

POLÍTICA DE PROTEÇÃO DE DADOS, PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Outubro de 2026

ÍNDICE

CAPÍTULO I. PROTEÇÃO DE DADOS E PRIVACIDADE 3
Cláusula 1ª. Compromisso de Proteção de Dados 3
Cláusula 2ª. Definições 3
Cláusula 3ª. Entidade Responsável pelo Tratamento 4
Cláusula 4ª. Encarregado de Proteção de Dados 4
Cláusula 5ª. Recolha e Tratamento de Dados Pessoais 4
Cláusula 6ª. Categorias de Dados Pessoais Tratados 5
Cláusula 7ª. Princípios Jurídicos 5
Cláusula 8ª. Fundamentos de Legitimidade 6
Cláusula 9ª. Finalidade do Tratamento 6
Cláusula 10ª. Transparência e Fornecimento dos Dados 7
Cláusula 11ª. Conservação dos Dados 7
Cláusula 12ª. Comunicação de Dados a Outras Entidades 8
Cláusula 13ª. Destinatários de Dados 9
Cláusula 14ª. Transferências Internacionais de Dados 9
Cláusula 15ª. Medidas de Segurança 9
Cláusula 16ª. Utilização de Cookies 10
Cláusula 17ª. Exercício dos Direitos dos Titulares dos Dados Pessoais 11
Cláusula 18ª. Reclamações e Sugestões 12
Cláusula 19ª. Comunicação de Incidentes 12
Cláusula 20ª. Consentimento Expresso e Conhecimento da Política 12
Cláusula 21ª. Atualizações à Informação Geral sobre Proteção de Dados 13
CAPÍTULO II. SEGURANÇA DA INFORMAÇÃO 13
Cláusula 22ª. Orientações Gerais 13
Cláusula 23ª. Âmbito de Aplicação e Destinatários 14
Cláusula 24ª. Valor da Informação 14
Cláusula 25ª. Importância da Segurança da Informação 14
Cláusula 26ª. Modelo de Segurança da Informação 15
Cláusula 27ª. Responsabilidades na Segurança da Informação 15
Cláusula 28ª. Manutenção e Comunicação das Políticas de Segurança 16

CAPÍTULO I. PROTEÇÃO DE DADOS E PRIVACIDADE

Cláusula 1ª. Compromisso de Proteção de Dados

1) A Junta de Freguesia da União das Freguesias de Sacavém e Prior Velho (de agora em diante abreviada para JFSPV) assume o compromisso de proteger os dados pessoais, a privacidade e a segurança da informação no exercício das suas atribuições e na prestação dos seus serviços.
2) O tratamento de dados pessoais observa o Regulamento (UE) 2016/679, de 27 de abril de 2016, Regulamento Geral sobre a Proteção de Dados (RGPD), a Lei n.º 58/2019, de 8 de agosto, e a legislação aplicável a cada atividade. A JFSPV adota medidas técnicas e organizativas adequadas e mantém evidência do cumprimento das suas obrigações, ambas na versão atual.
3) Esta política estabelece o enquadramento geral dos tratamentos de dados pessoais realizados no âmbito da atividade da JFSPV, independentemente do serviço, do canal de recolha ou do suporte utilizado. Abrange os serviços presenciais, os contatos telefónicos e por correspondência, os canais digitais e os sistemas internos.

Cláusula 2ª. Definições

1) Na presente Política de Proteção de Dados, Privacidade e Segurança da Informação, são utilizadas as seguintes principais definições:
   a) Dados pessoais: informações relativas a uma pessoa singular identificada ou identificável. A identificação pode resultar do nome, de um número de identificação, de dados de localização, de identificadores digitais ou da combinação de elementos relativos à pessoa;
   b) Tratamento: qualquer operação sobre dados pessoais, por meios automatizados ou não, incluindo recolha, registo, organização, consulta, utilização, comunicação, conservação, alteração, limitação, apagamento ou destruição;
   c) Responsável pelo tratamento: entidade que determina as finalidades e os meios de tratamento dos dados pessoais. Subcontratante: entidade que trata dados por conta do responsável, segundo as suas instruções;
   d) Cookies: pequenos ficheiros colocados no dispositivo através do navegador, que podem permitir o funcionamento de um serviço, guardar preferências ou apoiar outras funcionalidades, como a análise estatística da navegação.

Cláusula 3ª. Entidade Responsável pelo Tratamento

1) A JFSPV (União das Freguesias de Sacavém e Prior Velho), NIF n.º 510.839.355, com sede no Largo 1.º de Maio, n.º 1, 2685-099 Sacavém, é a responsável pelo tratamento dos dados pessoais disponibilizados no âmbito dos seus serviços e dos canais institucionais.
2) Quando a JFSPV intervenha num tratamento por conta de outra entidade ou em conjunto com ela, as responsabilidades são definidas de acordo com o enquadramento aplicável e comunicadas aos titulares dos dados.

Cláusula 4ª. Encarregado de Proteção de Dados

1) O Encarregado de Proteção de Dados (EPD) é o ponto de contato para esclarecimentos, exercício de direitos, reclamações e questões relativas a incidentes de proteção de dados. Exerce funções de informação, aconselhamento e acompanhamento com a independência prevista na lei.
2) As comunicações podem ser dirigidas a epd@uf-sacavemepriorvelho.pt, indicando no assunto "À atenção do Encarregado de Proteção de Dados", ou por correio para a sede, devendo ser indicado um meio de contato para resposta.
3) O contato do Responsável do Canal de Denúncia na JFSPV é o e-mail denuncias@uf-sacavemepriorvelho.pt. Para questões de proteção de dados relativas a uma denúncia, não é necessário enviar o seu conteúdo integral.

Cláusula 5ª. Recolha e Tratamento de Dados Pessoais

1) A JFSPV recolhe e utiliza apenas os dados pessoais necessários à apreciação de pedidos, à prestação de serviços e ao cumprimento das suas atribuições. A recolha pode ocorrer presencialmente, por telefone, por correio, por email, por formulários ou através das aplicações e plataformas digitais utilizadas pela JFSPV.
2) Os dados são obtidos junto do titular ou do seu representante e, quando exista fundamento, junto de outras entidades ou intervenientes nos processos. Na recolha indireta, é prestada a informação legalmente exigida, salvo exceção aplicável e fundamentada.
3) A utilização dos canais digitais pode gerar registos técnicos, como data e hora de acesso e informação sobre o dispositivo e o navegador. O tratamento pode ser informático ou manual e limita-se às finalidades comunicadas ao titular.
4) No canal de denúncia podem ser tratados a identificação e os contatos do denunciante, quando fornecidos, os factos comunicados, a identificação das pessoas visadas ou de terceiros, os documentos apresentados e a informação necessária ao seguimento.

Cláusula 6ª. Categorias de Dados Pessoais Tratados

1) As categorias de dados variam consoante o serviço e podem compreender:
   a) Dados de identificação, contato e representação;
   b) Elementos de pedidos, requerimentos, marcações, reservas etc.;
   c) Dados de faturação, pagamento e informação financeira ou patrimonial;
   d) Informação sobre a vida familiar, social e profissional, quando necessário;
   e) Dados de trabalhadores, candidatos e demais intervenientes na atividade interna da JFSPV;
   f) Correspondência, mensagens, documentos e elementos dos processos administrativos ou de denúncia;
   g) Dados técnicos de acesso e navegação, bem como moradas dos locais de execução dos serviços.
2) A indicação de uma categoria não significa que esses dados sejam recolhidos em todos os serviços.
3) Dados de saúde ou outras categorias especiais, bem como dados relativos a condenações e infrações penais, apenas podem ser tratados nas condições legais aplicáveis.
4) Em cada serviço são solicitados apenas os dados adequados e necessários à finalidade em causa, sendo o titular informado sobre a sua utilização no momento da recolha.
5) A referência a uma categoria de dados nesta política não autoriza a sua recolha indiscriminada.

Cláusula 7ª. Princípios Jurídicos

1) O tratamento de dados pessoais respeita os princípios de licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade.
2) Os dados são recolhidos para finalidades determinadas e legítimas, limitados ao necessário, mantidos corretos e protegidos contra utilização indevida, perda, alteração ou acesso não autorizado.
3) A duração da conservação é determinada pelas finalidades e pelas obrigações legais aplicáveis.
4) A JFSPV documenta o cumprimento destes princípios e integra a proteção de dados na conceção dos serviços e nas suas configurações por defeito.

Cláusula 8ª. Fundamentos de Legitimidade

1) O fundamento jurídico é identificado para cada tratamento.
2) No exercício das atribuições da JFSPV, são especialmente relevantes o cumprimento de obrigações jurídicas e o exercício de funções de interesse público ou de autoridade pública, nos termos das alíneas c) e e) do n.º 1 do artigo 6.º do RGPD.
3) Quando aplicável, o tratamento pode basear-se na execução de um contrato com o titular ou em diligências pré-contratuais por ele solicitadas, no consentimento livre, específico, informado e inequívoco, ou na proteção de interesses vitais, nas condições previstas na lei.
4) O interesse legítimo não é fundamento para os tratamentos efetuados por autoridades públicas na prossecução das suas atribuições.
5) A prestação de serviços públicos e o cumprimento de obrigações laborais não devem depender de consentimentos desnecessários.
6) O tratamento necessário à receção e ao seguimento de denúncias assenta, em especial, no cumprimento das obrigações previstas na Lei n.º 93/2021, de 20 de dezembro.
7) Os tratamentos de categorias especiais de dados ou de dados relativos a infrações penais exigem ainda o enquadramento dos artigos 9.º ou 10.º do RGPD, conforme o caso.

Cláusula 9ª. Finalidade do Tratamento

1) Os dados pessoais destinam-se à gestão e à resposta a pedidos, à emissão de documentos, ao atendimento, às marcações e reservas, à execução de serviços, à gestão de atividades e apoios e às comunicações necessárias ao relacionamento com a JFSPV.
2) No âmbito interno, podem ser necessários à gestão de recursos humanos e recrutamento, à organização do trabalho, aos processos eleitorais internos, à contratação, à gestão financeira e ao cumprimento de obrigações administrativas.
3) Estes tratamentos respeitam as competências, os regimes e os procedimentos próprios de cada atividade, incluindo o segredo do voto quando aplicável.
4) Os dados técnicos necessários destinam-se ao funcionamento e à segurança dos sistemas. A análise estatística dos canais digitais destina-se à melhoria dos serviços.
5) A gestão de denúncias tem a finalidade própria de receber, analisar e dar seguimento às infrações comunicadas, com acesso restrito e confidencialidade.

6) As subscrições facultativas, newsletters e outras comunicações adicionais, quando existentes, têm informação e fundamento próprios, com possibilidade de recusa ou retirada do consentimento quando aplicável.
7) A publicação de fotografias ou vídeos exige avaliação específica; a participação numa atividade não representa autorização geral para divulgar imagens.
8) Os dados não podem ser reutilizados para finalidades incompatíveis com as que justificaram a sua recolha.
9) A finalidade e o fundamento jurídico aplicáveis são comunicados ao titular no contexto da recolha e antes de uma utilização posterior para uma finalidade diferente, nos termos legais.

Cláusula 10ª. Transparência e Fornecimento dos Dados

1) A JFSPV presta informação sobre o tratamento de dados pessoais de forma clara, concisa, compreensível e acessível, no contexto da recolha e através dos meios adequados ao serviço. Esta política constitui o enquadramento geral dessa informação.
2) O titular é informado sobre a finalidade e o fundamento jurídico do tratamento, os destinatários ou categorias de destinatários, as eventuais transferências internacionais, a conservação e os direitos aplicáveis.
3) Os dados obrigatórios são distinguidos dos facultativos, com indicação das consequências de não fornecer os elementos indispensáveis ao pedido ou serviço.
4) Quando os dados sejam obtidos de outra fonte, a JFSPV informa o titular sobre a sua origem e as categorias em causa, nos termos e nas condições previstos no RGPD.
5) Quando aplicável, informa igualmente sobre decisões exclusivamente automatizadas com efeitos jurídicos ou impacto semelhante, incluindo a lógica, a importância e as consequências previstas, assegurando as garantias legais.
6) Nos serviços com requisitos próprios, incluindo o canal de denúncia, são observadas as regras legais relativas à informação dos intervenientes, à confidencialidade, ao acesso e ao exercício de direitos.

Cláusula 11ª. Conservação dos Dados

1) Os dados pessoais são conservados durante a gestão do pedido ou processo, a prestação do serviço ou a vigência da relação que justificou a sua recolha.
2) Após a sua conclusão, a conservação limita-se ao cumprimento de obrigações legais e arquivísticas, à resolução de reclamações ou processos pendentes e à declaração, ao exercício ou à defesa de direitos, enquanto subsistir o fundamento aplicável.

3) A duração da conservação é determinada pela finalidade do tratamento, pela duração do procedimento ou relação e pelos regimes legais de arquivo, prova e responsabilidade aplicáveis. São respeitadas as obrigações de conservação permanente e os regimes próprios, incluindo o previsto na Lei n.º 93/2021, de 20 de dezembro, na versão atual, para as denúncias.
4) Quando deixem de ser necessários e não subsista obrigação ou fundamento de conservação, os dados são eliminados de forma segura ou efetivamente anonimizados.
5) As cópias operacionais, exportações, registos técnicos e cópias de segurança ficam sujeitos a conservação limitada e adequada à respetiva função.

Cláusula 12ª. Comunicação de Dados a Outras Entidades

1) A prestação de serviços pode envolver entidades externas, nomeadamente fornecedores de alojamento, manutenção informática, comunicações, atendimento digital e outros serviços de apoio. O seu acesso aos dados limita-se ao necessário para a função desempenhada.
2) A JFSPV recorre à OVHcloud como prestador de serviços de alojamento dos seus canais digitais e aplicações institucionais, incluindo o site institucional, os portais de marcações e de denúncias, a intranet e outras aplicações institucionais alojadas na mesma infraestrutura.
3) Na medida em que trate dados pessoais por conta da JFSPV, a OVHcloud atua como subcontratante, nos termos contratuais e legais aplicáveis.
4) A JFSPV recorre a entidades que ofereçam garantias suficientes de proteção de dados. Quando estas atuem como subcontratantes, a JFSPV regula o tratamento por contrato ou outro instrumento jurídico conforme o artigo 28.º do RGPD, com instruções, confidencialidade, segurança e regras relativas a outros subcontratantes.
5) A eventual intervenção de fornecedores não permite utilizar os dados para finalidades próprias sem fundamento e informação adequados.
6) A JFSPV presta aos titulares informação sobre os destinatários ou categorias de destinatários envolvidos no tratamento dos seus dados.

Cláusula 13ª. Destinatários de Dados

1) Os dados são acessíveis aos serviços e às pessoas autorizadas que deles necessitem para o exercício das suas funções. Podem ser comunicados a entidades públicas, autoridades administrativas, judiciárias ou policiais e a outros destinatários quando exista fundamento jurídico aplicável.
2) A comunicação de dados limita-se aos destinatários legítimos e às finalidades informadas ao titular. A divulgação em atas, editais ou outros atos sujeitos a publicidade respeita a obrigação legal concreta e a minimização dos dados.
3) No canal de denúncia, o acesso cabe ao gestor e às pessoas expressamente autorizadas para a receção ou o seguimento, na medida necessária.
4) A identidade do denunciante e os elementos que a revelem são confidenciais, a sua divulgação apenas pode ocorrer nas condições legais, incluindo a informação prévia ao denunciante quando exigida.
5) Os dados das pessoas visadas e de terceiros beneficiam igualmente de proteção.

Cláusula 14ª. Transferências Internacionais de Dados

1) Uma transferência de dados pessoais para fora do Espaço Económico Europeu apenas pode ocorrer nas condições do Capítulo V do RGPD, nomeadamente com base numa decisão de adequação aplicável ou em garantias adequadas, incluindo cláusulas contratuais-tipo quando pertinentes.
2) A avaliação abrange o armazenamento, os acessos para efeitos de assistência técnica e a intervenção de outros prestadores.
3) A localização do alojamento principal na Europa não garante que todas as operações sejam realizadas nesse espaço.
4) Quando existam transferências, a JFSPV informa o titular sobre o seu enquadramento e sobre a forma de consultar ou obter as garantias aplicáveis. O titular pode pedir esclarecimentos ao EPD.

Cláusula 15ª. Medidas de Segurança

1) A JFSPV assegura medidas técnicas e organizativas adequadas à natureza dos dados e aos riscos para os titulares, tendo em conta o estado da técnica, os custos e o contexto do tratamento.
2) As medidas destinam-se a proteger contra acesso ou divulgação não autorizados, perda, destruição, alteração e outras utilizações ilícitas.

3) Este enquadramento abrange controlo de acessos, proteção das comunicações e credenciais, atualização dos sistemas, cópias de segurança, confidencialidade, gestão de incidentes e eliminação segura.

4) Os fornecedores com acesso a dados devem observar requisitos de proteção compatíveis com as suas funções.

5) Os utilizadores devem proteger os seus códigos e palavras-passe, não os partilhar e manter os dispositivos em condições de segurança. Estas precauções não afastam as responsabilidades da JFSPV.

6) As denúncias exigem acesso restrito e proteção reforçada da identidade dos intervenientes. Exportações, documentos enviados e cópias existentes nos dispositivos respeitam as restrições aplicáveis aos dados de origem. As orientações gerais de segurança da informação constam no Capítulo II desta política.

Cláusula 16ª. Utilização de Cookies

1) Os canais digitais podem utilizar cookies para assegurar o funcionamento dos serviços, guardar preferências e apoiar a análise estatística.

2) A informação sobre os cookies utilizados abrange as suas finalidades, os fornecedores e as durações, nos termos da política de cookies:

   a) Cookies Essenciais: permitem funções necessárias ao serviço solicitado, como a autenticação e a manutenção da sessão;

   b) Cookies de Funcionalidade: guardam preferências ou opções de utilização, o enquadramento depende da função concreta;

   c) Cookies Analíticos: permitem conhecer a utilização dos canais e apoiar a melhoria do serviço. Podem envolver identificadores ou outros dados pessoais, mesmo sem conter o nome do utilizador.

3) Quanto à duração, os cookies podem ser de sessão, eliminados no final da sessão, ou persistentes, mantidos pelo período definido ou até à sua eliminação.

4) O armazenamento ou acesso à informação no dispositivo depende de consentimento prévio, salvo as exceções legais para a transmissão de comunicações e para funções estritamente necessárias ao serviço expressamente solicitado.

5) Os cookies não essenciais devem permanecer bloqueados até existir consentimento válido, com possibilidade de recusa e posterior alteração ou retirada da escolha.

6) O utilizador pode também gerir ou eliminar cookies no navegador, embora o bloqueio dos essenciais possa afetar determinadas funcionalidades. As opções do navegador não substituem o mecanismo de consentimento do serviço.

7) É vedado o envio de conteúdos dos formulários, mensagens ou denúncias, bem como de nomes, emails ou outros elementos de identificação direta, para ferramentas de análise estatística.
8) A medição de aberturas ou cliques em comunicações eletrónicas exige informação e enquadramento próprios, sem ficar autorizada pela simples leitura desta política.
9) Política de cookies: https://uf-sacavemepriorvelho.pt/politica-de-cookies/.

Cláusula 17ª. Exercício dos Direitos dos Titulares dos Dados Pessoais

1) Nas condições previstas no RGPD, o titular pode solicitar acesso aos seus dados, retificação, apagamento, limitação do tratamento e oposição. A portabilidade aplica-se aos tratamentos automatizados baseados em consentimento ou contrato.
2) Quando o tratamento dependa de consentimento, este pode ser retirado sem afetar a licitude do tratamento anterior.
3) Nas condições do artigo 22.º do RGPD, o titular beneficia ainda do direito de não ficar sujeito a decisões baseadas exclusivamente no tratamento automatizado com efeitos jurídicos ou impacto semelhante, com as exceções e garantias previstas nesse artigo. Os direitos estão sujeitos às condições e limitações legais.
4) O apagamento pode não ser possível quando haja obrigação de conservação ou necessidade de exercício de funções públicas.
5) O acesso não confere direito a obter dados de terceiros sem fundamento ou a conhecer a identidade confidencial de um denunciante.
6) Os pedidos podem ser apresentados por escrito para o Encarregado de Proteção de Dados epd@uf-sacavemepriorvelho.pt, à atenção do EPD, ou por correio para a sede com a mesma indicação.
7) Questões relativas ao canal de denúncias podem também ser apresentadas através de denuncias@uf-sacavemepriorvelho.pt, evitando a divulgação desnecessária de informação confidencial.
8) A resposta é prestada nos prazos legais aplicáveis, a contar da receção do pedido.
9) A verificação da identidade limita-se ao necessário e o exercício dos direitos é, em regra, gratuito. Se o pedido não puder ser satisfeito, devem ser explicados os motivos e os meios de reclamação e recurso.

Cláusula 18ª. Reclamações e Sugestões

1) As reclamações e sugestões sobre proteção de dados podem ser dirigidas ao EPD através de epd@uf-sacavemepriorvelho.pt, à sua atenção.
2) O titular pode apresentar reclamação à Comissão Nacional de Proteção de Dados (CNPD), independentemente de reclamação interna prévia, sem prejuízo dos restantes meios administrativos e judiciais aplicáveis, em https://www.cnpd.pt/; email geral@cnpd.pt, Av. D. Carlos I, 134, 1.º, 1200-651 Lisboa, (+351) 213.928.400.
3) As reclamações sobre serviços e as denúncias de infrações seguem os respetivos procedimentos, ainda que também possam suscitar questões de proteção de dados.

Cláusula 19ª. Comunicação de Incidentes

1) A perda de documentos, o envio de informação para um destinatário errado, a divulgação indevida ou um acesso suspeito devem ser comunicados sem demora à JFSPV, pelos contatos gerais ou através do EPD.
2) A comunicação deve indicar o que aconteceu, quando, o serviço afetado e um contato para esclarecimentos, na medida em que estes elementos sejam conhecidos.
3) A JFSPV avalia e regista a ocorrência, contém os seus efeitos e adota as medidas adequadas.
4) Quando legalmente exigido, uma violação de dados pessoais deve ser notificada à CNPD sem demora injustificada e, sempre que possível, até 72 horas após o seu conhecimento. Se a notificação à CNPD ocorrer depois desse prazo, é acompanhada da justificação do atraso.
5) Quando a violação possa implicar elevado risco para os direitos e liberdades das pessoas, deve ser comunicada aos titulares sem demora injustificada, nas condições e com as exceções do artigo 34.º do RGPD. Nem todos os incidentes exigem comunicação externa, mas as decisões devem ser fundamentadas.

Cláusula 20ª. Consentimento Expresso e Conhecimento da Política

1) A disponibilização desta política permite conhecer as condições gerais de tratamento. A sua leitura, a utilização dos serviços ou o fornecimento dos dados necessários a um pedido não equivalem a consentimento geral para qualquer finalidade.
2) Quando o consentimento seja o fundamento aplicável, deve ser solicitado separadamente, com informação clara e escolha livre, específica e inequívoca, sem opções previamente selecionadas.

3) A JFSPV assegura a demonstração do consentimento e permite a sua retirada com facilidade equivalente à da sua prestação.
4) A confirmação de leitura da política deve ser distinguida do consentimento.
5) A recusa de finalidades facultativas não pode impedir tratamentos necessários por outro fundamento jurídico.

Cláusula 21ª. Atualizações à Informação Geral sobre Proteção de Dados

1) A presente política é revista quando se alterem a legislação, os serviços ou os tratamentos realizados. A versão em vigor é mantida identificada e disponível no site institucional e nos restantes canais adequados, com informação sobre alterações relevantes.
2) As alterações relevantes aos tratamentos são comunicadas aos titulares pelos meios adequados. Páginas externas ligadas a partir dos canais da JFSPV têm regras próprias; essas regras não substituem os deveres da JFSPV quanto aos tratamentos em que participe.

CAPÍTULO II. SEGURANÇA DA INFORMAÇÃO

Cláusula 22ª. Orientações Gerais

1) A política de segurança da informação estabelece orientações gerais para proteger a informação e assegurar a continuidade dos serviços da JFSPV.
2) A política de segurança da informação abrange a gestão e a utilização de documentos, equipamentos, aplicações, redes e demais meios que suportam a atividade da JFSPV.
3) A implementação da política de segurança da informação é coordenada pelos responsáveis designados pela JFSPV, com responsabilidades e meios definidos, sendo que as políticas e os procedimentos internos concretizam estas orientações para os serviços, sistemas e atividades da JFSPV.

Cláusula 23ª. Âmbito de Aplicação e Destinatários

1) Esta política destina-se aos trabalhadores, titulares dos órgãos, prestadores de serviços e demais pessoas autorizadas a aceder à informação ou aos sistemas da JFSPV, no âmbito das suas funções e vínculos.
2) As pessoas abrangidas devem conhecer e cumprir as regras aplicáveis à sua atividade, proteger a informação a que acedem e comunicar riscos ou ocorrências.
3) As obrigações dos fornecedores são estabelecidas nos instrumentos contratuais adequados.

Cláusula 24ª. Valor da Informação

1) A informação pode existir em papel, em suporte digital, em comunicações eletrónicas ou na transmissão verbal. A sua proteção aplica-se independentemente da forma que assume, de acordo com a sensibilidade, a finalidade, o valor para os serviços e as consequências de uma perda ou divulgação indevida.
2) Os responsáveis dos serviços definem os acessos necessários e distinguem a informação pública, de uso interno e de acesso restrito, respeitando a lei.
3) A disponibilidade dos sistemas e a confiança no serviço dependem da preservação e da utilização adequada dessa informação.
4) Os dados de denúncias, saúde, situações sociais e processos individuais exigem especial cuidado. A existência de acesso técnico a um sistema não representa autorização geral para consultar o seu conteúdo.

Cláusula 25ª. Importância da Segurança da Informação

1) A perda de confidencialidade, integridade ou disponibilidade pode afetar os direitos das pessoas, interromper serviços e comprometer a confiança na JFSPV.
2) A segurança abrange todo o ciclo de vida da informação, desde a recolha até à eliminação ou ao arquivo.
3) A escolha e a revisão das medidas atendem aos riscos e às alterações tecnológicas, legais ou organizativas, sendo que a política orienta a atuação nas seguintes vertentes:
    a) Gestão de pessoas: comunicação das regras, formação adequada e atribuição de responsabilidades;
    b) Gestão do risco: identificação dos riscos dos sistemas e serviços, avaliação das consequências e escolha de medidas adequadas;
    c) Definição de responsabilidades: identificação de quem autoriza acessos, gere a informação e executa as medidas de proteção;

d) Operação dos sistemas: procedimentos documentados, manutenção, atualização e registos proporcionais das operações relevantes;

e) Decisão informada: definição de prioridades e disponibilização de meios pelo Executivo, considerando os custos e os riscos;

f) Acompanhamento: verificação da eficácia das medidas, comunicação de ocorrências e adoção de ações corretivas.

Cláusula 26ª. Modelo de Segurança da Informação

1) O modelo de segurança da informação assenta em três objetivos complementares:

   a) Confidencialidade: permitir o acesso à informação apenas às pessoas autorizadas;

   b) Integridade: preservar a exatidão da informação e protegê-la contra alterações indevidas;

   c) Disponibilidade: assegurar o acesso legítimo à informação e aos serviços quando necessário.

2) Os procedimentos internos concretizam estes objetivos através de regras de acesso, proteção dos equipamentos e comunicações, atualização dos sistemas, cópias de segurança, recuperação e eliminação segura. As medidas abrangem documentos e dispositivos, bem como a partilha verbal de informação.

Cláusula 27ª. Responsabilidades na Segurança da Informação

1) O Executivo da JFSPV aprova as orientações, atribui responsabilidades e disponibiliza os meios adequados sobre a segurança da informação.

2) Os responsáveis dos serviços identificam necessidades, autorizam acessos no âmbito das suas competências e acompanham o cumprimento dos procedimentos.

3) As funções técnicas internas ou contratadas executam as medidas que lhes sejam atribuídas, mantêm a documentação necessária e comunicam vulnerabilidades e incidentes.

4) Todos os utilizadores devem proteger credenciais, observar as permissões concedidas e reportar ocorrências.

5) O EPD acompanha as matérias de proteção de dados com independência, sem substituir os serviços na execução das medidas ou assumir funções incompatíveis.

6) A receção e a resposta a incidentes são coordenadas pelos responsáveis designados, de acordo com os contatos, as responsabilidades e as prioridades definidos, incluindo a articulação com fornecedores.

Cláusula 28ª. Manutenção e Comunicação das Políticas de Segurança

1) As políticas e os procedimentos de segurança são revistos periodicamente e após alterações relevantes ou incidentes, para assegurar a sua adequação aos serviços e aos riscos existentes.
2) As versões aprovadas são disponibilizadas às pessoas abrangidas, através da intranet ou de outros meios internos, com comunicação e formação adequadas às funções.
3) A política geral é disponibilizada aos cidadãos e às demais partes interessadas nos canais institucionais.
4) Os detalhes técnicos cuja divulgação aumente o risco constam de documentação interna sujeita a acesso controlado.
5) A verificação da eficácia das medidas e da capacidade de recuperação dos serviços integra a revisão dos procedimentos, com adoção de melhorias quando necessário.