Política de Segurança da Informação

Junta de Freguesia de Praia de Mira

O Regulamento Geral sobre a Proteção de Dados Pessoais da Freguesia Europeia (RGPD) - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - estabelece as regras relativas à proteção de dados pessoais de pessoas singulares, sendo aplicável diretamente na ordem jurídica de todos os Estados-Membros. O RGPD atribui uma série de direitos aos titulares de dados e também impõe uma série de deveres às organizações de direito público e privado em relação ao tratamento desses dados.

De acordo com o Artigo 32.º do RGPD, as organizações são obrigadas a implementar medidas técnicas e organizativas apropriadas para garantir um nível de segurança adequado ao risco, tendo em conta o estado da técnica, os custos de implementação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares. Isso implica a implementação, entre outras medidas, de pseudonimização e cifragem de dados pessoais, a capacidade de assegurar continuamente a confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento, a habilidade de restaurar a disponibilidade e o acesso aos dados pessoais de forma rápida em caso de incidente físico ou técnico, e um processo para testar, avaliar e revisar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento.

1. Introdução

A Junta de Freguesia de Praia de Mira, doravante designada por Freguesia, reconhece a importância da segurança da informação e da proteção dos dados pessoais dos seus cidadãos. Esta Política de Segurança da Informação estabelece diretrizes e princípios para garantir a confidencialidade, integridade e disponibilidade dos dados tratados pela Freguesia.

A segurança da informação detida pela Freguesia é crucial para os nossos fregueses, funcionários e parceiros. É responsabilidade de cada funcionário e contratado garantir que as políticas criadas para auxiliar a segurança da nossa informação sejam seguidas. Esta política de segurança da informação delineia os requisitos que devem ser seguidos para garantir que os nossos objetivos de segurança da informação sejam alcançados.

Os objetivos da Freguesia para a segurança da informação são:

1. A segurança da informação é gerida 'de cima para baixo' e uma cultura de segurança da informação está integrada em todos os aspetos do tratamento de dados.

PA

2. Os processos de Recursos Humanos e os acordos contratuais dos funcionários apoiam os objetivos de segurança da informação da organização.
3. Todos os funcionários e contratados são informados, compreendem e cumprem as suas responsabilidades individuais de segurança da informação.
4. Utilizadores autorizados terão acesso seguro aos recursos de TI para poderem desempenhar o seu papel.
5. Controlos apropriados de segurança da informação serão aplicados a todos os sistemas, tecnologias e serviços com acesso aos ativos da Freguesia.
6. Os incidentes de segurança da informação serão geridos de forma eficiente e eficaz.
7. Os controlos de segurança da informação serão monitorizados para garantir que são adequados e eficazes.
8. Os ativos de informação organizacional serão identificados e protegidos adequadamente.
9. Apenas terceiros com acordos de segurança da informação adequados serão concedidos acesso aos sistemas ou dados da Freguesia.
10. Todas as instalações de TI têm disposições de segurança ambiental e física apropriadas em vigor.

2. Âmbito

Esta política aplica-se a toda a informação e ativos de TI da Freguesia e a todos os utilizadores de dados que têm acesso a eles. Toda a informação deve ser protegida em qualquer formato, incluindo, mas não se limitando a, documentos em papel e dados eletrónicos. A informação deve ser protegida enquanto está em repouso e quando é manuseada, transmitida ou comunicada. Os ativos de TI incluem todos os dispositivos e componentes de hardware/software da infraestrutura de TI, aplicações e repositórios de dados.

3. Responsabilidade pela Segurança da Informação

A Freguesia designará um Responsável pela Segurança da Informação (RSI) para supervisionar a implementação, manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação.

Executivo – O Executivo é responsável pela segurança da informação e deve garantir o cumprimento das políticas, normas, procedimentos e práticas de segurança.

Chefes de Divisão – Todos os Chefes de Divisão, incluindo, mas não se limitando a, Chefes de Departamento e Proprietários de atividades de tratamento, concordam em promover visivelmente e

PN

oferecer o suporte necessário para as iniciativas de segurança da informação em toda a Freguesia, e ajudar a garantir o cumprimento dentro das áreas que lideram.

Utilizadores de Dados (Todos os Funcionários e Contratados) – Todos os utilizadores de dados são responsáveis por ler e cumprir esta política. Os utilizadores de dados devem concluir formação de sensibilização para a segurança da informação e são responsáveis por tomar decisões informadas para proteger a informação e os ativos de TI da Freguesia.

4. Gestão de Riscos

A Freguesia realizará avaliações regulares de risco para identificar ameaças, vulnerabilidades e impactos associados aos dados pessoais e à segurança da informação.

Serão implementadas medidas adequadas para mitigar riscos identificados, priorizando a proteção dos dados pessoais.

5. Tratamento de Dados Pessoais

A recolha, tratamento e armazenamento de dados pessoais serão realizados em conformidade com o RGPD, garantindo a licitude, transparência e finalidade específica do tratamento.

Será dado especial enfoque aos direitos dos titulares dos dados, incluindo o direito de acesso, retificação, apagamento e portabilidade.

6. Acesso e Controlo

Serão estabelecidas políticas de acesso e controlo para garantir que os colaboradores e terceiros apenas tenham acesso às informações e sistemas necessários para cumprir as suas funções.

Serão implementadas medidas técnicas e organizativas para prevenir o acesso não autorizado:

1. O acesso a todos os ativos de informação será controlado, gerido e concedido com base no princípio do privilégio mínimo e nos requisitos de tratamento de dados.
2. O acesso aos ativos de informação e sistemas será regularmente revisto e mantido em conformidade com os requisitos departamentais.

PM

7. Formação

Todos os funcionários e contratados receberão formação regular sobre as políticas de segurança da informação, os procedimentos e as práticas recomendadas para manter a confidencialidade e a integridade dos dados pessoais:

1. Todos os funcionários e contratados completarão formação obrigatória em proteção de dados e sensibilização para segurança da informação, com atividades de sensibilização entregues continuamente ao longo do ano.
2. A eficácia da formação em proteção de dados e sensibilização para segurança da informação será monitorizada e reportada ao Executivo.

8. Gestão de Incidentes

Procedimentos de gestão de incidentes de segurança da informação serão implementados para garantir que os incidentes sejam detetados e reportados de forma atempada.

1. Procedimentos de resposta a incidentes serão implementados para reduzir o impacto dos incidentes, identificar a causa raiz e comunicar os incidentes às partes interessadas relevantes.
2. Os incidentes de segurança da informação serão registados juntamente com 'lições aprendidas' para evitar recorrências.

9. Terceiros

1. As disposições de segurança da informação de todos os fornecedores e prestadores de serviços terceirizados serão avaliadas para garantir que sejam robustas e adequadas.
2. O cumprimento de terceiros em relação às políticas e normas de segurança da informação será monitorizado.

10. Cumprimento e exceções

A Freguesia deverá realizar ações apropriadas de conformidade e garantia de segurança da informação para garantir que os objetivos de segurança da informação sejam alcançados. Qualquer violação desta política estará sujeita a medidas disciplinares. Violações graves podem resultar em processos criminais ou civis. Exceções a esta política podem ser concedidas mediante aprovação do Executivo. Todos os pedidos de exceção serão registados juntamente com o resultado da sua análise.

10. Auditorias e Revisões

O cumprimento das normas de referência de segurança de TI será monitorizado, e as exceções serão geridas como riscos através do quadro de gestão de riscos.

Monitorização periódica do cumprimento das políticas, normas, procedimentos e controlos de segurança da informação da Freguesia de Freguesia será realizada para garantir que são adequados, eficazes e estão a ser seguidos.

Esta política de Segurança da Informação será revista periodicamente para garantir a sua relevância e adequação, nomeadamente, quando houver uma alteração significativa no ambiente ou nos processos de tratamento de dados, para garantir que:

1. Permaneçam operacionalmente adequados ao propósito;
2. Reflitam as mudanças em tecnologias ou processos de tratamento;
3. Estejam alinhados com as melhores práticas;
4. Apoiem a continuidade da conformidade regulamentar, contratual e legal.

11. Revisão da Política

Esta Política e Procedimento serão revistos regularmente para garantir que estão em conformidade com a legislação atualizada e as melhores práticas de proteção de dados.

Esta Política e Procedimento para a segurança da informação são adotados pela Junta de Freguesia de Praia de Mira, a partir desta data.

Praia de Mira, 26 de fevereiro de 2026

Assinatura:

Junta de Freguesia
da Praia de Mira
NIPC: 509007058
Rua da Junta de Freguesia S/N,
3070-441 PRAIA DE MIRA

(Presidente da Junta de Freguesia de Praia de Mira)

Praia de Mira
Junta de Freguesia

Registo de Versões:

Data de Aprovação	Versão	Autor	Descrição da Alteração
26/02/26	1.0	V. Cervantes	Versão inicial

www.praiademira.pt
geral@praiademira.pt
Telf.: (+351) 231 472 796

Rua das Pontes
3070-341 Praia de Mira
n.i.p.c. 509007058