Política de Segurança da Informação

(Informação Pública (P) – 2025 01)

Hydra iT

Política de Segurança da Informação

HISTORIAL DO DOCUMENTO

Versão	Elaboração/Revisão	Data	Descrição de alterações	Tipo de alteração (maior ou menor)
1	Luis Boutto	20-01-2025	Documento Inicial	

VALIDADE DO DOCUMENTO

Aprovação	Data	Observações
Gerência	03-02-2025	

Este documento é um documento controlado que revoga todas as anteriores versões. Quaisquer cópias com versões anteriores à atual ou com data anterior à data de publicação não deverão ser consideradas como válidas. Aquele que obtiver uma versão impressa deste documento é responsável por assegurar que a versão que possui é a última. A versão original deste documento encontra -se publicada no Portal interno da Organização no site do Sistema de Segurança da Informação.

Quaisquer nomes de produtos aqui utilizados são somente para fins de identificação, e podem ser marcas registadas das respetivas organizações.

Política de Segurança da Informação

ÍNDICE

Conteúdo

1. OBJETIVOS 4
1.1 Objetivo Geral 4
1.2 Objetivos Específicos 4
2. ÂMBITO 5
3. A INFORMAÇÃO E A SEGURANÇA DA INFORMAÇÃO 5
4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 5
5. RESPONSABILIDADES 6
6. MANUTENÇÃO 7

Política de Segurança da Informação

1. OBJETIVOS

1.1 Objetivo Geral

Definir um quadro de referência para garantir a proteção integral dos dados e recursos tecnológicos da Hydra iT, através da implementação de políticas, controlos de segurança e boas práticas, que minimizem os riscos de cibersegurança, assegurem o cumprimento normativo e promovam um ambiente de trabalho seguro e confiável para todos os utilizadores.

1.2 Objetivos Específicos

- ✓ **Estabelecer controlos de acesso e gestão de permissões:** Definir e aplicar políticas de acesso baseadas no princípio do privilégio mínimo, garantindo que os utilizadores apenas possam aceder à informação e funcionalidades necessárias para o seu papel.
- ✓ **Desenvolver um plano de resposta a incidentes de segurança:** Estabelecer um plano claro e eficaz para a identificação, contenção e mitigação de incidentes de segurança, bem como para a recuperação de dados e a continuidade do serviço.
- ✓ **Promover a formação e consciencialização em cibersegurança:** Conceber programas de formação contínua para os utilizadores, com foco na prevenção de ameaças comuns como o phishing e o manuseamento seguro da informação.
- ✓ **Compromisso com a melhoria contínua:** Garantir a eficácia dos processos de segurança da informação, em conformidade com a ISSO/IEC 27001, promovendo a proteção de dados e a gestão de riscos de forma sustentável.
- ✓ **Cumprir com as normativas e regulamentações aplicáveis:** Alinhar as políticas de segurança da Hydra iT com as normativas legais e regulamentares, garantindo o cumprimento e evitando sanções.
- ✓ **Estabelecer um sistema robusto de backup e recuperação de dados:** Implementar procedimentos regulares de cópias de segurança e planos de recuperação em caso de desastre para assegurar a disponibilidade e proteção dos dados críticos em caso de incidentes.

2. ÂMBITO

Esta política aplica-se a todos os colaboradores, subcontratados, parceiros e qualquer outra pessoa que tenha acesso aos sistemas de informação da organização. Abrange todos os sistemas, redes, dispositivos, aplicações e dados que sejam propriedade da organização ou que estejam sob o seu controlo.

3. A INFORMAÇÃO E A SEGURANÇA DA INFORMAÇÃO

A informação constitui o ativo mais valioso para as organizações. Por este motivo, a Hydra iT assume a responsabilidade de garantir que tanto os seus dados como os dos clientes que administra são geridos em conformidade com os seguintes princípios fundamentais:

- ✓ **Confidencialidade**: A informação deve ser protegida contra o acesso não autorizado. Apenas as pessoas autorizadas devem ter acesso à informação com base nos seus papéis e responsabilidades.
- ✓ **Integridade**: Os dados e sistemas devem ser precisos e estar protegidos contra modificações não autorizadas ou não intencionais. A integridade da informação é essencial para tomar decisões fiáveis.
- ✓ **Disponibilidade**: A informação e os sistemas devem estar disponíveis para os utilizadores autorizados quando necessário.

4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A proteção no tratamento de informação de parceiros de negócio e dados pessoais sob responsabilidade da Hydra iT de forma consistente com os requisitos profissionais, éticos, legais, regulamentares e contratuais, é uma das maiores prioridades da Empresa e algo que é considerado fundamental para o seu sucesso. A perda ou roubo de informação ou dados pessoais pode ter consequências graves a nível legal, financeiro e/ou reputacional, estando a Hydra iT comprometida

com a salvaguarda da privacidade, confidencialidade, integridade e disponibilidade da sua informação ou de parceiros de negócio, quer esta se encontre em suporte físico, digital ou intelectual.

5. RESPONSABILIDADES

Para garantir a eficácia do Sistema de Gestão de Segurança da Informação (SGSI), é crucial que cada nível da organização compreenda e assuma as suas responsabilidades específicas. A seguir, descrevem-se as funções e obrigações dos diversos papéis, desde a alta direção até aos colaboradores, assegurando uma abordagem integrada e consistente na proteção dos ativos de informação.

- ✓ **Direção**: É responsável por fornecer liderança, apoio e recursos para implementar e manter o SGSI. Deve garantir que a política seja revista periodicamente e ajustada conforme necessário.
- ✓ **Responsável pela Segurança da Informação (RSI)**: O RSI é responsável por desenvolver, implementar, manter e gerir o SGSI, garantindo o cumprimento da política de segurança em toda a organização.
- ✓ **Diretores e Gestores de equipas**: Os supervisores ou coordenadores de departamentos são responsáveis por garantir a aplicação eficaz das políticas de segurança da informação nas suas equipas. Devem monitorizar o cumprimento das diretrizes, promover a formação em segurança e reportar incidentes ou não conformidades.
- ✓ **Colaboradores e Subcontratados**: Todos os colaboradores e contratados devem cumprir esta política e os procedimentos de segurança associados. Qualquer violação da política deve ser imediatamente comunicada.

Todos os colaboradores, bem como terceiros, que de alguma forma possam interagir com informação de parceiros, colaboradores e da própria Hydra iT, estão obrigados a cumprir e a fazer cumprir todas as normas de segurança da informação, devendo prontamente reportar ao RSI qualquer evento que possa provocar, ou que tenha provocado, uma quebra de privacidade ou segurança da informação via email para servicedesk@hydra.pt.

Os colaboradores, bem como terceiros, poderão ser responsabilizados em caso de incumprimento com políticas e normas de segurança da informação estabelecidas pela Hydra iT.

6. MANUTENÇÃO

A Política de Segurança da Informação deverá ser revista sempre que necessário e, obrigatoriamente, pelo menos uma vez por ano, de forma a garantir que continua a ser adequada à Hydra iT e deve ser comunicada a todos os colaboradores.