					Insira aqui a designação da entidade jurídica registada							
Número do documento: P08S					Título do documento: **Política de sensibilização e formação em segurança da informação**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 7	
ISO/IEC 27002:2022	Controlo 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Diretiva NIS2 da UE	Artigo 21(2)(i)	
DORA da UE	Artigo 13	
COBIT 2019	BAI08, DSS05	
RGPD da UE	Artigo 32, 39	

1. Finalidade

1.1. Esta política assegura que todos os trabalhadores e prestadores de serviços compreendem as suas responsabilidades em matéria de segurança da informação.

1.2. Visa reduzir a probabilidade de erro humano, melhorar a capacidade de deteção e notificação de incidentes e promover uma cultura de segurança em toda a organização.

1.3. Esta política permite o cumprimento da ISO/IEC 27001, da NIS2, do RGPD e do DORA, ao integrar a sensibilização para a segurança nos comportamentos diários de trabalho e nas expectativas associadas a cada função.

2. Âmbito

2.1. Esta política aplica-se a todos os trabalhadores, prestadores de serviços, estagiários e terceiros que tenham acesso aos sistemas ou aos dados da empresa.

2.2. Inclui:

2.2.1. Formação inicial de sensibilização para a segurança no processo de integração de novos colaboradores

2.2.2. Formação anual de reciclagem em segurança

2.2.3. Ações ad hoc de sensibilização (por exemplo, atualizações relacionadas com incidentes, cartazes ou recomendações)

2.3. Aplica-se a todas as funções, departamentos e locais de trabalho.

3. Objetivos

3.1. Assegurar que todo o pessoal recebe formação de sensibilização para a segurança de forma atempada, compreensível e relevante.

3.2. Capacitar os trabalhadores para identificar e evitar ameaças comuns, como phishing, malware e fugas de dados.

3.3. Assegurar o registo da conclusão da formação para demonstrar o cumprimento de requisitos legais, contratuais e de auditoria.

3.4. Manter os conteúdos de formação atualizados, refletindo as políticas, ameaças e regulamentos aplicáveis à organização.

3.5. Promover uma postura proativa entre o pessoal, em que a segurança seja considerada parte da responsabilidade diária.

4. Papéis e responsabilidades

4.1. Diretor-Geral

4.1.1. Aprova os requisitos de formação e assegura a afetação dos recursos necessários.

4.1.2. Revê os relatórios de conclusão e procede ao escalonamento dos casos de incumprimento, quando necessário.

4.2. Responsável de escritório / Recursos Humanos

4.2.1. Coordena a realização da formação para novas admissões e da formação anual de reciclagem.

4.2.2. Mantém os registos de formação e de conclusão.

4.2.3. Assegura a confirmação, pelos trabalhadores, das principais políticas de segurança da informação e dos acordos de confidencialidade.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1. Revisão anual

9.1.1. Esta política deve ser revista anualmente pelo Diretor-Geral e pelos Recursos Humanos para assegurar que reflete os riscos, regulamentos e necessidades atuais da força de trabalho.

9.2. Atualizações intercalares

9.2.1. A política e o conteúdo da formação devem também ser revistos e atualizados após:

9.2.1.1. Um incidente de segurança significativo

9.2.1.2. Alterações legais ou contratuais

9.2.1.3. Reestruturação organizacional ou migrações de sistemas

9.3. Controlo de versões e distribuição

9.3.1. Cada atualização deve incluir:

9.3.1.1. Número da versão e data de entrada em vigor

9.3.1.2. Resumo das alterações

9.3.1.3. Aprovação pelo Diretor-Geral

9.3.1.4. Arquivo de todas as versões anteriores, conservado durante pelo menos três anos

9.4. Comunicação aos trabalhadores

9.4.1. As atualizações da política devem ser comunicadas a todo o pessoal, devendo ser obtida confirmação quando existam alterações materiais.

10. Políticas relacionadas e articulações

10.1. Esta política suporta o seguinte:

10.1.1. P2S – Política de Papéis e Responsabilidades de Governação: atribui a responsabilidade pela coordenação da formação e pela supervisão

10.1.2. P3S – Política de Utilização Aceitável: reforça as expectativas de comportamento abordadas na formação

10.1.3. P4S – Política de Controlo de Acessos: assegura que os utilizadores compreendem a importância da segurança dos acessos

10.1.4. P7S – Política de Admissão e Cessação: integra a formação no processo de entrada

10.1.5. P30S – Política de Resposta a Incidentes (P30): assegura que o pessoal sabe como notificar incidentes de forma imediata e correta

11. Normas e quadros de referência

11.1. ISO/IEC 27001

11.1.1. Cláusula 7.3 – Exige que as organizações assegurem que o pessoal está consciente das suas responsabilidades e dos impactos na segurança

11.2. ISO/IEC 27002

11.2.1. Controlo 6.3 – Detalha as expectativas relativas ao âmbito e à realização da formação em segurança

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Exige formação de sensibilização para utilizadores com acesso ao sistema

11.3.2. AT-4 – Abrange a formação específica para a função e as consequências do incumprimento

11.4. RGPD da UE

11.4.1. Artigo 32 – Exige medidas de segurança, incluindo a formação do pessoal, para proteger dados pessoais

11.4.2. Artigo 39 – Exige que os EPD supervisionem a sensibilização e a formação, quando aplicável

11.5. Diretiva NIS2 da UE

11.5.1. Artigo 21(2)(i) – Exige programas contínuos de sensibilização e formação em cibersegurança

11.6. DORA da UE

11.6.1. Artigo 13 – Exige que as entidades financeiras implementem ações de educação e formação para todo o pessoal com responsabilidades relacionadas com as TIC

11.7. COBIT 2019

11.7.1. BAI08 – Gerir Conhecimento: assegura que o pessoal é competente e devidamente formado

11.7.2. DSS05 – Gerir Serviços de Segurança: enfatiza a sensibilização como um controlo de proteção essencial