informação. Para obter detalhes sobre quais os controlos do Anexo A que foram implementados e quais os que foram excluídos, consulte a Declaração de Aplicabilidade.

USO PÚBLICO

Além disso, controlos melhorados e adicionais do seguinte código de prática serão adotados e implementados quando apropriado:

- ISO / IEC 27002 - Código de prática para controlos de segurança da informação;

A adoção destes códigos de prática fornecerá garantia adicional aos munícipes e ajudará ainda mais a conformidade com a legislação internacional de proteção de dados.

1.3 Melhoria Contínua do SGSI

A política da Câmara Municipal de Matosinhos em relação à melhoria contínua é:

- Melhorar continuamente a eficácia do SGSI;
- Melhorar os processos atuais para alinhá-los com as boas práticas, conforme definido na ISO / IEC 27001:2022 e normas relacionadas;
- Obter a certificação ISO / IEC 27001:2022 no Departamento de Sistemas de Informação e mantê-la continuamente;
- Aumentar o nível de proatividade (e a perceção das partes interessadas de proatividade) no que diz respeito à segurança da informação;
- Tornar os processos e controlos da Segurança da Informação mais mensuráveis, a fim de fornecer uma base sólida para decisões informadas;
- Rever as métricas relevantes anualmente para avaliar se é apropriado alterá-las, com base nos dados históricos coletados;
- Obter ideias para melhorias por meio de reuniões regulares e outras formas de comunicação com as partes interessadas;
- Rever ideias para melhoria em reuniões regulares de gestão, a fim de priorizar e avaliar prazos e benefícios.

Ideias para melhorias podem ser obtidas de qualquer fonte, incluindo colaboradores, munícipes, fornecedores, equipa de TI, avaliações de risco e relatórios de serviço. Uma vez identificadas, serão registadas e avaliadas como parte das análises críticas pela administração.

1.4 Áreas da Política da Segurança da Informação

A Câmara Municipal de Matosinhos define a política numa ampla variedade de áreas relacionadas com a Segurança da Informação, que são descritas em detalhe num conjunto de documentação que acompanha esta política abrangente de segurança da informação.

Cada uma dessas políticas é definida e acordada por uma ou mais pessoas com competência na área em questão e, uma vez formalmente aprovada, é comunicada ao público adequado, interno e externo à organização.

A tabela abaixo mostra as políticas individuais dentro do conjunto de documentação e resume o conteúdo de cada política e o público-alvo das partes interessadas.

USO PÚBLICO

Política	Áreas abordadas	Público-alvo
Política de Uso Aceitável da Internet	Uso comercial da Internet, uso pessoal da Internet, gestão de contas na Internet, segurança e monitorização e usos proibidos do serviço de Internet.	Utilizadores do serviço de Internet
Política de Computação Cloud	Procedimento, inscrição, configuração, gestão e remoção de serviços de computação em cloud.	Colaboradores envolvidos na aquisição e gestão de serviços em cloud
Política de Dispositivos Móveis	Cuidado e segurança de dispositivos móveis como laptops, tablets e smartphones, que sejam fornecidos pela organização ou pelo próprio indivíduo para uso profissional.	Utilizadores de dispositivos móveis fornecidos pela empresa e BYOD (Traga seu próprio dispositivo)
Política de Teletrabalho	Considerações de segurança da informação no estabelecimento e administração de um local de teletrabalho, por exemplo segurança física, seguro e equipamentos.	Gestão e Colaboradores envolvidos na criação e manutenção de um site de teletrabalho
Política de Controlo de Acessos	Registo e cancelamento de registo do utilizador, disponibilização de direitos de acesso, acesso externo, análises de acesso, política password, responsabilidades do utilizador e controlo de acesso a sistemas e aplicações.	Colaboradores envolvidos na configuração e gestão de controlo de acessos
Política de Criptografia	Avaliação do risco, seleção de técnica, implementação, teste e revisão de criptografia e gestão de passwords.	Colaboradores envolvidos na configuração e gestão do uso de tecnologia e técnicas criptográficas
Política de Segurança Física	Áreas seguras, segurança da informação disponível em papel e em equipamentos e gestão de ciclo de vida de equipamentos	Todos Colaboradores
Política Anti-Malware	Firewalls, antivírus, filtragem de spam, instalação de software, gestão de vulnerabilidades, formação de consciencialização do utilizador, monitorização e alertas de ameaças, análises técnicas e gestão de incidentes de malware.	Colaboradores responsáveis por proteger a infraestrutura da organização contra malware
Política de Backup	Ciclos de backup, backups em cloud, armazenamento externo, documentação, teste de recuperação e proteção de média de armazenamento	Colaboradores responsáveis por projetar e implementar regimes de backup

USO PÚBLICO

Política	Áreas abordadas	Público-alvo
Política de Software	Compra de software, registo, instalação e remoção de software, desenvolvimento interno de software e uso de software na cloud.	Todos os colaboradores
Política Gestão de vulnerabilidades Técnicas	Definição de vulnerabilidade, fontes de informação, patches e atualizações, avaliação de vulnerabilidade, fortalecimento e formação de consciencialização.	Colaboradores responsáveis por proteger a infraestrutura da organização contra malware
Política de Segurança de Rede	Projeto de segurança de rede, incluindo segregação de rede, segurança de perímetro, redes sem fio e acesso remoto; gestão de segurança de rede, incluindo funções e responsabilidades, registo, monitorização e alterações.	Colaboradores responsáveis por projetar, implementar e gerir redes
Política de Mensagens Eletrónicas	Envio e receção de mensagens eletrónicas, monitorização dos recursos de mensagens eletrónicas e utilização de e-mail.	Utilizadores de instalações de mensagens eletrónicas
Política de Segurança da Informação para Relações com Fornecedores	Acordos com fornecedores, monitorização e revisão de serviços, mudanças e término de contrato.	Colaboradores envolvidos na criação e gestão de relacionamento com fornecedores
Política de Gestão de Disponibilidade	Requisitos de disponibilidade e design; monitorização e relatórios; indisponibilidade; planos de disponibilidade de teste e gestão de alterações.	Colaboradores responsáveis por projetar sistemas e gerir a entrega de serviços
Política de Conformidade de IP e Copyright	Proteção de propriedade intelectual, a lei, penalidades e conformidade de licença de software.	Todos os Colaboradores
Política de Retenção e Proteção de Arquivos	Período de retenção para tipos de registos específicos, uso de criptografia, seleção de media, recuperação, destruição e revisão de registos.	Colaboradores responsáveis pela criação e gestão de registos
Política de Privacidade e Proteção de Dados Pessoais	Legislação de proteção de dados aplicável, definições e requisitos.	Colaboradores responsáveis por projetar e gerir sistemas que contém dados pessoais
Política de Secretária Limpa e Ecrã Limpo	Segurança das informações exibidas nos ecrãs, impressas e armazenadas em média removível	Todos os Colaboradores

Tabela 1 - Conjunto de documentos de políticas

USO PÚBLICO

1.5 Aplicação da Política de Segurança da Informação

As declarações da política feitas neste documento e no conjunto de políticas de apoio listadas na Tabela 1 foram revistas e aprovadas pela Presidência da Câmara Municipal de Matosinhos e devem ser cumpridas. O não cumprimento destas políticas por parte de um colaborador, pode resultar em ações disciplinares tomadas de acordo com o Processo Disciplinar do colaborador da organização.

Perguntas sobre qualquer política da Câmara Municipal de Matosinhos devem ser dirigidas em primeira instância ao chefe direto do colaborador.

USO PÚBLICO