REGULAMENTO GERAL DE SEGURANÇA DA INFORMAÇÃO (RGSI)

Ajuda
Junta de Freguesia

Indíce

1 INTRODUÇÃO

"A sociedade, a economia e o Estado são dependentes das tecnologias de informação e de comunicação (TIC). Temos assistido a um desenvolvimento acelerado da sociedade da informação e a uma crescente dependência das TIC em funções vitais do funcionamento do País."[1]

A informação, independentemente do seu formato ou meio de suporte, é um ativo muito importante para a **Junta de Freguesia da Ajuda** ("**JFA**"). A adequada preservação da confidencialidade, integridade e disponibilidade da informação constitui um imperativo legal, regulamentar e ético para a **Freguesia** e para todas os seus serviços e estruturas, e um pilar de confiança e sustentabilidade na relação da **JFA** com os seus Cidadãos, Colaboradores e quaisquer outras partes interessadas.

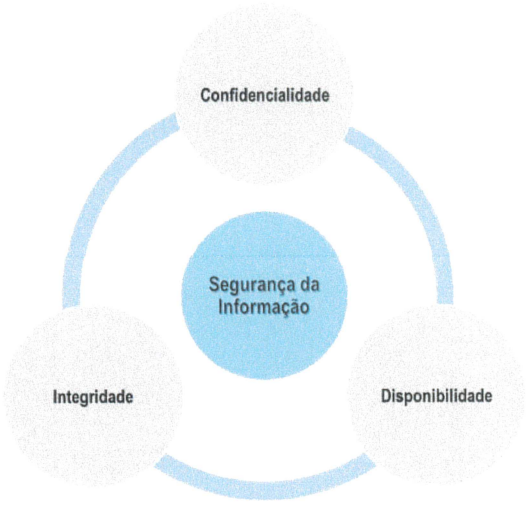

Figura 1: Confidencialidade, Integridade e Disponibilidade - os pilares da Segurança da Informação

Esta atualização do RGSI da **Junta de Freguesia da Ajuda (JFA)** incorpora:

(i) o 'Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança', e
(ii) o 'Roteiro para Capacidades Mínimas de Cibersegurança' do CNCS,
(iii) o Decreto-Lei n.º 125/2025 (transposição da Diretiva NIS2), com enfoque nas obrigações aplicáveis às entidades públicas e implicações para fornecedores e cadeia de abastecimento que prestam serviços à JFA.

2 CONCEITOS

Confidencialidade - a propriedade de a informação não estar acessível nem ser divulgada a pessoas ou entidades não autorizadas ou segundo processos não autorizados.

Integridade - a propriedade de salvaguardar que a informação não é modificada ou destruída de forma indevida ou não autorizada, bem como a salvaguarda da sua proveniência de fonte fidedigna (autenticidade).

Disponibilidade - a propriedade de a informação estar acessível e utilizável sempre que solicitada por uma entidade autorizada.

Informação - todos os dados e registos, tangíveis ou intangíveis, incluindo voz e imagem, independentemente do seu formato, modo de tratamento, meio de transmissão e tipo de suporte, físico ou lógico, relativos à vida da JFA ou às relações desta com os seus clientes e restantes partes interessadas.

[1] Resolução de Conselho de Ministro nº 36/2015

Tecnologias de Informação e Comunicação (TIC) - todas as tecnologias, *hardware* e software, utilizadas para criar, registar, recolher, processar, usar, armazenar, publicar, comunicar, transmitir, transferir, transportar, proteger, recuperar ou eliminar informação.

Segurança da Informação - preservação adequada da confidencialidade, integridade e disponibilidade da informação; envolve também a capacidade das TIC para resistir, com um adequado nível de confiança, a ações que comprometam a confidencialidade, integridade ou disponibilidade dos dados armazenados, transmitidos ou tratados ou a segurança de serviços conexos da JFA.

3 ÂMBITO, OBJETIVOS E ENQUADRAMENTO

*A estratégia de Segurança da Informação na **JFA** desenvolve-se nos seguintes objetivos estratégicos:*

a) *Promover uma utilização consciente, livre, segura e eficiente do espaço digital;*

b) *Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;*

c) *Fortalecer e garantir a segurança do ciberespaço, das infraestruturas e dos serviços da JFA;*

d) *Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.*

O presente **Regulamento** visa formalizar e comunicar a toda a organização as orientações estratégicas e programáticas aprovadas pelo Órgão Executivo da **JFA** no âmbito da Segurança da Informação, bem como o seu compromisso para satisfazer os requisitos legais aplicáveis relacionados com a Segurança da Informação.

O modelo normativo da segurança da informação da **JFA** encontra-se estruturado a partir do presente **Regulamento**, integrando um modelo de Governação e políticas sectoriais, procedimentos, manuais, instruções e outros documentos de carácter imperativo ou orientativo.

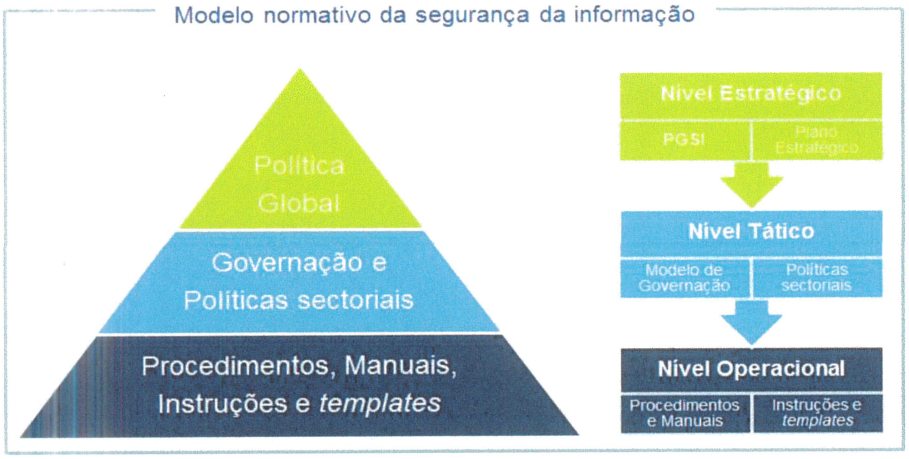

Figura 2: Modelo normativo de segurança da informação – níveis estratégico, tático e operacional

As regras e princípios que integram a presente Regulamento e os outros normativos internos de segurança da informação incorporam boas práticas consagradas na família de normas internacionais, nomeadamente a ISO/IEC 27000, considerando os requisitos internos e externos relevantes no contexto da **JFA**, aplicando-se a **todos os dados e registos, tangíveis ou intangíveis**, incluindo voz e imagem, independentemente do seu formato, modo de tratamento, meio de transmissão e tipo de suporte, físico ou lógico, **relativos à vida da JFA ou às relações desta com os seus Clientes e restantes partes interessadas**.

Para melhor enquadramento são indicados nos Anexos I e II, respetivamente, alguns dos normativos internos e documentação de referência relacionados com este Regulamento.

4 FINALIDADE E OBJETIVOS

A Segurança da Informação visa preservar a confidencialidade, integridade e disponibilidade da informação, considerando o contexto externo e interno e contribuindo para atingir os objetivos estratégicos da JFA e manter a confiança de todas as partes interessadas.

São objetivos globais da **JFA** para a Segurança da Informação:

- Garantir o alinhamento da Segurança da Informação com as competências dispostas nos Estatutos, Regulamentos próprios e na lei aplicável à **Administração Local** ;
- Garantir a identificação, avaliação, tratamento e minimização dos Riscos de Segurança da Informação, incluindo os riscos de cibersegurança relevantes para a JFA;
- Garantir a consistência do modelo normativo de Segurança da Informação e da sua implementação;
- Providenciar aos Colaboradores a formação adequada de acordo com as responsabilidades de Segurança da Informação adstritas às suas funções;
- Elevar a maturidade em Segurança da Informação, assegurar a melhoria contínua e corrigir as não conformidades;
- Demonstrar a todas as partes interessadas o compromisso e a capacidade da organização relativamente à Segurança da Informação;
- Adotar uma cultura de Segurança da Informação.

A definição, medição, reporte e revisão dos objetivos de Segurança da Informação deverá ser efetuada de acordo com indicadores, metas, periodicidades e responsabilidades específicas, definidos em **Manual do Sistema de Gestão da Segurança da Informação (MSGSI)**.

5 PRINCÍPIOS

Os princípios gerais da JFA para a Segurança da Informação são:

a) **Salvaguarda da informação**, designadamente contra a sua perda ou destruição, divulgação, difusão, alteração, armazenamento ou acesso não autorizados, independentemente do seu formato, modo de tratamento, meio de transmissão e tipo de suporte;

b) **Atuação prudente e ponderada** relativamente aos riscos de Segurança da Informação, assegurando o seu enquadramento nos processos de **Gestão do Risco** operacional e a tomada das medidas apropriadas de mitigação ou redução para níveis aceitáveis de risco;

c) **Promoção de uma cultura de segurança**, adotando progressivamente boas práticas consagradas nos referenciais standard da segurança, nomeadamente a ISO/IEC 27001/27002, e assegurando que todos os Colaboradores compreendem e exercem adequadamente as suas responsabilidades com os princípios da Segurança da Informação;

d) **Observância dos requisitos legais, regulamentares e contratuais aplicáveis** no contexto da Segurança da Informação;

e) **Melhoria contínua** de forma a garantir a sua permanente aplicabilidade, adequabilidade e eficácia, designadamente através do Sistema de Gestão da Segurança da Informação.

6 RESPONSABILIDADES

6.1 Responsabilidades Gerais de Segurança da Informação

A Segurança da Informação constitui uma prioridade da JFA, e uma responsabilidade a ser exercida de forma contínua e transversal por toda a organização.

Todos os Colaboradores têm responsabilidades na aplicação da Segurança da Informação.

Compete-lhes, designadamente, adotar uma atitude responsável e ponderada no manuseamento da informação e das TIC, proteger as suas credenciais de autenticação, conhecer e cumprir, no âmbito das suas funções, o disposto nos normativos internos de Segurança da Informação que lhes sejam aplicáveis, desde logo a presente Regulamento. Devem, ainda, observar os alertas e recomendações de segurança da informação que lhes sejam comunicadas através dos meios institucionais da JFA, ou das suas hierarquias, com vista à prevenção e contenção de incidentes.

É da responsabilidade e do âmbito de competências de todos os **Órgãos da JFA** (Executivo, Assembleia de Freguesia e outros órgãos de estrutura, incluindo Órgãos Consultivos) promover uma Cultura de Segurança que assegure a preservação da confidencialidade, integridade e disponibilidade da informação.

Os membros destes Órgãos, coordenadores e outros quadros com funções de chefia desempenham um papel decisivo na Segurança da Informação. Neste sentido, são os principais responsáveis por diligenciar e zelar pelo cumprimento da presente Regulamento e demais normativos internos de Segurança da Informação, designadamente no âmbito das suas áreas de intervenção direta e no relacionamento com outros Órgãos de estrutura, fornecedores e outros parceiros.

6.2 Governação da Segurança da Informação

A governação da segurança da informação envolve todos os intervenientes e responsáveis da JFA, desde o Órgão Executivo às unidades de serviços, áreas de suporte ao seu funcionamento e funções de controlo (i.e. Direção Administrativa, *Compliance* e/ou Auditoria interna).

São intervenientes diretos na governação da segurança da informação, designadamente, o órgão Executivo e o **Comité Geral de Segurança da Informação (CGSI),** constituído por membros designar pela JFA.

7 DIRETIVAS GLOBAIS

7.1 Diretivas Globais para a Segurança da Informação

A JFA adota as seguintes diretivas globais para a segurança da informação:

1) **Desenvolver e manter atualizado o modelo normativo da segurança da informação**, proporcionando diretrizes e apoio da gestão para a segurança da informação de acordo com os requisitos legais, estatutários, regulamentares e organizacionais relevantes neste âmbito.

2) **Definir e atribuir papéis e responsabilidades de segurança da informação de forma abrangente** a todas as áreas e projetos da organização, , de acordo com o modelo de governação instituído, observando uma adequada segregação de funções e a prevenção de conflitos de interesses.

3) **Manter contactos apropriados com as autoridades competentes** e com grupos de interesse especial e outros fóruns relevantes no âmbito da segurança da informação da JFA e da cibersegurança, em particular com o Centro Nacional de Cibersegurança (CNCS).

4) **Endereçar a segurança da informação na gestão de projeto,** independentemente do tipo de projeto, designadamente assegurando a identificação e tratamento dos riscos de segurança da informação como parte dos projetos em que a JFA participa.

5) **Instituir políticas, procedimentos e controlos de segurança** para gerir adequadamente os riscos associados à mobilidade no acesso à informação e aos serviços, incluindo em matéria de acessos remotos, dispositivos móveis e dispositivos amovíveis.

6) **Comunicar os deveres de segurança da informação a que os colaboradores estão adstritos no exercício das suas funções** e assegurar a sua adequada formação nesta matéria.

7) **Assegurar a classificação da informação em função da sua criticidade e importância**, salvaguardando e protegendo a informação de acordo com a sua classificação de segurança.

8) **Garantir a identificação e autenticação inequívocas dos utilizadores no acesso à informação e às TIC**, assegurando mecanismos e processos ajustados aos riscos de segurança e exigindo aos utilizadores a devida proteção das suas credenciais de autenticação.

9) **Prevenir acessos não autorizados à informação e às TIC**, assegurando aos utilizadores autorizados o acesso restrito de acordo com o mínimo necessário, observando uma adequada segregação de funções e a prevenção de conflitos de interesses.

10) **Aplicar adequadamente controlos criptográficos para proteger a confidencialidade e integridade da informação**, considerando a classificação de segurança da informação e a avaliação de risco.

11) Assegurar a aplicação de adequadas medidas de segurança física e ambiental contra acesso não autorizado, dano, interferência, perda, furtos e outros riscos relevantes para a segurança da informação e das TIC, dentro e fora das instalações da JFA.

12) **Assegurar a operação correta e segura das TIC**, assente em procedimentos documentados, na adequada separação entre ambientes e no controlo efetivo de quaisquer alterações que possam afetar a segurança da informação, considerando a avaliação de riscos.

13) **Implementar e operar controlos detetivos, preventivos e corretivos** para proteção contra *software* malicioso, e assegurar um programa eficaz de consciencialização e formação dos utilizadores.

14) **Garantir as redundâncias necessárias e salvaguardar a informação**, incluindo *software* e imagens dos sistemas, para proteger contra perdas de dados, observando os requisitos de continuidade de negócio e assegurando a confidencialidade e integridade da informação.

15) **Produzir, proteger e monitorizar registos de eventos relevantes** em matéria de acessos, utilização e operação da informação e das TIC, considerando os requisitos aplicáveis e a avaliação de riscos.

16) Identificar, avaliar e assegurar o tratamento atempado das vulnerabilidades técnicas nas TIC, considerando a avaliação de riscos.

17) **Assegurar a adequada segregação de redes informáticas**, protegendo a informação e os serviços disponibilizados através das mesmas bem como a devida filtragem do tráfego de rede.

18) **Proteger a informação transferida através de canais de comunicação**, incluindo para entidades externas, considerando a classificação de segurança da informação e a avaliação de riscos.

19) **Integrar a segurança da informação ao longo de todo o ciclo de vida das TIC**, desde a especificação e análise de requisitos, no desenvolvimento e nos processos de suporte, na proteção dos dados usados para testes e no tratamento adequado dos riscos de segurança.

20) **Estabelecer e contratualizar requisitos e obrigações de segurança da informação** a cumprir pelos fornecedores, considerando a importância e sensibilidade da informação e das TIC envolvidas, e atribuir papéis e autoridades para gerir a entrega dos serviços acordados e respetivas alterações.

21) **Identificar, registar e analisar incidentes e pontos fracos de segurança da informação**, assegurando os procedimentos de resposta e resolução adequados, preservando evidências e utilizando o conhecimento adquirido para reduzir a probabilidade ou o impacto de futuros incidentes.

22) Contemplar, no sistema de gestão da continuidade de negócio, os requisitos de segurança da informação e a necessária continuidade da gestão de segurança da informação em contexto de crises, desastres ou outras situações adversas.

23) Observar os requisitos legais, estatutários, regulamentares e organizacionais relevantes no contexto da segurança da informação, assegurando que os mesmos são identificados explicitamente e mantidos atualizados e que as não conformidades são corrigidas.

24) Reavaliar os riscos de segurança da informação com regularidade e quando ocorram alterações significativas.

25) Assegurar a revisão independente, incluindo auditorias, à gestão da segurança da informação e à sua implementação.

8 GESTÃO DE RISCOS DE CIBERSEGURANÇA

A JFA compromete-se a cumprir o novo Regime Jurídico da Cibersegurança, conforme Decreto-Lei n.º 125/2025 (NIS 2), adotando medidas técnicas e organizativas proporcionais ao risco, dimensão das operações e à sua tipologia setorial. Em particular:

1) Governação e responsabilidade: realizar e manter a nomeação de responsável pela cibersegurança e uma definição de cadeia de responsabilidades.

2) Gestão de riscos: manter processo contínuo de identificação de riscos, análise, avaliação e tratamento de riscos, incluindo na cadeia de fornecimento.

3) Medidas mínimas cobrem: (i) tratamento de incidentes; (ii) continuidade (backups e recuperação); (iii) segurança da cadeia de abastecimento; (iv) desenvolvimento seguro e gestão de vulnerabilidades; (v) monitorização e auditoria; (vi) políticas de criptografia e MFA; (vii) gestão de identidades e de ativos; (viii) formação e ciber-higiene.

4) Monitorização e reporte de incidentes: mecanismos de deteção, registo e notificação de incidentes ao CNCS e demais autoridades competentes, nos prazos previstos no diploma.

5) Supervisão e auditoria: preparação para auditorias e inspeções por autoridades competentes e implementação de ações corretivas.

A JFA no âmbito da gestão de riscos adota a metodologia divulgada pelo CNCS baseada nas etapas: (i) Estabelecer contexto; (ii) Levantamento (identificação, análise e avaliação); (iii) Tratamento; (iv) Comunicação e consulta; (v) Monitorização e revisão.

9 CONFORMIDADE

O disposto na presente **Regulamento** e nos outros normativos aplicáveis em matéria de Segurança da Informação tem carácter obrigatório e vinculativo a todos os Órgãos de Estrutura e Colaboradores, dentro do seu âmbito de responsabilidade.

A observância desta Regulamento não exonera os Órgãos de Estrutura e os Colaboradores do conhecimento e do cumprimento das outras normas internas e das disposições legais e regulamentares aplicáveis.

As situações de incumprimento, ainda que na forma tentada, relativamente ao presente Regulamento ou demais normativos internos e externos de carácter obrigatório, incluindo legislação ou regulamentação vigente, poderão dar origem à aplicação de sanções e/ou à comunicação às autoridades ou outras entidades competentes, em conformidade com os termos legais, contratuais e regulamentares aplicáveis.

10 AVALIAÇÃO PERIÓDICA

A presente **Regulamento** será objeto de revisão anual ou sempre que se verifiquem alterações internas e/ou externas com impactos importantes sobre a mesma.

O acompanhamento da sua aplicação na JFA será assegurado pelo **Comité Geral de Segurança da Informação** (**CGSI**), também com o suporte do **Encarregado de Proteção de Dados** (EPD).

11 DISPOSIÇÕES FINAIS

O presente **Regulamento** aplica-se a todos os Órgãos e Serviços da JFA, salvaguardando-se eventuais especificidades organizacionais, regulamentares e regimes legais.

REGULAMENTO GERAL DE SEGURANÇA DA INFORMAÇÃO (RGSI)	Data: 01/01/2026
Elaborado por: Ricardo Marques (EPD)	
Aprovado por: Executivo da Freguesia da Ajuda	
Nome: Jorge Manuel Jacinto Marques Aprovado por unanimidade em 19/03/2026	
Assinatura:	

1 ANEXO I

1.1 NORMATIVOS INTERNOS

A elaborar pelo **Comité Geral de Segurança da Informação (CGSI)**.

Ordem de Serviço (OS)

- Modelo de Governação da Segurança da Informação
- Comités Gerais

2 ANEXO II

2.1 DOCUMENTAÇÃO DE REFERÊNCIA

International Organization for Standardization:

- Information Security Management Systems - Overview and vocabulary - ISO/IEC 27000
- Sistemas de Gestão de Segurança da Informação - Requisitos - NP ISO/IEC 27001
- Code of Practice for Information Security Controls - ISO/IEC 27002
- Information Security Management Guidelines for Financial Services – ISO/IEC TR 27015
- Guidelines for Cybersecurity - ISO/IEC 27032

Legislação nacional e europeia:

- Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, aprovou a primeira **Estratégia Nacional de Segurança do Ciberespaço.**
- Lei n.º 46/2018 de 13 de agosto que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC)
- Decreto-Lei n.º 65/2021 de 30 de julho que regulamenta o **Regime Jurídico da Segurança do Ciberespaço**
- REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016
- **Lei n.º 58/2019** de 8 de agosto que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016
- **Lei n.º 59/2019** de 8 de agosto que 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
- Lei n.º 109/2009 de 15 de setembro que aprova a **Lei do Cibercrime**, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro
- Diretiva sobre Ataques contra os Sistemas de Informação (Diretiva 2013/40/UE)
- Diretiva sobre Segurança das Redes e da Informação (Diretiva 2016/1148/UE)