					Insira aqui a designação da entidade jurídica registada							
Número do documento: P08					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 7.3, Controlo 6.3 do Anexo A	Estabelece os requisitos de sensibilização e formação abrangidos por esta política
ISO/IEC 27002:2022	Controlo 6	Suporta formação de sensibilização adequada e baseada na função
NIST SP 800-53 Rev.5	AT-1 a AT-5	Alinha-se com política e procedimentos, formação de sensibilização, formação específica por função, registos de formação e contacto com grupos de segurança
RGPD da UE	Artigos 32, 39; Considerando 78	Exige formação para intervenientes no tratamento de dados pessoais e sensibilização geral dos trabalhadores
Diretiva NIS2 da UE	Artigos 21(2)(a, b), 21(3)	Exige políticas de análise de riscos e formação em segurança, bem como iniciativas de sensibilização
DORA da UE	Artigos 5, 8, 13	Exige sensibilização e formação em gestão do risco das TIC como parte dos controlos de resiliência
COBIT 2019	APO07, DSS05, MEA	Reforça a sensibilização da força de trabalho, a formação dos utilizadores e a monitorização do cumprimento

1. Finalidade

1.1 Esta política estabelece o quadro formal para assegurar que todo o pessoal conhece as suas responsabilidades em matéria de segurança da informação e recebe a formação necessária para proteger a Confidencialidade, Integridade e Disponibilidade dos ativos de informação.

1.2 Esta política suporta a Cláusula 7.3 e o Controlo 6.3 do Anexo A da ISO/IEC 27001, exigindo um programa estruturado de sensibilização e formação, baseado no risco e adaptado às funções organizacionais e à evolução das ameaças.

1.3 A política contribui para a redução de vulnerabilidades relacionadas com o fator humano, para a promoção de comportamentos conscientes em matéria de segurança e para o reforço contínuo de práticas seguras em conformidade com requisitos regulamentares e contratuais.

2. Âmbito

2.1 Esta política aplica-se a todos os indivíduos internos e externos com acesso aos sistemas de informação, dados ou instalações da organização, incluindo:

2.1.1 Trabalhadores (a tempo inteiro, a tempo parcial, temporários)

2.1.2 Prestadores de serviços, consultores, fornecedores e estagiários

2.1.3 Terceiros com acesso lógico ou físico ao abrigo de acordos de serviço

2.2 O âmbito inclui:

2.2.1 Formação inicial de sensibilização para a segurança no processo de integração

2.2.2 Formação específica por função (por exemplo, programadores, pessoal da área financeira, utilizadores com privilégios elevados)

2.2.3 Formação de reciclagem periódica e campanhas de sensibilização

2.2.4 Formação ad hoc em resposta a incidentes ou a novas ameaças

2.3 Os métodos de disponibilização da formação abrangidos por esta política incluem e-learning, briefings presenciais, simulações, testes de conhecimentos, cartazes, boletins informativos de segurança e confirmações obrigatórias.

3. Objetivos

3.1 Assegurar que todo o pessoal compreende as suas responsabilidades na salvaguarda dos ativos da organização e no cumprimento das políticas de segurança.

3.2 Disponibilizar formação de sensibilização contínua e mensurável, alinhada com a exposição ao risco em função do perfil de cada função.

3.3 Integrar comportamentos seguros nas operações diárias, reforçando práticas como a utilização segura de palavras-passe, a notificação de incidentes e a proteção contra phishing.

3.4 Assegurar o cumprimento regulamentar e a capacidade de demonstrar conformidade em auditoria relativamente à formação obrigatória em segurança da informação em diferentes setores e jurisdições.

3.5 Reduzir incidentes de segurança resultantes de negligência, falta de sensibilização ou fraco discernimento através do condicionamento comportamental e do reforço contínuo.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova a estratégia de formação em segurança da informação da organização e assegura que esta dispõe de recursos adequados e está integrada nas prioridades da organização.

4.1.2 Monitoriza o cumprimento ao nível da gestão e assegura a aplicação da política em todos os departamentos.

4.2 Diretor de Segurança da Informação / Gestor do SGSI

4.2.1 É responsável por esta política e define o quadro de sensibilização e formação em função do risco, da conformidade e das necessidades do negócio.

4.2.2 Supervisiona a conceção, disponibilização, acompanhamento e revisão de todas as iniciativas de formação em segurança.

4.2.3 Assegura que a formação é atualizada periodicamente e reflete a evolução das ameaças e das tecnologias emergentes.

[... 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 Frequência de revisão

9.1.1 Esta política e o programa de formação associado devem ser revistos:

9.1.1.1 Anualmente, ou

9.1.1.2 Após incidentes graves envolvendo erro humano ou ameaça interna

9.1.1.3 Aquando da introdução de novas tecnologias ou ameaças significativas

9.1.1.4 Em resposta a alterações nas obrigações legais, contratuais ou de certificação

9.2 Processo de revisão

9.2.1 A revisão deve ser conduzida pelo Diretor de Segurança da Informação em coordenação com:

9.2.1.1 Os departamentos de Recursos Humanos e Formação

9.2.1.2 O Encarregado da Proteção de Dados e a função Jurídica

9.2.1.3 As funções de Segurança de TI e Risco Operacional

9.2.2 Todas as atualizações devem ser:

9.2.2.1 Aprovadas pelo Comité de Direção do SGSI

9.2.2.2 Sujeitas a controlo de versões e documentadas no Registo de Documentos do SGSI

9.2.2.3 Comunicadas aos utilizadores se alterações materiais afetarem o âmbito da formação ou as responsabilidades

9.3 Governação da atualização de conteúdos

9.3.1 Os módulos de formação e os materiais de sensibilização devem ser revistos a cada 12 meses para assegurar:

9.3.1.1 Relevância para o panorama de ameaças

9.3.1.2 Rigor regulamentar

9.3.1.3 Compatibilidade de formato (por exemplo, acessibilidade, localização)

9.3.2 O conteúdo desatualizado ou suscetível de induzir em erro deve ser retirado imediatamente e substituído por alternativas aprovadas.

10. Políticas relacionadas e ligações

10.1 Esta política é suportada por e suporta a aplicação das seguintes políticas:

10.1.1 P01 – Política de Segurança da Informação: Estabelece a sensibilização para a segurança como um controlo fundamental no SGSI da organização.

10.1.2 P03 – Política de Utilização Aceitável: Exige a confirmação do utilizador durante a formação e clarifica responsabilidades associadas à utilização diária da tecnologia.

10.1.3 P07 – Política de Admissão e Cessação: Assegura que a formação é integrada no momento de entrada e acompanhada ao longo da relação laboral.

10.1.4 P06 – Política de Gestão de Riscos: Liga a formação centrada no fator humano à modelação de ameaças e às estratégias de redução do risco residual.

10.1.5 P33 – Política de Monitorização de Auditoria e Conformidade: Valida que os controlos de sensibilização são operacionais, mensuráveis e eficazes durante as auditorias.

10.2 Em conjunto, estas políticas formam um quadro abrangente de controlos comportamentais que integra sensibilização, responsabilização e reforço cultural.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 7.3 – Sensibilização: Exige que as organizações assegurem que os trabalhadores conhecem as políticas de segurança da informação e as suas responsabilidades. Esta política operacionaliza esse requisito através de integração estruturada, formação periódica e participação mensurável em campanhas.

11.1.2 Controlo 6.3 do Anexo A – Sensibilização, educação e formação em segurança da informação: Totalmente tratado através de programas de formação iniciais, baseados em funções e contínuos, adaptados aos perfis de risco dos utilizadores.

11.2 ISO/IEC 27002:2022 – Controlo 6

11.2.1 Suporta o desenvolvimento e a disponibilização de formação de sensibilização adequada às funções profissionais, com ênfase no reforço de comportamentos seguros e em atualizações periódicas baseadas em informações sobre ameaças e feedback de auditoria.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 a AT-5 (família Awareness and Training): Esta política alinha-se com o AT-1 (Política e Procedimentos), AT-2 (Formação de Sensibilização), AT-3 (Formação Baseada em Funções), AT-4 (Registos de Formação em Segurança) e AT-5 (Contacto com Grupos de Segurança).

11.3.2 IA-5, AC-2: Reforça a responsabilidade do utilizador pela autenticação segura e pela utilização aceitável, centrais para os resultados comportamentais dos programas de sensibilização.

11.3.3 IR-1 a IR-8: A preparação para a resposta a incidentes é reforçada através de campanhas de sensibilização direcionadas e simulações.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 32 – Segurança do Tratamento: Exige que o pessoal que trata dados pessoais receba formação para reconhecer, prevenir e reportar riscos para os dados pessoais. Esta política assegura que os intervenientes no tratamento de dados e todas as funções relevantes recebem formação em conformidade.

11.4.2 Artigo 39 – Tarefas do Encarregado da Proteção de Dados: Inclui a promoção da sensibilização e a formação do pessoal envolvido em operações de tratamento.

11.4.3 Considerando 78: Incentiva medidas adequadas de sensibilização para assegurar práticas de segurança robustas e o cumprimento das políticas.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(a, b): Exige que as entidades adotem políticas de análise de riscos e de formação em segurança para todo o pessoal relevante. Esta política cumpre esse requisito ao estabelecer processos contínuos de formação adaptados à função.

11.5.2 Artigo 21(3): Incentiva a promoção da sensibilização para os riscos de cibersegurança junto da gestão e do pessoal através de iniciativas de sensibilização e simulações.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 13 – Estratégia de resiliência operacional digital: Exige que a sensibilização e a formação sobre o risco das TIC façam parte do modelo de governação. Esta política assegura que o risco humano é tratado através de formação contínua e simulação de ameaças.

11.6.2 Artigos 5 e 8: Salientam a importância de quadros de controlo interno, dos quais a sensibilização e a formação são componentes fundamentais para a resiliência das TIC e a higiene cibernética.

11.7 COBIT 2019

11.7.1 APO07 – APO07 Gerir recursos humanos: Reforça a necessidade de desenvolver a sensibilização para as responsabilidades de segurança e de a integrar na gestão da força de trabalho.

11.7.2 DSS05 – DSS05 Gerir Serviços de Segurança: Estabelece controlos sobre a formação dos utilizadores e a notificação de incidentes, ambos abrangidos por esta política.

11.7.3 MEA03 – Monitorizar, Avaliar e Analisar o Cumprimento: Exige a revisão da eficácia do comportamento dos utilizadores e do cumprimento da política, implementada aqui através de testes de phishing, questionários e métricas de campanhas de sensibilização.