					Insira aqui a designação da entidade jurídica registada							
Número do documento: P02					Título do documento: **Política de Papéis e Responsabilidades de Governação**							
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 aplicáveis

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 5.3; Controlo 5 do Anexo A	
ISO/IEC 27002:2022	Controlo 5	
NIST SP 800-53 Rev.5	PL-1 a PL-4, PM-1 a PM-13	
RGPD da UE	Artigos 5(1)(f), 24, 37	
Diretiva NIS2 da UE	Artigo 21(2)(a)	
DORA da UE	Artigo 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Finalidade

1.1 Esta política define o modelo de governação, os papéis organizacionais e as responsabilidades necessários para operar um Sistema de Gestão da Segurança da Informação (SGSI) eficaz.

1.2 Estabelece linhas claras de responsabilização, autoridade para a tomada de decisão e canais de escalonamento, de forma a assegurar que a segurança da informação está integrada em todos os níveis da organização e alinhada com os objetivos estratégicos do negócio.

1.3 A presente política implementa os requisitos da Cláusula 5.3 e do Controlo A.5.2 da ISO/IEC 27001:2022, assegurando que as responsabilidades pelas atividades relacionadas com a segurança são claramente atribuídas, documentadas, comunicadas e revistas periodicamente.

1.4 Esta política estabelece igualmente uma base para a governação integrada com outras disciplinas, como a gestão do risco, a conformidade, as operações de TI e as funções jurídicas.

2. Âmbito

2.1 Esta política aplica-se a todos os indivíduos e entidades envolvidos na governação, operação e supervisão da segurança da informação no âmbito do SGSI. Isto inclui:

2.1.1 Liderança executiva, direção de topo e membros do conselho de administração

2.1.2 Gestores do SGSI, Diretores de Segurança da Informação e Proprietários de controlos

2.1.3 Proprietários de processos e de ativos

2.1.4 Contratados e prestadores de serviços terceiros com responsabilidades de segurança delegadas

2.2 Abrange tanto funções internas como funções externalizadas (por exemplo, Centro de Operações de Segurança externalizado, administradores de plataformas na nuvem), quando os papéis de governação sejam formalmente atribuídos ou definidos contratualmente.

2.3 A política aplica-se igualmente a unidades organizacionais, departamentos e equipas de projeto que gerem ou influenciem ativos, sistemas ou serviços relevantes para a segurança.

3. Objetivos

3.1 Assegurar que os papéis e responsabilidades de segurança da informação são formalmente definidos, atribuídos, comunicados e documentados.

3.2 Manter um modelo de governação que assegure a segregação de funções, elimine conflitos de interesses e permita o escalonamento de questões de segurança não resolvidas.

3.3 Assegurar que a responsabilização e a autoridade para decisões de segurança são distribuídas em alinhamento com o impacto no negócio e com a estrutura organizacional.

3.4 Estabelecer um quadro para a gestão de delegações, alterações de funções e revisão das responsabilidades atribuídas.

3.5 Proporcionar garantia às partes interessadas — incluindo reguladores, auditores e clientes — de que a segurança da informação é governada de forma eficaz e em conformidade com as normas aplicáveis.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Assegura a supervisão estratégica, afeta recursos e garante o alinhamento entre os objetivos do SGSI e os objetivos do negócio.

4.1.2 Aprova a documentação principal do SGSI, incluindo a Política de Segurança da Informação, os planos de tratamento do risco e as decisões de remediação resultantes de auditorias.

4.1.3 Participa nas revisões pela gestão do SGSI e escalona para o Conselho de Administração as decisões que exijam aprovação a esse nível.

4.1.4 Promove uma cultura de segurança e incentiva o cumprimento organizacional dos princípios de governação da segurança.

4.2 Comité de Direção de Segurança da Informação

4.2.1 Atua como órgão transversal de governação para a supervisão do SGSI.

4.2.2 Revê a postura de risco, o desempenho dos controlos, as constatações de auditoria e as iniciativas estratégicas de segurança.

4.2.3 Facilita a coordenação entre departamentos (por exemplo, TI, Jurídico, Recursos Humanos, Risco, Conformidade, Operações).

4.2.4 Aprova limiares de escalonamento, dotações orçamentais e alterações às políticas que exijam contributo executivo.

[... 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 Calendário de revisão

9.1.1 Esta política deve ser revista pelo menos anualmente ou sempre que ocorra qualquer um dos seguintes eventos:

9.1.1.1 Alterações à estrutura organizacional ou à equipa executiva

9.1.1.2 Expansão ou redefinição do âmbito do SGSI

9.1.1.3 Alterações regulatórias que afetem a atribuição de funções ou a supervisão

9.1.1.4 Constatações de auditoria significativas ou incidentes que envolvam falhas de governação

9.2 Processo de revisão e aprovação

9.2.1 O Gestor do SGSI deve iniciar e liderar o processo de revisão, incluindo a recolha de contributos das partes interessadas e do feedback de auditoria.

9.2.2 As atualizações propostas devem ser revistas pelo Comité de Direção de Segurança da Informação e formalmente aprovadas pela Alta Direção.

9.2.3 Cada versão deve ser acompanhada no Registo de Documentos do SGSI e incluir os seguintes metadados:

9.2.3.1 ID e título da política

9.2.3.2 Número da versão e resumo das alterações

9.2.3.3 Data de entrada em vigor e data da próxima revisão

9.2.3.4 Proprietário e aprovador da política

9.2.3.5 Nível de classificação do documento

9.2.3.6 Histórico de retenção e arquivo

10. Políticas relacionadas e ligações

10.1 Esta política deve ser interpretada em conjunto com as seguintes políticas:

10.1.1 P1 – Política de Segurança da Informação: Estabelece o programa global de segurança e define as responsabilidades da liderança na aprovação da política e na supervisão estratégica.

10.1.2 P5 – Política de Gestão de Alterações: Assegura que as alterações às estruturas de governação, funções ou responsabilidades estão sujeitas a aprovação documentada e revisão de risco.

10.1.3 P6 – Política de Gestão de Riscos: Identifica e trata riscos de governação decorrentes de conflitos de funções, deveres não atribuídos ou ausência de escalonamento.

10.1.4 P7 – Política de Admissão e Cessação: Aplica processos de atribuição e revogação de controlos durante alterações no ciclo de vida do pessoal.

10.1.5 P33 – Política de Monitorização de Auditoria e Conformidade: Suporta a revisão independente da eficácia da governação e define ações corretivas para casos de incumprimento.

10.2 Estas políticas suportam, em conjunto, um quadro de governação do SGSI unificado e aplicável.

11. Normas e quadros de referência

11.1 Esta política está alinhada com normas e quadros de referência globalmente reconhecidos para a governação da segurança da informação e a responsabilização por funções. Assegura a rastreabilidade face a requisitos regulatórios e de certificação e suporta uma estrutura de SGSI defensável.

11.2 ISO/IEC 27001

11.2.1 Cláusula 5.3 – Papéis, responsabilidades e autoridades organizacionais: Esta política cumpre o requisito de que as funções relevantes para a segurança da informação sejam claramente atribuídas, comunicadas e documentadas.

11.2.2 Cláusula 9.3 – Revisão pela gestão: Esta política impõe a supervisão executiva dos papéis e da governação do SGSI através de revisões trimestrais e anuais.

11.2.3 Controlo 5.2 do Anexo A – Papéis e responsabilidades em segurança da informação: Define funções nos níveis técnico, operacional e estratégico para assegurar a segregação de funções, a titularidade do risco e a responsabilização rastreável.

11.3 ISO/IEC 27002:2022 – Controlo 5

11.3.1 Fornece orientações de implementação para a atribuição de responsabilidades de segurança da informação em toda a organização. Esta política adota essas orientações ao definir tipos de funções, regras de delegação, procedimentos de escalonamento e mecanismos de revisão.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 a PL-4: Impõem a necessidade de documentação formal de planeamento, incluindo políticas que definam a governação e atribuam responsabilidades de segurança.

11.4.2 PM-1 (Plano do Programa de Segurança da Informação) e PM-2 (Responsável Sénior pela Segurança da Informação): Refletidos nesta política através da atribuição do Diretor de Segurança da Informação/Gestor do SGSI e de papéis formais de governação.

11.4.3 PM-5 a PM-13: Esta política satisfaz os requisitos de documentação de funções, papéis de risco à escala empresarial, supervisão da gestão da configuração e integração com funções de missão/negócio.

11.5 RGPD da UE (2016/679)

11.5.1 Artigo 5(1)(f): Exige que os dados pessoais sejam protegidos contra tratamento não autorizado ou ilícito. Esta política assegura que os indivíduos responsáveis pela proteção de dados são claramente designados e monitorizados.

11.5.2 Artigo 24: Exige medidas organizacionais adequadas, incluindo estruturas de governação.

11.5.3 Artigo 37: Exige a designação de um Encarregado da Proteção de Dados (EPD), o que deve refletir-se no quadro de governação e no registo de responsabilidades da organização.

11.6 Diretiva NIS2 da UE (2022/2555)

11.6.1 Artigo 21(2)(a): Determina que as entidades implementem políticas sobre análise de riscos e segurança dos sistemas de informação, incluindo responsabilidades específicas por função. Esta política define essas funções e os respetivos mecanismos de governação.

11.7 DORA da UE (2022/2554)

11.7.1 Artigo 5 – Quadro de governação e controlo interno: Exige a atribuição formal de responsabilidades de gestão do risco de TIC, papéis de tomada de decisão e canais de reporte. Esta política estabelece a base para a governação de papéis relacionados com a segurança em ambientes de TIC.

11.8 COBIT 2019

11.8.1 EDM01 – Definição do quadro de governação assegurada: Esta política assegura que o SGSI dispõe de uma estrutura de governação claramente definida e alinhada com as necessidades da organização.

11.8.2 EDM02 – Entrega de benefícios assegurada: Alinha atividades de segurança baseadas em funções com objetivos estratégicos e operacionais, assegurando responsabilização e resultados mensuráveis.

11.8.3 APO01 – Quadro de gestão de I&T gerido e APO12 – Risco gerido: Esta política suporta a gestão estruturada de funções de segurança da informação no âmbito de um quadro mais amplo de governação e risco de TI.

11.8.4 MEA01 – Monitorizar, Avaliar e Analisar o desempenho: Incorpora mecanismos de revisão para verificar que os papéis de governação são eficazes, atuais e aplicados.