					Insira aqui a designação da entidade jurídica registada							
Número do documento: P06					Título do documento: **Política de Gestão de Riscos**							
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	Cláusulas 6.1, 8.32, 10	Núcleo da identificação e gestão de riscos, integração na gestão de alterações, melhoria contínua
ISO/IEC 27005:2024	Metodologia completa do ciclo de vida do risco	Processo completo de gestão de riscos em conformidade com a norma
ISO 31000:2018	Princípios e quadro de gestão de riscos	Princípios de gestão de riscos adotados no quadro
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Orientação e estrutura para avaliações de risco, governação de riscos por níveis
RGPD da UE	Artigos 24, 25, 32	Processos e controlos de risco para proteção de dados
Diretiva NIS2 da UE	Artigo 21(2)(a–d)	Obrigações de avaliação de risco e de segurança
DORA da UE	Artigos 5, 6	Gestão do risco das TIC e resiliência operacional
COBIT 2019	APO12, MEA	Estrutura e supervisão da gestão de riscos

1. Finalidade

1.1 Esta política estabelece um quadro unificado e formalizado para identificar, analisar, avaliar, tratar, monitorizar e rever os riscos de segurança da informação em toda a organização.

1.2 Assegura a aplicação consistente de princípios baseados no risco que protegem a Confidencialidade, Integridade e Disponibilidade dos ativos de informação, em conformidade com a Cláusula 6.1 da ISO/IEC 27001:2022 e com a ISO 31000:2018.

1.3 Esta política integra a gestão dos riscos de segurança da informação nos processos de tomada de decisão da organização, de modo a cumprir os objetivos estratégicos internos e os requisitos regulatórios externos.

2. Âmbito

2.1 Esta política aplica-se a todas as unidades organizacionais, processos de negócio, sistemas, pessoal e relações com terceiros envolvidos no tratamento, desenvolvimento, armazenamento ou gestão de ativos de informação.

2.2 O âmbito estende-se a ativos físicos, digitais e alojados na nuvem, incluindo dados estruturados e não estruturados, aplicações, infraestruturas, redes e serviços.

2.3 Abrange riscos de segurança da informação aos níveis estratégico, operacional, de projeto e técnico, sendo obrigatória para todos os trabalhadores e prestadores de serviços envolvidos em atividades do SGSI.

2.4 A gestão de riscos deve ser aplicada aos seguintes cenários:

2.4.1 Implementação de novo projeto ou sistema

2.4.1.1 Alterações significativas (por exemplo, arquitetura, titularidade, processos)

2.4.1.2 Integração de fornecedores e celebração de acordos com terceiros

2.4.1.3 Resposta a incidentes e revisão pós-incidente

2.4.1.4 Revisões periódicas de risco organizacional ou auditorias

3. Objetivos

3.1 Estabelecer e operacionalizar um processo de gestão de riscos repetível e aplicável a toda a organização, com base nas metodologias ISO/IEC 27005 e ISO 31000.

3.2 Assegurar que os riscos são identificados, analisados, avaliados e tratados através de métodos estruturados e rastreáveis, incluindo a definição da titularidade do risco e das ligações aos controlos.

3.3 Manter um Registo de Riscos centralizado e sujeito a controlo de versões, bem como um plano de tratamento de riscos, refletindo o estado atual do risco, a cobertura de controlos e o progresso da mitigação.

3.4 Alinhar as decisões de risco com o apetite ao risco documentado e com os níveis de tolerância definidos, permitindo decisões de governação informadas quanto à aceitação, mitigação, transferência ou evitação do risco.

3.5 Monitorizar continuamente as tendências de risco e assegurar a eficácia dos tratamentos de risco, permitindo ajustes proativos com base na evolução das ameaças ou em alterações do negócio.

4. Papéis e responsabilidades

4.1 Alta Direção / Conselho de Administração

4.1.1 Aprova o quadro de gestão de riscos e define o apetite ao risco aceitável e os limiares de tolerância.

4.1.2 Autoriza estratégias de tratamento de riscos para riscos residuais que excedam a tolerância.

4.1.3 Aloca recursos e assegura supervisão para o funcionamento eficaz do programa de gestão de riscos.

4.2 Gestor do SGSI / Responsável pelo Risco

4.2.1 É responsável por esta política e assegura o seu alinhamento com as normas ISO/IEC 27001 e 27005.

4.2.2 Lidera o processo de avaliação de risco organizacional e mantém o Registo de Riscos e o plano de tratamento de riscos.

4.2.3 Assegura revisões periódicas e o escalonamento dos principais riscos para a direção executiva ou para o Comité de Direção do SGSI.

[... 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 Esta política e o respetivo quadro devem ser revistos anualmente, ou:

9.1.1 Após um evento de risco relevante ou incidente de segurança

9.1.2 Na sequência de alteração organizacional ou técnica significativa

9.1.3 Em resposta a conclusões de auditoria ou a novos requisitos regulatórios

9.2 O Gestor do SGSI, o Responsável pelo Risco e a equipa de Conformidade são conjuntamente responsáveis por:

9.2.1 Iniciar o ciclo de revisão

9.2.2 Recolher contributos das unidades de negócio

9.2.3 Rever procedimentos e limiares, conforme necessário

9.3 Todas as revisões devem ser:

9.3.1 Sujeitas a controlo de versões e registadas

9.3.2 Aprovadas pela Alta Direção

9.3.3 Comunicadas às partes interessadas

9.3.4 Retidas no repositório de auditoria por um período mínimo de 5 anos

10. Políticas relacionadas e ligações

10.1 Esta política é interdependente das seguintes políticas de segurança da informação:

10.1.1 P1 – Política de Segurança da Informação: Estabelece o modelo global de governação da segurança no qual esta política de risco opera.

10.1.2 P2 – Política de Papéis e Responsabilidades de Governação: Define os responsáveis e os níveis de governação referidos na matriz de escalonamento de risco.

10.1.3 P5 – P05 Política de Gestão de Alterações: Desencadeia a reavaliação de riscos para alterações de infraestrutura e organizacionais.

10.1.4 P13 – Política de Classificação e Rotulagem da Informação: Apoia a avaliação de impacto durante a identificação de riscos.

10.1.5 P33 – Política de Monitorização de Auditoria e Conformidade: Valida o cumprimento da política, incluindo a completude do Registo de Riscos e a evidência dos tratamentos.

11. Normas e referenciais aplicáveis

11.1 Esta política está explicitamente alinhada com as seguintes normas e referenciais, para assegurar o cumprimento das melhores práticas internacionais e das expectativas regulatórias aplicáveis à gestão de riscos de segurança da informação:

11.2 ISO/IEC 27001:

11.2.1 Cláusula 6.1: Estabelece os requisitos para a identificação de riscos e oportunidades, incluindo o ciclo de vida completo das avaliações e tratamentos do risco de segurança da informação. Esta política operacionaliza a Cláusula 6.1.2 e a Cláusula 6.1.3 através de um quadro estruturado que impõe a identificação, análise, avaliação, tratamento e aceitação do risco residual de forma documentada.

11.2.2 Cláusula 8.32: A integração da abordagem baseada no risco nos processos de gestão de alterações assegura que todas as alterações organizacionais significativas desencadeiam reavaliações formais do risco.

11.2.3 Cláusula 10: A melhoria contínua está incorporada através de revisões regulares da política, análise de tendências de risco e atualizações da SoA orientadas por informação de risco.

11.3 ISO/IEC 27005:

11.3.1 Fornece orientação especializada e detalhada sobre a gestão de riscos de segurança da informação. Esta política implementa o modelo completo do processo de risco da ISO/IEC 27005: estabelecimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos, aceitação do risco, comunicação do risco, monitorização de riscos e revisão.

11.4 ISO 31000:

11.4.1 Esta política integra princípios da ISO 31000, tais como o compromisso da liderança, a integração na tomada de decisão e a melhoria contínua. Assegura que a gestão de riscos está incorporada na cultura e nas operações da organização.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Está alinhada com o guia do NIST para a realização de avaliações de risco, incluindo identificação de ameaças, análise de vulnerabilidades, estimativa da probabilidade e determinação do impacto. A estrutura desta política reflete as etapas de avaliação de risco definidas pelo NIST e adapta-as tanto aos processos técnicos como aos processos de negócio.

11.6 NIST SP 800-39:

11.6.1 Suporta a governação de riscos ao nível organizacional, enfatizando a gestão de riscos pelos níveis organizacional, missão/processo de negócio e sistema de informação. A política assegura que a titularidade do risco está claramente definida em todos os níveis e inclui estratégias de tratamento ao nível organizacional.

11.7 RGPD da UE:

11.7.1 Artigo 24: Exige a implementação de medidas técnicas e organizativas adequadas para assegurar que os riscos de proteção de dados são devidamente geridos — tratado através do processo estruturado de risco definido nesta política.

11.7.2 Artigo 25: A "proteção de dados desde a conceção e por defeito" está alinhada com a integração do tratamento de riscos na conceção de sistemas e processos.

11.7.3 Artigo 32: Impõe uma abordagem baseada no risco às medidas de segurança — cumprida através de avaliações de risco baseadas no impacto e da seleção de controlos.

11.8 Diretiva NIS2 da UE:

11.8.1 Artigo 21(2)(a–d): Exige que as entidades realizem avaliações de risco, implementem políticas sobre análise de riscos e assegurem medidas de segurança proporcionais. Esta política cumpre estas obrigações através da aplicação contínua do ciclo de vida do risco e de uma governação documentada.

11.9 DORA da UE:

11.9.1 Artigo 5: Exige um quadro documentado de gestão do risco das TIC — integralmente abrangido pela arquitetura desta política, incluindo o mapeamento para a SoA e os KRI.

11.9.2 Artigo 6: Exige a integração da gestão de riscos nas estratégias de resiliência operacional, tratada através de matrizes de escalonamento e do acompanhamento de ativos críticos.

11.10 COBIT 2019:

11.10.1 APO12 – Gerir o Risco: Corresponde diretamente ao estabelecimento, pela organização, de uma abordagem estruturada de gestão de riscos, com atribuição de papéis, acompanhamento de tratamentos e responsabilização ao nível do Conselho de Administração.

11.10.2 MEA01 – Monitorizar, Avaliar e Analisar o Desempenho e a Conformidade: Refletido no enfoque desta política na análise de tendências, na monitorização de KRI e na integração de feedback de auditoria em ciclos de melhoria contínua.