					Insira aqui a designação da entidade jurídica registada							
Número do documento: P01					Título do documento: **Política de 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**

1. Finalidade

1.1 Esta política define o compromisso global da organização com a segurança da informação, mediante o estabelecimento de um Sistema de Gestão da Segurança da Informação (SGSI) formal.

1.2 Estabelece a orientação estratégica e os requisitos fundamentais para proteger a Confidencialidade, Integridade e Disponibilidade, bem como a resiliência, de todos os ativos de informação em ambientes físicos, digitais e na nuvem.

1.3 Esta política cumpre as Cláusulas 5.1 e 5.2 da ISO/IEC 27001:2022, ao expressar a intenção da liderança, o compromisso da Alta Direção e o alinhamento das atividades de segurança com os objetivos organizacionais.

1.4 Constitui a referência normativa para todas as políticas subordinadas, normas e procedimentos no âmbito do SGSI e é essencial para sustentar um ambiente de segurança baseado no risco, orientado para a conformidade e para a melhoria contínua.

2. Âmbito

2.1 Esta política aplica-se a todos os indivíduos, ativos e processos definidos no âmbito do SGSI, incluindo:

2.1.1 Todas as unidades de negócio, departamentos, subsidiárias e filiais

2.1.2 Trabalhadores e prestadores de serviços, pessoal temporário, consultores e prestadores de serviços terceiros

2.1.3 Todos os dados, sistemas de informação, aplicações, infraestruturas e canais de comunicação

2.1.4 Todos os ambientes físicos, na nuvem, remotos e híbridos onde os dados da organização sejam tratados ou acedidos

2.2 A política é vinculativa para todas as entidades que tratem informação da organização e aplica-se a todas as fases do ciclo de vida da informação, desde a criação e transmissão até ao armazenamento e eliminação.

2.3 Quaisquer exclusões ou limitações a este âmbito devem ser documentadas na declaração de âmbito do SGSI e justificadas com aprovação formal da Alta Direção.

3. Objetivos

3.1 Estabelecer um SGSI alinhado com a ISO/IEC 27001:2022 e capaz de suportar a tomada de decisão baseada no risco em toda a organização.

3.2 Assegurar que os princípios de segurança da Confidencialidade, Integridade e Disponibilidade estão incorporados em todas as atividades, sistemas e parcerias da organização.

3.3 Assegurar a conformidade regulamentar e contratual através da definição de objetivos mensuráveis de segurança, orientados por políticas, e da sua integração nas operações de negócio.

3.4 Minimizar a probabilidade e o impacto de incidentes de segurança da informação através de controlos preventivos, detetivos e corretivos eficazes.

3.5 Promover a melhoria contínua da maturidade da segurança da informação, através de indicadores de desempenho definidos, resultados de auditoria e revisões pela gestão do SGSI.

3.6 Promover uma cultura de responsabilização, sensibilização e resiliência em que as responsabilidades de segurança sejam compreendidas e executadas por todo o pessoal.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova e ratifica a Política de Segurança da Informação e o quadro do SGSI.

4.1.2 Assegura o alinhamento entre os objetivos de segurança e a estratégia de negócio.

4.1.3 Dá o exemplo e promove uma cultura sólida de segurança da informação.

4.1.4 Revê e aprova alterações significativas ao âmbito do SGSI, ao tratamento de riscos e à estrutura de governação.

4.2 Diretor de Segurança da Informação (CISO) / Gestor do SGSI

4.2.1 É responsável pelo SGSI e mantém esta política em conformidade com a ISO/IEC 27001.

4.2.2 Lidera os processos de avaliação de riscos, implementação de controlos e melhoria contínua.

4.2.3 Assegura a coordenação transversal dos esforços de segurança e supervisiona as políticas subordinadas.

4.2.4 Reporta à liderança executiva o estado do SGSI, incidentes, resultados de auditoria e métricas.

4.2.5 Assegura que as revisões e atualizações da política são realizadas em conformidade com a Secção 9 deste documento.

[... 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 deve ser revista pelo menos anualmente ou sempre que ocorra qualquer um dos seguintes fatores desencadeantes:

9.1.1.1 Alterações significativas às obrigações legais, regulamentares ou contratuais

9.1.1.2 Alterações materiais ao perfil de risco da organização

9.1.1.3 Resultados de auditorias internas ou externas

9.1.1.4 Incidentes graves ou falhas de controlo

9.2 Autoridade e processo de revisão

9.2.1 O Diretor de Segurança da Informação ou o Gestor do SGSI designado deve liderar o processo de revisão.

9.2.2 Os contributos para a revisão devem incluir:

9.2.2.1 Resultados de auditoria interna

9.2.2.2 Tendências das avaliações de risco

9.2.2.3 Alterações aos processos de negócio e à tecnologia

9.2.2.4 Desempenho face aos KPIs e limiares de risco

9.2.3 Todas as atualizações devem:

9.2.3.1 Estar sujeitas a controlo de versões e ser documentadas

9.2.3.2 Ser aprovadas pela Alta Direção

9.2.3.3 Ser distribuídas a todas as partes afetadas através dos canais oficiais de comunicação

9.2.3.4 Desencadear as atualizações necessárias à documentação subordinada e à formação

10. Políticas relacionadas e articulações

10.1 Esta política base está diretamente articulada com as seguintes políticas e quadros de segurança da organização:

10.1.1 P2 – Política de Papéis e Responsabilidades de Governação: define a estrutura de governação e a hierarquia de autoridade referidas neste documento.

10.1.2 P3 – Política de Utilização Aceitável: estabelece os requisitos de conduta e de utilização aceitável dos ativos de informação.

10.1.3 P4 – Política de Controlo de Acessos: operacionaliza os controlos relacionados com acessos decorrentes desta política de nível superior.

10.1.4 P6 – Política de Gestão de Riscos: fornece o contexto baseado no risco para a seleção de controlos e a aceitação de riscos residuais.

10.1.5 P33 – Política de Monitorização, Auditoria e Conformidade: detalha a forma como os mecanismos internos de garantia validam a aplicação da política.

10.2 Estas interdependências asseguram alinhamento abrangente e rastreabilidade em todo o SGSI e suportam uma governação unificada do risco e da conformidade.

11. Normas e quadros de referência

11.1 Esta Política de Segurança da Informação está formalmente alinhada com as seguintes normas e quadros, de modo a assegurar a conformidade integral, a capacidade de demonstrar conformidade em auditoria e a robustez perante o escrutínio regulamentar:

11.2 ISO/IEC 27001

11.2.1 Cláusula 5.1 – Liderança e compromisso: esta política demonstra o compromisso da Alta Direção com a segurança da informação e define responsabilidades e afetação de recursos para o SGSI.

11.2.2 Cláusula 5.2 – Política de Segurança da Informação: este documento constitui a política formal de segurança da organização, alinhada com os objetivos de segurança declarados, a estratégia de negócio e os requisitos da ISO/IEC 27001.

11.2.3 Cláusula 6.1 – Ações para tratar riscos e oportunidades: a abordagem baseada no risco refletida nesta política assegura que os recursos de segurança são aplicados de forma proporcional às ameaças.

11.2.4 Cláusula 9.2 – Auditoria Interna e Cláusula 10 – Melhoria: esta política está integrada no ciclo de melhoria contínua da organização e sujeita a validação por auditoria interna.

11.2.5 ISO/IEC 27002:2022 – Controlo 5.1: especifica orientações para estabelecer e manter políticas de segurança. Esta política reflete as recomendações da ISO/IEC 27002 relativas à documentação hierárquica, aos ciclos de revisão e à aplicabilidade.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Política e Procedimentos de Planeamento da Segurança): esta política satisfaz o requisito de desenvolver, divulgar e rever uma política formal de segurança da informação aplicável a toda a organização.

11.3.2 PM-1 a PM-5: aborda a governação ao nível do programa, incluindo papéis de segurança da informação, afetação de recursos, estratégia de risco e integração do planeamento de segurança nas operações empresariais.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 5(2): aplica o princípio da responsabilização. Esta política define responsáveis e ações de aplicação rastreáveis.

11.4.2 Artigo 24: exige a implementação de medidas técnicas e organizativas, incluindo políticas alinhadas com o risco.

11.4.3 Artigo 32: suporta a implementação de medidas adequadas para assegurar a segurança dos dados pessoais ao longo do respetivo ciclo de vida.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(a): exige que as entidades implementem uma política de segurança documentada que aborde a gestão de riscos e a governação. Esta política cumpre esse requisito e apoia uma preparação mais abrangente em cibersegurança e a proteção de infraestruturas críticas.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 5(2): exige um quadro de controlo interno documentado para a gestão do risco das TIC. Esta política apoia a conformidade no setor financeiro através da atribuição de papéis, controlos e funções de supervisão alinhados com as expectativas de governação do DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Definição do quadro de governação: esta política apoia a governação empresarial ao definir os papéis do SGSI, os compromissos da liderança e os objetivos estratégicos.

11.7.2 APO01 – Quadro de gestão: apoia o estabelecimento e a operação de um SGSI estruturado.

11.7.3 APO12 – Gestão de riscos: fornece a base para a governação dos riscos de segurança da informação.

11.7.4 MEA01/MEA03 – Monitorização, Avaliação e Análise: reforça a avaliação contínua do desempenho e a monitorização do controlo interno através da aplicação da política e da verificação da conformidade.