Política de Segurança da Informação (PSI)

Junta de Freguesia da Ajuda

Refª SGSI.02.PSI

Aviso: A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA. Versões impressas deste documento podem não estar atualizadas e este documento assume o estado de "Cópia não controlada".		
Data: 20/03/2024		Elaborado por: Ricardo Marques
Versão: 1		Aprovado por: Executivo da JFA
Classificação: Pública		Distribuição autorizada: Trabalhadores, Parceiros e prestadores de serviços, Clientes

Histórico de alterações

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

Data	Versão	Criado por	Descrição das alterações
20.03.2024	1.0	Ricardo Marques	Documento inicial – sujeito a validação

Conteúdo

1. **INTRODUÇÃO** 3
2. **OBJETIVO E CAMPO DE APLICAÇÃO** 3
   - 2.1. FINALIDADE, ABRANGÊNCIA E UTILIZADORES 3
   - 2.2. REFERÊNCIAS NORMATIVAS 3
3. **TERMOS E DEFINIÇÕES** 4
4. **CONTEXTO DA ORGANIZAÇÃO** 4
   - 4.1. ÂMBITO E APLICABILIDADE DA PSI 4
5. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** 5
   - 5.1. A SEGURANÇA DA INFORMAÇÃO 5
   - 5.2. DOMÍNIOS DA PSI 5
   - 5.3. RESPONSABILIDADES DO UTILIZADOR DE ATIVOS DE INFORMAÇÃO DA JFA 7
     - *5.3.1. Responsabilidade pelos ativos* 7
     - *5.3.2. Utilização e Atividades proibidas* 7
     - *5.3.3. Saída de equipamentos* 7
     - *5.3.4. Procedimentos de Backups* 10
     - *5.3.5. Proteção de Antivírus* 7
     - *5.3.6. Autorização de Acesso aos Sistemas de Informação* 7
     - *5.3.7. Responsabilidade relativa às Contas de Utilizador* 8
     - *5.3.8. Definição de senhas de utilizador* 8
     - *5.3.9. Utilização de Internet* 8
     - *5.3.10. E-mail e outros métodos de envio de informação / mensagens* 9
     - *5.3.11. Conversas em Locais Públicos e registo de informações* 9
     - *5.3.12. Copyright* 10
     - *5.3.13. Leis e Regulamentos* 10
6. **VALIDAÇÃO E APROVAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** 11

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

1 Introdução

A **Freguesia da Ajuda** (doravante **"JFA"**), freguesia do Município de Lisboa, preocupa-se em proteger os dados pessoais fornecidos pelos seus cidadãos e utentes, no âmbito da prestação de serviços e na utilização das plataformas de informação e comunicação que sejam sua propriedade ou estejam sob a sua gestão. A recolha e tratamento dos dados pessoais dos seus cidadãos e utentes é essencial para garantir a prestação de um serviço público de qualidade.

A atividade heterogénea da JFA necessita e requer uma transparência de processos, a disponibilidade de comunicação e partilha de sistemas de informação por todas as áreas de serviços e parceiros, mas também o processamento e tratamento de diversos tipos de informação, incluindo dados e informação pessoal, de diversas categorias de titulares de dados pessoais.

Esta versão da Política de Segurança da Informação (PSI) da JFA atualiza a versão v1.0, integrando o Roteiro para Capacidades Mínimas de Cibersegurança para PME do CNCS, o **Guia de Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança** do CNCS, e o novo **Regime Jurídico da Cibersegurança** aprovado pelo Decreto-Lei n.º 125/2025.

2 Objetivo e campo de aplicação

A informação é considerada um ativo estratégico para a **Freguesia da Ajuda**, fundamental para o desenvolvimento sustentável das competências atribuídas e normal atividade da Freguesia, razão pela qual é vital a definição e aplicação desta Política de Segurança da Informação (**PSI**), de forma a salvaguardar a **Confidencialidade**, a **Integridade** e a **Disponibilidade** da informação tratada.

Tendo por base este entendimento a **JFA** procura tratar de forma integrada a segurança da informação física e lógica, bem como sensibilizar todos aqueles com quem se relaciona de modo a assegurar a proteção da informação nos processos críticos de negócio e garantir a qualidade do serviço prestado.

2.1 Finalidade, abrangência e utilizadores

A finalidade deste documento é definir de forma clara as regras de uso dos sistemas de informação e dos Ativos de Informação da JFA.

A **Segurança da Informação** exige um esforço contínuo para a proteção dos ativos de informação, e visa atingir os seguintes objetivos:

a) **Confidencialidade**: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
b) **Integridade**: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositadas;
c) **Disponibilidade**: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

Os utilizadores deste documento são todos os utilizadores de serviços, parceiros, prestadores de serviços, fornecedores, trabalhadores e outras partes interessadas.

A divulgação deste documento entre os utilizadores evidencia que os objetivos da gestão da segurança da informação estão estruturados, estabelecidos e implementados.

2.2 Referências normativas

Os seguintes documentos são referenciados na conceção das normas neste documento e indispensáveis para a interpretação da sua aplicação:

- NP EN ISO/IEC 27000 - Information technology – Information security management systems
- NP EN ISO/IEC 27001 - ISO 27001 Information security management systems - Requirements
- NP EN ISO/IEC 27002 - Code of practice for information security controls
- REGULAMENTO GERAL DE SEGURANÇA DA INFORMAÇÃO (RGSI)
- Regulamento (UE) 2016/679 (RGPD) e a Política de Privacidade e Proteção de Dados da JFA~
- Decreto-Lei n.º 125/2025 - novo Regime Jurídico da Cibersegurança (transposição da Diretiva (UE) 2022/2555 – NIS 2)

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

3 Termos e definições

a) **"Ativos de Informação"** – no contexto desta Política, o termo Ativo de Informação é referente aos sistemas de informação e outros dados/equipamentos incluindo documentos em papel, telemóveis, computadores portáteis, discos portáteis, etc.
b) **"Equipamento informático"** - processador informático, nomeadamente desktop, desktop virtual, portátil, monitor, teclado, rato, unidades de armazenamento, e todos os serviços e recursos informáticos disponibilizados, designadamente impressoras, correio eletrónico (interno ou externo), internet e intranet.
c) **Confidencialidade dos dados** - classificação da informação que pretende garantir o acesso unicamente às pessoas autorizadas. A classificação pode ser Pública, Restrita ou Confidencial.
d) **Incidente significativo:** evento com impacto grave na disponibilidade, integridade, autenticidade ou confidencialidade de dados/serviços.
e) **Integridade** - é a manutenção e a garantia da exatidão e consistência dos dados durante todo o ciclo de vida da informação (desde que são recolhidos, tratados e destruídos), assegurando que não são alterados de forma ilícita ou acidental
f) **Disponibilidade da informação –** obrigação e objetivo da organização de manter os serviços disponibilizados aos utilizadores o máximo de tempo possível. associada com a capacidade de restabelecer a disponibilidade e o acesso aos dados de forma atempada no caso de um incidente físico ou técnico.
g) **"Segurança da Informação"** - processo organizado e estruturado que permite preservar a confidencialidade, integridade e disponibilidade da informação.
h) **"Sistemas de Informação"** - inclui todos os servidores e postos, infraestrutura de rede, software de sistemas e aplicações, dados e outros equipamentos e componentes informáticos detidos e/ou usados pela organização ou sobre a sua responsabilidade. O uso de um Sistema de Informação também inclui todos os serviços internos e externos, como acesso à internet, e-mail, etc.
i) "**Uso Aceitável**" - os **Ativos de Informação** devem ser usados apenas no âmbito dos serviços prestados com o objetivo de executar tarefas relacionadas com a missão da organização.
j) **DTI -** Direção de Tecnologias de Informação, departamento ou a equipa de TI, responsável pelas seguintes funções na organização:
    a. Planear e coordenar as atividades relacionadas com a estratégia e os sistemas e tecnologias e informação recolhidos e processados pela Organização, com o objetivo de garantir a sua qualidade e a sua otimização, e
    b. Apoiar a definição das políticas, procedimentos e objetivos relacionados com os sistemas e tecnologias de informação.

4 Contexto da Organização

A **Freguesia da Ajuda** identifica as questões internas e externas relevantes para o tratamento da informação no âmbito do fornecimento e prestação de produtos e serviços (finalidades) e que afetam a capacidade para alcançar o(s) resultado(s) pretendido(s) do Sistema de Gestão da Segurança da Informação.

4.1 Âmbito e aplicabilidade da PSI

Os princípios e regras da PSI são aplicáveis a todas as unidades e áreas e ativos / processos da JFA.

Por definição, estes princípios e regras de segurança da informação, integrados num programa crítico e fundamental para a JFA, abrangem *bases de dados, qualquer ambiente informático, ferramentas tecnológicas e/ou aplicacionais* que envolvam a estrutura da organização, documentos e arquivos em qualquer formato ou suporte.

A PSI aplica-se a todos os processos de negócio, operacionais, de suporte e de gestão, bem como aos sistemas de informação e recursos utilizados para suportar tais processos e dos quais a JFA é responsável incluindo, as atividades executadas externamente ou por terceiros por conta da organização.

Estes princípios e regras são destinados e de cumprimento obrigatório para todos os **trabalhadores, parceiros e prestadores de serviço**.

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

5 Política de Segurança da Informação

5.1 A Segurança da Informação

Entende-se por **Informação** qualquer fluxo de comunicação ou representação de conhecimento como dados, factos ou opiniões, em qualquer meio ou formato (e.g. textual, numérico, gráfico, cartográfico, narrativo, audiovisual ou conjunção destes).

A PSI da JFA deve assegurar um conjunto de princípios de segurança:



A segurança da informação deve estar também em **conformidade,** com as políticas internas da **JFA**, com a lei e demais disposições normativas documentados nos contratos e acordos operacionais com clientes, parceiros e/ou outras partes interessadas.

5.2 Domínios da PSI

A **JFA** adota os standards e as boas práticas relativas à segurança da informação como referenciais para o desenvolvimento da sua Política de Segurança da Informação (PSI), abrangendo esta as áreas cobertas pelas normas da ISO 27000, pelo Regulamento Geral de Proteção de Dados Pessoais ("RGPD") e pelo disposto na Resolução do Conselho de Ministros n.º 41/2018.

Os principais domínios de segurança da informação que constituem a framework adotada pela **JFA** são os seguintes:

1) **Organização de segurança da Informação:**
   i. Estabelecer um **modelo de referência** de gestão para iniciar e controlar a operação de segurança da informação da JFA;
   ii. Assegurar a segurança no teletrabalho e na utilização de dispositivos móveis;
   iii. Definir a **política de uso aceitável** que deve conter regras para a utilização dos recursos da JFA, ficando o uso destes condicionado ao conhecimento e à concordância por parte de cada utilizador;
   iv. Definir os procedimentos para a gestão dos suportes de tratamento, armazenamento e salvaguarda da informação;
   v. Assegurar a proteção da informação e ativos da JFA nas relações com fornecedores.
2) **Segurança na gestão de Recursos Humanos:**
   i. Assegurar que todos os trabalhadores e prestadores de serviços conhecem, entendem e cumprem as suas responsabilidades na área da segurança da informação em conformidade com as funções para as quais estão a ser considerados;
   ii. Assegurar que os interesses e responsabilidades da JFA e dos utilizadores são cumpridos ao longo do processo de admissão, mudança ou cessação de funções;

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

3) **Gestão de ativos de informação:**
   i. Assegurar a identificação dos ativos de informação da JFA e definir as responsabilidades pela proteção apropriadas;
   ii. Definir a **política de classificação de segurança**, assegurando que a informação receba um nível adequado de proteção de acordo com o seu valor e criticidade;
4) **Controlo de Acessos:**
   i. Limitar o acesso à informação e aos recursos de processamento de informação;
   ii. Assegurar o acesso de utilizadores autorizados e prevenir o acesso não autorizado a sistemas, serviços e instalações da JFA;
   iii. Definir os processos de atribuição de acessos, físico e lógicos, em conformidade com as boas práticas e os requisitos legais aplicáveis, e.g. Resolução de Conselho de Ministros 41/2018;
5) **Segurança Física e Ambiental:**
   i. Proteger as informações, equipamentos e instalações da JFA de acesso físico não autorizado,
   ii. Prevenir a perda, dano, furto ou comprometimento de ativos e interrupção das operações da JFA, na definição de serviços de suporte, manutenção e remoção de ativos;
6) **Segurança de operações:**
   i. Assegurar a operação segura e correta dos recursos de processamento da informação, e.g. documentar e divulgar os procedimentos de operação aos utilizadores apropriados;
   ii. Assegurar a separação de ambientes de produção, desenvolvimento e teste;
   iii. Assegurar que a informação e os recursos de processamento estão protegidos contra código malicioso;
   iv. Definir a **política de Backups** que assegure a proteção contra a perda de dados, através de cópias e testes regulares da salvaguarda da informação;
   v. Criar mecanismos que permitam controlar e auditar a conformidade das operações com as políticas de segurança da informação;
   vi. Analisar e prevenir a exploração de vulnerabilidades técnicas;
   vii. Definir a **política de criptografia** que assegure a utilização adequada de criptografia para proteger a informação.
7) **Segurança de comunicações:**
   i. Assegurar a proteção da informação nas redes e nos seus recursos de tratamento de informação;
   ii. Garantir a segurança da informação transmitida dentro da organização e com quaisquer entidades externas.
8) **Aquisição, desenvolvimento e manutenção de sistemas;**
   i. Assegurar a integração da segurança da informação nos sistemas de informação ao longo do seu ciclo de vida, desde a conceção, melhorias, atualizações ao suporte contínuo.
9) **Incidentes de segurança da informação:**
   i. Assegurar a definição de responsabilidades e os procedimentos para a gestão eficaz de incidentes de segurança da informação,
   ii. Definir processo de comunicação e registo de eventos, avaliação e resposta a incidentes, reporte de riscos e revisão periódica dos processos de melhoria contínua.
10) **Continuidade de segurança da informação:**
   i. Planear, implementar e avaliar a continuidade da segurança da informação no plano da continuidade do negócio da organização em situações de desastre;
   ii. Planear e implementar os recursos e ativos de informação com a redundância adequada para cumprir com os requisitos de disponibilidade.
11) **Conformidade:**
   i. Assegurar o cumprimento das obrigações legais, estatutárias, regulamentares e contratuais, bem como de quaisquer requisitos de segurança da informação;
   ii. Planear as revisões e avaliação de segurança da informação (objetivos, políticas, processo e procedimentos) de forma independente e em intervalos planeados.
12) **Proteção de Dados Pessoais:**

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

i. Identificar e localizar a informação que contem dados pessoais, o seu propósito, risco potencial e valor;
ii. Garantir que os procedimentos a estabelecer sejam adequados às obrigações de proteção de dados pessoais decorrentes, nomeadamente, do Regulamento (UE) 2016/679 e outra legislação nacional aplicável.

5.3 Responsabilidades do utilizador de ativos de informação da JFA

5.3.1 Responsabilidade pelos ativos

O trabalhador é responsável pela confidencialidade, integridade e disponibilidade da informação nos ativos que lhes são atribuídos pela **JFA** para a execução das suas funções.

Cada Ativo de Informação deve ter um trabalhador atribuído no inventário de Equipamentos dos SI, seja um utilizador (atribuição do ativo de forma exclusiva) ou um Coordenador / Responsável de serviço (atribuição de um ativo a uma unidade de serviços com grupo de utilizadores).

5.3.2 Utilização e Atividades proibidas

Os Sistemas e equipamentos de informação da JFA apenas devem ser utilizados para as finalidades profissionais para as quais foram atribuídos. Desta forma, é proibido o uso destes ativos de informação de formas desnecessárias que reduzam a capacidade, diminuam o desempenho do sistema ou coloquem riscos de segurança.

Incluem-se nesta proibição as seguintes atividades:

- Descarregar imagens ou vídeos que não tenham um propósito de negócio, enviar cadeia de e-mails, jogar jogos, etc. ,
- Instalar software no computador local sem autorização explicita da DTI
- O uso de aplicações Java, controles Active X e outros códigos móveis, exceto quando autorizado formalmente pela DTI
- O uso de ferramentas de encriptação num computador, exceto em casos autorizados ou determinados no Procedimento de Classificação da Informação.
- Descarregar programas ou ficheiros de origem não-autorizada através de dispositivos externos (ex. USP-Pen)
- Instalar ou usar periféricos como modems, cartões de memória e outros dispositivos de leitura e escrita (ex. USB-Pens) sem autorização da DTI

5.3.3 Saída de equipamentos

Equipamentos, dados ou software, independentemente da sua forma ou dispositivo, não podem ser levados para fora das instalações da JFA, salvo no âmbito dos procedimentos já definidos ou com consentimento escrito da DTI. No período em que os ativos estejam fora da organização é responsabilidade da pessoa autorizada assegurar o controlo e a segurança do ativo (Equipamento, software e dados)

No término da utilização de um Ativo ou no término do contrato do trabalhador ou prestador de serviços, o utilizador autorizado é responsável por devolver os ativos de informação à respetiva Chefia / Direção.

5.3.4 Proteção de Antivírus

A equipa de TI deve assegurar a instalação e funcionamento do software nos computadores e com as atualizações automáticas ativas. O utilizador é responsável por assegurar o normal funcionamento do software instalado no equipamento que lhe foi atribuído. Em caso de anomalia no seu funcionamento o software notifica ao utilizador, que deve reportar de imediato à equipa de TI através do endereço de email informatica@jf-ajuda.pt.

5.3.5 Copyright

Os Trabalhadores da **JFA** não podem realizar e instalar cópias não autorizadas de software de terceiros ou open-source em ativos de informação da organização, exceto em casos permitidos ou autorizados pela DTI.

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

- Os utilizadores que realizem ou instalem cópias de software ou outros conteúdos originais de outras fontes podem incorrer em responsabilidade civil, criminal e disciplinar.

5.4 Gestão de Identidades, Autenticação e Palavras-passe

A JFA assegura a gestão integral do Ciclo de vida de utilizadores, para garantir que cada utilizador tem acesso apenas aos dados necessários para executar as suas funções, bem como, a atualização, a revisão periódica de privilégios e a revogação imediata (por mudança ou termino da função).

5.4.1 Autorização de Acesso aos Sistemas de Informação

Os trabalhadores da JFA só devem aceder aos Ativos de Informação (físicos e digitais) para os quais têm autorização explicita no âmbito das suas funções profissionais.

- Os utilizadores só devem ter acesso aos Sistemas de Informação para as finalidades para que estão autorizados e para as quais receberam os respetivos direitos de acesso.
- Os utilizadores não devem participar em atividades que possam ser usadas para contornar os sistemas de segurança da informação e os controlos de acesso implementados.

5.4.2 Definição de senhas de utilizador

Os utilizadores são responsáveis por aplicar as boas práticas de segurança quando recebem, criam e utilizam as suas senhas de acesso "passwords". Aplicam-se as seguintes regras:

- As senhas não devem ser divulgadas a outras pessoas, incluindo superiores hierárquicos e administradores de sistemas;
- As senhas não devem ser escritas e mantidas em meios de fácil acesso, salvo por procedimentos aprovados pela DTI – sugere-se que o utilizador use a software KeyPass ou similar para o efeito.
- As senhas geradas pelos utilizadores não devem ser comunicadas a terceiros por qualquer meio (seja verbal, escrito ou eletrónico);
- As senhas devem ser alteradas em caso de haver indícios de que as senhas ou os sistemas estejam comprometidos – neste caso, deverá ser reportado de imediato um incidente de segurança;
- As senhas fortes são constituídas da seguinte forma:
    - Ter um mínimo de nove caracteres;
    - Terem três dos quatro seguintes conjuntos de caracteres:
        - Ter um mínimo de carater numérico;
        - Ter um mínimo de uma letra maiúscula;
        - Ter um mínimo de uma letra minúscula;
        - Ter um mínimo carater especial;
    - A senha não deve ser baseada em dados pessoais (exemplo: data de nascimento, morada, nome de familiares, etc.) Não podem utilizar as últimas 3 senhas
- As senhas devem ser alteradas no mínimo a cada 3 meses (perfil *Key-user / Gestor*) e 6 meses (perfil *Utilizador regular*);
- As senhas devem ser alteradas na primeira utilização;
- As senhas não devem ser gravadas em sistemas de autenticação automática (exemplo: macro ou browser)
- As senhas usadas para fins pessoais não devem ser as mesmas usadas para fins profissionais.

5.4.3 Responsabilidade relativa às Contas de Utilizador

O utilizador não deve direta ou indiretamente permitir que outra pessoa use as suas credenciais / passwords de acesso e não deve usar o utilizador e/ou senha de outra pessoa.

- O uso de contas de utilizadores de grupo é restrito sob autorização da **DTI e/ou Executivo**.
- O detentor da conta de utilizador é o próprio utilizador, que será o único responsável pela sua utilização por todas as operações efetuadas com a sua conta de utilizador.

5.5 Envio de Informação, Correio Eletrónico e Classificação

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

A **JFA** determina o método de comunicação adequado que pode ser usado por cada tipo de informação, e possíveis restrições à utilização de canais de comunicação para envio da mesma de acordo com procedimentos aprovados.

5.5.1 Utilização de Internet

A internet deve ser apenas acedida pela rede local da **JFA** com a proteção da infraestrutura de rede e firewall. As ligações diretas à internet através de modems, internet móvel, redes wireless ou outros equipamentos de ligação são proibidas.

- A equipa de TI pode bloquear o acesso a páginas de internet a determinados indivíduos, grupos ou todos os trabalhadores da organização. No caso de algumas páginas estarem bloqueadas, o utilizador pode submeter um pedido à DTI para autorização a essas páginas. O utilizador não deve tentar contornar a restrição ao acesso de forma autónoma.

O utilizador deve considerar a informação recebida por sites não seguros como não confiável. Tal informação só deve usada no âmbito da organização, após a verificação da sua autenticidade e exatidão.

O trabalhador pode incorrer em responsabilidade civil, criminal e disciplinar em caso de uso não autorizado ou impróprio do serviço ou conteúdos da internet.

5.5.2 E-mail e outros métodos de envio de informação / mensagens

A equipa de TI determina o método de comunicação adequado que pode usado por cada tipo de informação e possíveis restrições à utilização de canais de comunicação para envio de informação de acordo com os Procedimentos de Segurança para o Departamento TI.

- Os Trabalhadores apenas devem enviar mensagens com informação profissional por canais autorizados e para destinatários fidedignos.
- É proibido enviar conteúdos perturbadores, desagradáveis, sexualmente explícitos, difamatórios ou com qualquer outro conteúdo inaceitável ou ilegal. Os trabalhadores não devem enviar mensagens de spam.
- Os trabalhadores devem reportar a receção de qualquer email de spam para o email de suporte de TI, informatica@jf-ajuda.pt.
- Os trabalhadores devem gravar as mensagens com informação relevante para a organização de acordo com o(s) método(s) definido(s) pela equipa de TI.
- Todos os emails devem incluir um "**Aviso de Privacidade e Confidencialidade**", exceto as mensagens enviadas por sistemas automáticos definidos pela DTI.
- No caso de um utilizador colocar uma mensagem em sistemas de trocas de mensagens (fóruns, redes sociais, etc.) deve de forma inequívoca afirmar que a sua opinião não deve representa o ponto de vista da organização.

Nota: para além do correio eletrónico (emails) são considerados métodos de transferência de mensagens: os ficheiros descarregados pela internet, transferência de dados através de WeTransfer ou serviços similares, telefones, fax, mensagens de texto de SMS, pens USB, discos externos ou redes sociais, como o Facebook e Twitter.

5.5.3 Conversas em Locais Públicos e registo de informações

Não discutir ou comentar assuntos privados ou confidenciais em locais públicos ou por meio de mensagens de texto.

5.6 Rede de comunicação

A **JFA** deve adotar procedimentos de análise para a monitorização dos fluxos de tráfego na rede, incluindo adotar alarmística que permita identificar situações de acesso, tentativas ou utilização indevida de redes e sistemas.

5.7 Dispositivos, Trabalho Remoto e Acesso Externo

O armazenamento de dados deve ser realizado preferencialmente em sistemas internos, e os Acessos remotos apenas devem ser realizados por VPN segura.

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

- Cifragem de disco em portáteis e dispositivos móveis;
- Ativar o bloqueio após tentativas falhadas; ativar funcionalidades de remote-wipe e localização quando aplicável.

A DTI é responsável pela gestão e atualizações de sistema/firmware e hardening; ativação e conservação de logs, quando tecnicamente aplicável.

5.8 Cópias de Segurança e Continuidade

A **JFA** deve definir uma política de Backups que assegure a disponibilidade de Backups atualizados, testados e protegidos (incluindo cópias imutáveis/offline quando adequado), segregados das bases de dados principais, com testes de recuperação regulares.

5.8.1 Procedimentos de Backups

Os utilizadores de computadores e portáteis devem monitorizar o correto funcionamento do software que efetua o backup de toda a informação de carater sensível do seu computador, pelo menos uma vez por semana. Em caso de anomalia na realização do backup, o software notifica o utilizador, que deve reportar de imediato à DTI através do endereço de email informatica@jf-ajuda.pt.

5.9 Documentos em Papel e Transporte de Informação

A **JFA** assegura uma política de gestão de documentos em papel, assegurando a conservação em Arquivos em local controlado, fechado e resistente.

A destruição de documentos com informação sensível deve ser segura e realizada por equipamento adequado.

No Transporte de informação e dados deve assegurar a mitigação dos riscos de leitura/cópia/alteração/eliminação por pessoas não autorizadas.

6 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:

- **Governação e responsabilidade**: realizar e manter a nomeação de responsável pela cibersegurança e uma definição de cadeia de responsabilidades.
- **Gestão de riscos**: manter processo contínuo de identificação de riscos (ver ANEXO I), análise, avaliação e tratamento de riscos, incluindo na cadeia de fornecimento.
- **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.
- **Monitorização e reporte de incidentes**: mecanismos de deteção, registo e notificação de incidentes ao CNCS e demais autoridades competentes, nos prazos previstos no diploma.
- **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.

7 Gestão de Incidentes e Notificações

A **JFA** define e assegura o exercício regular do Plano de resposta a incidentes e recuperação do desastre, prevendo os mecanismos adequados para garantir a segurança da informação e a resiliência dos sistemas e serviços, bem como assegura que a disponibilidade dos dados é restabelecida atempadamente após um incidente.

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

Deveres de comunicação com a Autoridade de supervisão e Terceiros:

- CNCS (para incidentes significativos): notificação inicial até 24h após verificação e atualização até 72h; fim de impacto em 24h e relatório final em 30 dias.
- CNPD (violação de dados pessoais): notificação de incidente até 72h e, quando aplicável, comunicação a titulares com elevado risco, logo que possível.
- Comunicação a Clientes e destinatários de serviços quando incidentes possam afetá-los negativamente.

A **JFA** deverá assegurar a preservação de evidências conforme as boas práticas e os requisitos legais em vigor.

8 Proteção de Dados desde a conceção e por defeito

A **JFA**, os seus colaboradores e parceiros deverão aplicar as medidas técnicas e organizativas, nas fases iniciais da conceção das operações de tratamento, de forma a garantir os princípios da privacidade e proteção de dados logo desde o início:

- **Proteção de dados desde a conceção**: a DSI, sob orientação da área responsável, deverá assegurar a avaliação do risco do tratamento para os titulares em todo o processo de conceção de um serviço, produto ou sistema. Tal significa avaliar e implementar as medidas técnicas e organizacionais adequados (ex pseudonimização e cifragem) desde o início para garantir que o tratamento está em conformidade com a legislação e protege os direitos dos titulares dos dados em causa.

A **JFA**, os seus colaboradores e parceiros deverão garantir que os dados pessoais sejam tratados com a mais elevada proteção da privacidade (por exemplo, apenas os dados necessários devem ser tratados, período de conservação limitado, acessibilidade limitada) para que, por defeito, os dados pessoais sejam disponibilizados ao número estritamente necessário de pessoas:

- **Proteção de dados por defeito**: a **JFA**, sob orientação da área responsável, deverá assegurar os mecanismos para garantir que, por defeito, apenas os dados pessoais que são necessários para cada finalidade específica do tratamento deverão ser recolhidos, tratados e acessíveis ao um número estritamente necessário de pessoas. Esta obrigação aplica-se à extensão dos dados recolhidos, ao seu tratamento, ao prazo de conservação e à sua acessibilidade.

9 Monitorização, Formação e Conformidade

A **JFA** promove uma cultura da proteção da privacidade, segurança da informação e cibersegurança, para que cada colaborador esteja capacitado para reconhecer potenciais ameaças e agir em conformidade, incluindo um plano de formação periódica e a monitorização da eficácia das medidas e a mitigação de riscos identificados nas não conformidades.

A **JFA** compromete-se a adaptar o seu modelo de serviço público e os respetivos meios técnicos e organizativos para assegurar a conformidade e efetivo cumprimento da lei, da proteção da privacidade, segurança da informação e da esfera de interesses, direitos e liberdades dos seus Cidadãos.

10 Legislação e Regulamentos

É responsabilidade do trabalhador conhecer a legislação e cumprir as imposições legais, as normas, regulamentos e procedimentos vigentes da JFA.

11 Validação e Aprovação da Política de Segurança da Informação

Este documento deve ser revisto, e caso necessário, atualizado com a periodicidade mínima de um ano.

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

Esta Política foi aprovada pela Freguesia da Ajuda em reunião de Executivo no dia 19 de março de 2026.

A presente versão da Política entra em vigor em após a data da sua aprovação e divulgação aos Colaboradores.

Ajuda, 19 de março de 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:	

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

12 Anexo I — Tabela de Tipos de Ameaças (CNCS)

A Tabela a seguir contém exemplos de ameaças comuns. A lista pode ser usada durante o processo de avaliação dos riscos.

A lista também indica, para cada tipo de ameaça, se ela pode ser considerada A (acidental), I (intencional), ou N (natural).

Tipo de Ameaça	Exemplos	Origem
Falha de sistema	Falha de equipamento/sistema; Saturação do sistema de informação; Violação das condições de uso do sistema de informação que possibilitam a sua manutenção; Defeitos/bugs no sistema; Abuso de permissões	A A/ I A/ I A/ I A/ I A/ I
Fenómeno natural	Fenómeno climático, Fenómeno sísmico, vulcânico ou meteorológico; Inundação; Fenómeno pandémico/epidemia	N
Erro humano	Divulgação indevida de informação; introdução de dados de fontes não confiáveis; Utilização indevida de equipamentos; Erro de utilização; Acesso não autorizado a sistemas; Uso de Software ilegal ou falsificado; Adulteração de software; Violação de leis e regulamentos	A / I
Ataque malicioso	Terrorismo/sabotagem; Engenharia social; Interceção de informações; Ciberespionagem; Furtos de equipamentos, dispositivos ou documentos Furto de credenciais; Introdução de dados de fontes não confiáveis; Adulteração de hardware/software/dados; Exploração via comunicações web; Tratamento não autorizado de dados pessoais; Entrada não autorizada / intrusão de instalações; Envio de Malware; Intrusão em sistemas; Spoofing; Ataque a sistemas (DDoS); Chantagem/suborno/extorsão; Uso impróprio de recursos computação; Forjamento de direitos	I (alguns A) I I I I I A, I A, I I I I A, I I I I I I I
Falha de terceiros	Interrupções de abastecimento; Interrupção de refrigeração/AVAC; Perda de fornecimento energia; Interrupção de serviço de Telecomunicações; Falha de equipamentos de telecomunicações	A, I A, I A, I, N A, I A,I
Outros	Fogo; água; poluição/radiação; acidente grave; explosão; poeira/corrosão/congelamento; Radiação eletromagnética/térmica; Impulsos eletromagnéticos; Falta de recursos humanos/financeiros	A / I / N

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.

13 Anexo II — Catálogo de Vulnerabilidades (CNCS)

A Tabela a seguir contém alguns exemplos de vulnerabilidades. A lista pode ser usada durante o processo de avaliação dos riscos.

Tipo	Exemplos de vulnerabilidades
Hardware	Manutenção/instalação deficiente; Ausência de rotina de substituição; Humidade/poeira; radiação EM; Controlo de mudanças insuficiente; variações de voltagem/temperatura; armazenamento não protegido; descarte sem sanitização; Cópias não controladas
Software	Testes insuficientes; falhas conhecidas; ausência de logout; reutilização de suportes sem limpeza; ausência de registos; direitos de acesso indevidos; software amplamente distribuído; dados errados; UI complexa; documentação insuficiente; parâmetros mal configurados; datas incorretas; ausência de autenticação; listas de passwords desprotegidas; gestão fraca de passwords; serviços desnecessários ativos; software imaturo; especificações confusas; controlo de mudanças ineficaz; downloads não controlados; falta de backups; falta de relatórios de gestão
Rede	Evidências de envio/receção inexistentes; Linhas desprotegidas; Tráfego sensível desprotegido; cablagem deficiente; Ponto único de falha; Autenticação do emissor/recetor ineficaz; Arquitetura insegura; Passwords em claro; Gestão de rede inadequada; Ligações públicas desprotegidas
Pessoas	Ausência de RH; Recrutamento inadequado; Formação insuficiente; Uso incorreto de TI; Falta de consciencialização; Ausência de monitorização; Trabalho não supervisionado; Políticas insuficientes de telecomunicações e mensagens
Local/Instalações	Uso inadequado de controlos de acesso físico; localização em zonas inundáveis; fornecimento instável de energia; proteção física insuficiente (prédio/portas/janelas)
Organização	Registo/remoção de utilizadores inexistente; revisão de acessos ineficaz; cláusulas de segurança insuficientes em contratos; monitorização deficiente das instalações; auditorias inexistentes; processo de gestão de risco inexistente; logs de administradores insuficientes; resposta de manutenção inadequada; SLA inexistente; gestão de mudanças ineficaz; controlo documental do SGSI ineficaz; supervisão de registos do SGSI ineficaz; autorização de informação pública ineficaz; responsabilidades de SI mal atribuídas; PCN inexistente/desatualizado; política de e-mail ineficaz; procedimentos de instalação de software ineficazes; manuseamento de informação classificada ineficaz; ausências de responsabilidades de SI nas funções; cláusulas contratuais com funcionários insuficientes; processo disciplinar inadequado; política de dispositivos móveis inadequada; controlo de ativos off-site insuficiente; política de secretária/ecrã limpos insuficiente; autorizações de acesso às instalações inexistentes; monitorização de violações de segurança insuficiente; reporte de fragilidades inexistente; cumprimento de DPI insuficiente.

A reprodução ou comunicação, escrita ou verbal, ainda que parcial, deste documento, sem aprovação prévia da JFA é estritamente proibida e punida nos termos da lei. As informações contidas neste documento são propriedade da JFA.