POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

Tipo de documento:	**Política**		
Criado por:	Divisão de Sistemas e Tecnologias de Informação e Comunicação		
Aprovado por:	Comissão da Segurança da Informação		
Nível de confidencialidade	**Público**		
Data:	**Versão/Revisão**	**Criado/Modificado por:**	**Descrição da alteração:**
31-07-2020	0.0	Anabela Lourenço, Ricardo Jorge Simões e Ricardo Madeira Simões	Esboço básico do documento
07-08-2020	1.0	Anabela Lourenço, Ricardo Jorge Simões e Ricardo Madeira Simões	Conclusão do documento *Nota: Separação do Manual do SGSI*
26-10-2021	1.1	Anabela Lourenço, Cidália Jorge, Ricardo Jorge Simões e Ricardo Madeira Simões	Atualização do ficheiro. Erros detetados cabeçalho. Publicação na Intranet
15/11/2023	01/02	Cidália Jorge/ Ricardo Jorge Simões	Revisão do texto e novo cabeçalho e histórico de versões

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

Índice

1 Finalidade e utilizadores

O objetivo desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação.

Esta política aplica-se a todo o Sistema de gestão da segurança da informação (SGSI).
Os utilizadores deste documento são trabalhadores e colaboradores da Câmara Municipal da Amadora (CMA), assim como as partes externas relevantes.

2 Documentos de referência

- Norma ISO/IEC 27001, cláusulas 2 e 5.3
- Documento sobre o objeto do SGSI
- Metodologia de Gestão do Risco
- Declaração de aplicabilidade
- Lista de obrigações Legais, Regulamentares e Contratuais
- Política de continuidade de negócios
- Plano de resposta a incidentes

3 Terminologia básica de segurança da informação

Confidencialidade – características das informações que estão disponíveis somente para pessoas autorizadas ou sistemas.
Integridade - características das informações que são alteradas somente por pessoas autorizadas.
Disponibilidade - características das informações que somente podem ser acedidas por pessoas autorizadas, quando for necessário.
Segurança da informação - preservação da confidencialidade, integridade e disponibilidade da informação
Manual do Sistema de gestão da segurança da informação - a parte do sistema de gestão que cuida do planeamento, implementação, manutenção, revisão e melhoramento da segurança da informação.

4 Aperfeiçoando a segurança da informação

4.1 Objetivos e medição

Os objetivos gerais para a gestão de segurança da informação são os seguintes: criar uma melhor imagem no município e no país, reduzir os danos causados por possíveis incidentes, e, se eles estão em linha com os objetivos de negócios da organização, estratégia e plano de negócios. O Gestor de Processo é responsável por rever estes objetivos SGSI gerais e por definir novos objetivos. Os objetivos dos controlos de segurança ou grupos de controlos são definidos pela Comissão de Segurança da Informação (CSI), e aprovados pela Comissão de Segurança da Informação (CSI) na Declaração de aplicabilidade. Todos os objetivos devem ser revistos pelo menos uma vez por ano.

A Comissão de Segurança da Informação é responsável por definir o método para a medição da realização dos objetivos – a medição será executada pelo menos uma vez por ano e o Gestor do Processo irá analisar a avaliar os resultados da medição e reportá-los para a Gestão de Topo como material para a revisão de gestão.
Os pontos cruciais para a Gestão da Segurança da Informação são:

- Abordagem para o estabelecimento de objetivos;
- Princípios orientadores para a Segurança da informação;

- Princípios de ação relacionados com a Segurança da Informação;
- Abordagem por processos;
- Abordagem para a melhoria contínua do Sistema;
- Abordagem para a gestão da conformidade legal, regulatória e contratual.

4.2 Requisitos de segurança da informação

Esta Política e todo o SGSI deve estar em conformidade com os requisitos legais e regulamentares da organização na área de segurança da informação, bem como com as obrigações contratuais.

Uma lista detalhada de todos os requisitos contratuais e legais na Lista de obrigações regulamentares e contratuais.

4.3 Controlos da segurança da informação

Os processos para selecionar òs controlos estão definidos na Metodologia de Avaliação de Riscos e de Tratamento do Risco.

Os controlos selecionados e sua condição de implementação estão descritos na Declaração de Aplicabilidade.

4.4 Continuidade de negócios

A gestão de continuidade de negócio é descrita na Política de continuidade de negócio.

4.5 Responsabilidades

As responsabilidades básicas para o SGSI são:

- A Gestão de Topo é responsável por garantir que o SGSI seja implementado de acordo com esta Política e para garantir todos os recursos necessários;
- A Comissão de Segurança da Informação é responsável pela coordenação operacional do SGSI, bem como reportar sobre o desempenho do SGSI;
- O Responsável da Segurança da Informação (RSI) deve analisar o SGSI pelo menos uma vez por ano ou sempre que ocorrer uma mudança importante e elaborar minutas sobre a reunião. A finalidade da revisão da gestão é definir a adequabilidade e a eficácia do SGSI;
- A CSI implementará programas de sensibilização e treino sobre segurança da informação para os trabalhadores e colaboradores;
- A proteção da integridade, disponibilidade e confidencialidade é responsabilidade do proprietário de cada ativo;
- Todos os incidentes e as fragilidades de segurança devem ser reportados, ao serviço de informática, ao Gestor do Processo e, por sua vez, este informa a Gestão de Topo;
- O RSI irá definir quais as informações, relativas à segurança da informação, serão comunicadas, às partes interessadas, por quem e quando;
- A CSI é responsável por adotar e implementar um Plano de formação, que se aplique a todas as pessoas que têm uma função na gestão da segurança da informação.

4.6 Comunicação da política

A Gestão de Topo deve garantir que todos trabalhadores e colaboradores da CMA, bem como todos as partes externas interessadas conheçam esta Política.

5 Suporte para a implementação do SGSI

A Gestão de Topo declara que a implementação do SGSI e seu contínuo melhoramento serão suportadas pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como provir todos os requisitos identificados.

6 Validade e gestão de documentos

Este documento é válido a partir de 03 de setembro de 2020.

O proprietário do documento é a Comissão de Segurança da Informação, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de trabalhadores, colaboradores e terceiros que têm um papel no SGSI, mas não conhecem este documento
- não conformidade do SGSI com as leis e as regulamentações, as obrigações contratuais e outros documentos internos da organização
- ineficácia da manutenção e da implementação do SGSI
- responsabilidades confusas na implementação do SGSI

Amadora, 15 de novembro de 2023

O Vereador do Pelouro,
Ana Venâncio