

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - CSVH

APROVAÇÃO DO DOCUMENTO

	Função	Nome e assinatura	Data
Elaborado por	SI	Responsável de Segurança da Informação	07/04/2025
Aprovado por	PRD	Jorge Pereira	14/04/2025

REGISTOS DE ALTERAÇÕES / MODIFICAÇÕES

Edição	Data	Páginas alteradas	Alteração
1	07/04/2025	Todas	Redação Inicial

ÍNDICE

PREÂMBULO	3
1. OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO	4
2. ÂMBITO DE APLICAÇÃO E INCUMPRIMENTO	4
3. PRINCÍPIOS FUNDAMENTAIS	5
4. RESPONSABILIDADES	7
5. REGRAS E BOAS PRÁTICAS DE SEGURANÇA PREVENTIVA	8
5.1. UTILIZAÇÃO DE DISPOSITIVOS, SISTEMAS E TECNOLOGIAS DE INFORMAÇÃO	8
5.2. UTILIZAÇÃO DA INTERNET E DE CORREIO ELETRÓNICO (EMAIL)	9
5.3. PALAVRAS-PASSE (PASSWORDS) E AUTENTICAÇÃO FORTE.....	9
5.4. POSTOS DE TRABALHO FÍSICOS E IMPRESSORAS.....	10
6. CONFORMIDADE LEGAL.....	10
7. ENTRADA EM VIGOR E REVISÃO	10

Preâmbulo

O Centro Social do Vale do Homem, também designado por CSVH, enquanto IPSS, recolhe, armazena, processa e transmite informações em vários formatos (físicos e eletrónicos), com diferentes graus de sensibilidade. A proteção desta informação, bem como dos ativos que a suportam, é fundamental para que o CSVH cumpra a sua missão de prestar serviços de apoio à comunidade, promovendo o desenvolvimento e o bem-estar dos utentes e colaboradores, mantendo uma relação de confiança com todas as partes interessadas.

Esta Política de Segurança da Informação define objetivos e princípios para prevenir quaisquer ameaças (acidentais ou deliberadas, internas ou externas) que possam representar riscos para a segurança da informação. Neste sentido, atribuem-se responsabilidades e adotam-se medidas organizativas fundamentais, adequadas à especificidade da atividade.

Trata-se de um documento abrangente, que não substitui nem se sobrepõe à legislação em vigor. Com o objetivo de ser compreendido por todos, apresenta princípios gerais sendo que, aspetos mais específicos ou técnicos são regulados em normativos ou procedimentos internos mais detalhados.

1. Objetivos da Segurança da Informação

Os principais objetivos da segurança da informação do CSVH são:

- **Salvaguardar a privacidade, a integridade e a acessibilidade da informação**

O CSVH compromete-se a assegurar que a informação, em todas as suas formas, está protegida contra acessos não autorizados, modificações ilícitas e indisponibilidade. Esta salvaguarda é essencial para garantir a gestão segura e de confiança da informação.

- **Sustentar a funcionalidade do CSVH**

O CSVH procura proteger os seus sistemas de informação contra ameaças acidentais ou intencionais, assegurando a continuidade dos serviços.

- **Garantir a conformidade com leis, regulamentos e contratos**

No que respeita à segurança da informação, o CSVH empenha-se em cumprir a legislação aplicável. Assim, reforça-se a reputação da instituição e previnem-se incidentes de segurança que possam afetar a confiança de utentes, colaboradores, fornecedores e outras partes interessadas.

- **Alinhar as práticas de segurança da informação com os objetivos gerais do CSVH**

A segurança da informação é parte integrante da missão do CSVH prestar serviços de apoio à comunidade de forma transparente e eficaz. Assim, estas práticas são concebidas para sustentar a estratégia global do CSVH.

2. Âmbito de aplicação e Incumprimento

A Política de Segurança da Informação do CSVH é aplicável a todos os membros dos órgãos da instituição, colaboradores, prestadores de serviços, consultores, parceiros ou qualquer outra entidade (individual ou coletiva) que tenha acesso às instalações, equipamentos ou sistemas de informação da CSVH, assinando para o efeito, no momento da celebração de contrato / acordo, a Declaração de Leitura e Tomada de Conhecimento da Política de Segurança da Informação. (Anexo 1)

Para efeitos desta Política, consideram-se “colaboradores do CSVH” todas as pessoas que desempenham a sua atividade no CSVH num posto de trabalho com acesso aos sistemas de informação da instituição, independentemente da natureza ou duração do vínculo, incluindo dirigentes, trabalhadores, prestadores de serviços, estagiários, voluntários e outros.

Todos os indivíduos mencionados são obrigados a conhecer, aderir e cumprir a Política de Segurança da Informação.

É da responsabilidade de todas as partes interessadas contribuírem proactivamente para a segurança da informação.

Todas as partes interessadas que estão abrangidas pela Política de Segurança da Informação e que deliberadamente violem esta ou outra política decorrente da atividade do CSVH, ficam sujeitas a sanções e outras ações, que podem ir até à cessação de contrato e/ou à participação às autoridades policiais ou judiciais das situações que indiciem a prática de crime.

Em caso de dúvida, as pessoas abrangidas por esta Política devem atuar com prudência, evitando comportamentos de risco, e podem solicitar esclarecimentos ao Responsável pela Segurança da Informação.

3. Princípios Fundamentais

A Política de Segurança da Informação do CSVH orienta-se pelos seguintes princípios:

- **Preservação**

Todos os colaboradores abrangidos pela Política são responsáveis pela preservação da segurança da informação, reportando imediatamente qualquer violação e atuando de acordo com normas e boas práticas vigentes usando para o efeito o seguinte endereço eletrónico: suporteinformatico@csvh.pt

- **Confidencialidade**

A informação deve ser acessível apenas a utilizadores autorizados, prevenindo-se acessos indevidos, deliberados ou acidentais, a dados sensíveis, sistemas, redes e outros recursos críticos, como plataformas digitais ou sistemas de gestão administrativa.

- **Integridade**

O CSVH protege a integridade — completude e exatidão da informação — prevenindo a destruição ou modificação não autorizada de ativos físicos ou digitais, para salvaguardar a fiabilidade dos dados e processos administrativos.

- **Disponibilidade**

O CSVH garante que a informação está disponível para as pessoas autorizadas sempre que necessário, a fim de assegurar a continuidade dos serviços. São implementadas configurações técnicas que permitem detetar e responder rapidamente a incidentes que possam afetar a disponibilidade dos sistemas e dados.

Compromissos Adicionais

- **Autenticação**

Assegurar a identidade dos utilizadores e a legitimidade dos processos que acedem ou transmitem informação, permitindo acesso apenas a pessoas autorizadas.

- **Não Repúdio**

Evitar que um utilizador envolvido na produção ou troca de informação possa negar a sua participação no processo, mantendo registos que permitam rastrear a origem das ações.

- **Privacidade e Proteção de Dados**

Proteger a informação de acordo com a sua relevância e de acordo com o definido no Regulamento Geral de Proteção de Dados do CSVH, garantindo que dados pessoais são tratados exclusivamente para as finalidades legais e protegidos contra acessos não autorizados, com atenção especial a dados sensíveis de utentes, colaboradores e outras partes interessadas.

- **Legalidade**

Cumprir e fazer cumprir toda a legislação e regulamentação aplicáveis em matéria de segurança da informação e proteção de dados pessoais, alinhando com os requisitos nacionais e europeus.

- **Transparência, Comunicação e Informação**

Promover comunicações claras sobre a política geral, políticas específicas, procedimentos e normas de segurança, assegurando que todos conhecem as suas responsabilidades. Proporcionar orientações específicas para diferentes áreas e equipas, garantindo a transparência e o envolvimento de todos.

- **Formação**

Implementar um plano de formação contínua em segurança da informação, disponibilizando ações formativas adaptadas aos diversos setores do CSVH, com foco nas necessidades específicas das várias áreas de atuação.

4. Responsabilidades

Todos os que se encontram abrangidos pela presente Política são responsáveis por cumpri-la e fazê-la cumprir.

Em particular:

- **Órgãos de Gestão (Direção, Assembleia Geral e Conselho Fiscal)**
 - Garantir que os objetivos de segurança da informação estão alinhados com a atividade da instituição e integrados em processos relevantes.
 - Aprovar, publicar e promover a Política de Segurança da Informação.
- **Responsável de Segurança da Informação**
 - Executar as estratégias definidas pelos órgãos competentes, gerindo requisitos de segurança e notificações de incidentes.
 - Elaborar e atualizar o Plano de Segurança e o relatório anual relativo à matéria de segurança, enviado para o Departamento da Qualidade, até 31/01 de cada ano referente ao ano anterior.
 - Apoiar o Executivo na definição da estratégia de segurança da informação.
 - Identificar ameaças, avaliar vulnerabilidades e propor políticas de cibersegurança, caso exigível pelas autoridades nacionais competentes (p. ex. CNCS).
 - Supervisionar a gestão de ativos e promover formação e sensibilização em procedimentos específicos.
 - Acompanhar a implementação das medidas de segurança, assegurando o cumprimento das obrigações legais.
 - Em colaboração com o Encarregado de Proteção de Dados, atuar como ponto de contacto com a Comissão Nacional de Proteção de Dados (CNPd).
- **Encarregado de Proteção de Dados (DPO)**
 - Sensibilizar os utilizadores para a importância da deteção e comunicação atempada de incidentes de segurança.
- **Colaboradores, Fornecedores, Prestadores de Serviço e outras partes interessadas**
 - Adotar as regras e boas práticas de segurança preventiva estabelecidas.
 - Conhecer e cumprir a Política de Segurança da Informação.
 - Contribuir para salvaguardar a segurança da informação e a continuidade dos serviços prestados pela Instituição.
 - Assumir responsabilidade pela utilização indevida das suas contas e dos recursos que lhes são atribuídos, em qualquer situação.

- Comunicar imediatamente qualquer falha ou não conformidade detetada, de acordo com o procedimento de notificação de incidentes, ao Responsável pela Segurança da Informação.
- Participar ativamente em ações de formação disponibilizadas pelo CSVH, adequando-se às funções de cada um, mantendo atualizados os conhecimentos e competências neste domínio.
- No caso dos fornecedores, assegurar a segurança da informação do CSVH apenas nos sistemas abrangidos pelo contrato em vigor e apresentar evidências de maturidade em cibersegurança, se solicitado.

5. Regras e Boas Práticas de Segurança Preventiva

5.1. Utilização de Dispositivos, Sistemas e Tecnologias de Informação

- Os equipamentos (computadores, telemóveis, tablets, etc.) e os sistemas de informação disponibilizados são propriedade do CSVH. A sua utilização é exclusiva de pessoas autorizadas e para fins profissionais.
- Ao utilizar um dispositivo da instituição, o utilizador tem consciência de que a informação criada, editada ou armazenada pode ser monitorizada, auditada ou entregue a terceiros nos termos da lei.
- É proibida a divulgação de informação interna e/ou confidencial sem autorização. Qualquer pedido de acesso a informação deve ser encaminhado ao(à) responsável competente para obter autorização de acesso.
- A instalação de software só pode ser realizada por administradores autorizados ou em coordenação com estes. Não é permitida a instalação ou execução de software não autorizado ou sem licença.
- Não devem ser ligados dispositivos externos não autorizados (por exemplo, discos externos, routers, Wi-Fi privadas) à infraestrutura do CSVH. Caso seja autorizada a utilização de hardware privado para fins profissionais, devem ser cumpridas as regras de proteção contra qualquer tipo de Malware.
- O uso de soluções antivírus e antimalware é obrigatório, não devendo o colaborador desativar ou contornar estas soluções. Qualquer suspeita de infeção deve ser comunicada de imediato.
- Sempre que um utilizador se ausente do seu posto, deve bloquear o computador. Nos postos de trabalho partilhados, ao final do dia, as aplicações devem ser fechadas e o computador deve ser desligado.

5.2. Utilização da Internet e de Correio Eletrónico (Email)

- Não é permitida a utilização da infraestrutura da instituição para transferir conteúdos ilegais ou que contradigam as normas em vigor ou o regulamento interno, pondo em causa a segurança da informação.
- Não é permitido alterar as configurações de rede ou desativar sistemas de segurança implementados no acesso à Internet.
- Os utilizadores não devem abrir ou descarregar ficheiros de sítios eletrónicos desconhecidos ou sem os mecanismos de deteção de vírus ativados.
- Não devem ser abertos emails de origem desconhecida ou com anexos suspeitos. Em caso de dúvida, é recomendável contactar o Responsável pela Segurança da Informação utilizando para o efeito o seguinte endereço eletrónico suporteinformatico@csvh.pt

5.3. Palavras-passe (Passwords) e Autenticação Forte

- Todas as palavras-passe utilizadas no CSVH são consideradas informação confidencial e intransmissível.
- O utilizador é responsável por alterar a palavra-passe inicial atribuída por defeito, definindo uma própria.
- A palavra-passe escolhida deve ser complexa (preferencialmente entre 10 e 12 caracteres, misturando maiúsculas, minúsculas, números e símbolos), de acordo com as regras específicas de cada sistema.
- Não deve ser selecionada a opção de gravação automática de palavras-passe em navegadores ou aplicações.
- Cada utilizador é responsável pela segurança das respetivas credenciais, não devendo divulgá-las nem armazená-las em locais com baixos índices de segurança.
- É proibido disfarçar a identidade eletrónica ou usar credenciais de terceiros nos sistemas de informação do CSVH.
- Se existir suspeita de violação ou comprometimento de uma palavra-passe, esta deve ser alterada imediatamente e comunicada a situação ao Responsável pela Segurança da Informação.
- No caso de contas partilhadas (quando justificadas), as palavras-passe não devem ser fornecidas a pessoas fora do grupo autorizado.
- Será privilegiada a adoção de mecanismos de autenticação forte, nomeadamente a utilização de dois fatores de autenticação (ex.: palavra-passe + código único enviado para telemóvel ou aplicação).

5.4. Postos de Trabalho Físicos e Impressoras

- Cada posto de trabalho deve estar organizado, cumprindo o princípio de clean desk, não deixando documentação confidencial ou reservada exposta ou em locais de fácil acesso.
- Os espaços onde se arquiva informação confidencial ou reservada devem ser trancados na ausência dos profissionais responsáveis.
- Documentos, impressões e anotações com dados sensíveis devem ser manuseados de forma a impedir o acesso de terceiros não autorizados.
- Ao imprimir ou fotocopiar documentação confidencial ou reservada, o responsável deve acompanhar a operação, de modo a impedir o extravio de informações.

6. Conformidade Legal

O CSVH compromete-se a cumprir todos os normativos legais em matéria de segurança da informação, nomeadamente:

- **Regulamento Geral sobre a Proteção de Dados (RGPD)** — Regulamento (UE) 2016/679, de 27 de abril
- **Lei n.º 46/2018, de 13 de agosto** (Regime Jurídico da Segurança do Ciberespaço)

7. Entrada em Vigor e Revisão

A presente Política de Segurança da Informação entra em vigor na data da sua publicação interna e será revista sempre que tal se revele necessário, por alteração legislativa, tecnológica ou organizativa, mantendo-se atualizada e adequada às necessidades do CSVH e às exigências legais em vigor.

DECLARAÇÃO DE LEITURA E TOMADA DE CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Eu, _____, com a categoria/cargo de _____, declaro, para todos os efeitos legais, que:

1. **Tomei conhecimento e li na íntegra** o conteúdo da Política de Segurança da Informação do CSVH, disponibilizada para consulta.
2. **Compreendi** todas as normas, responsabilidades e eventuais consequências do não cumprimento dos deveres nela estabelecidos.
3. **Comprometo-me** a respeitar e cumprir todas as diretrizes e instruções previstas na referida Política de Segurança da Informação.

Local: _____

Data: ____/____/____

Assinatura do(a) Declarante: _____

(O presente documento deve ser arquivado nos registos internos do CSVH.)

