					Insira aqui a designação da entidade jurídica registada							
Número do documento: P02S					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**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 5	
ISO/IEC 27002:2022	Controlos: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
RGPD da UE	Artigos 5(2), 32	

1. Finalidade

1.1 Esta política define a forma como as responsabilidades de governação da segurança da informação são atribuídas, delegadas e geridas na organização, de modo a assegurar o cumprimento integral da ISO/IEC 27001:2022 e de outras obrigações regulamentares.

1.2 Assegura a responsabilização a todos os níveis e apoia a eficácia operacional, identificando de forma clara quem é responsável por cada função relacionada com a segurança.

1.3 Esta política reforça a capacidade de demonstrar conformidade em auditoria e aumenta a confiança dos clientes, ao evidenciar uma governação formal da segurança, mesmo em organizações com recursos técnicos limitados ou com TI externalizadas.

2. Âmbito

2.1 Esta política aplica-se a todos os indivíduos que utilizem sistemas ou tratem dados da organização, incluindo:

2.1.1 Proprietários do negócio e diretores-gerais

2.1.2 Trabalhadores e prestadores de serviços

2.1.3 Prestadores externos de serviços de TI ou consultores

2.2 Abrange todos os sistemas, ambientes e serviços utilizados para processar, transmitir ou armazenar informação da organização ou de clientes, incluindo:

2.2.1 Infraestrutura de TI de escritório e dispositivos de trabalho remoto

2.2.2 Plataformas alojadas na nuvem e serviços de correio eletrónico

2.2.3 Registos físicos e unidades partilhadas

2.3 O âmbito inclui atividades internas e externalizadas que envolvam a governação da segurança da informação.

3. Objetivos

3.1 Estabelecer uma responsabilização clara por todos os deveres relacionados com a segurança, incluindo a gestão de políticas, o controlo de acessos, a resposta a incidentes e a monitorização.

3.2 Assegurar uma segregação eficaz de funções para reduzir conflitos de interesses ou riscos de fraude.

3.3 Assegurar que as tarefas e funções de segurança estão claramente documentadas e são revistas regularmente.

3.4 Permitir a tomada de decisões informadas, o escalonamento e a supervisão dos riscos de TI e de segurança.

3.5 Apoiar a certificação ISO/IEC 27001:2022 e reforçar a confiança de clientes, parceiros e auditores.

4. Papéis e responsabilidades

4.1 Diretor-Geral / Proprietário do negócio

4.1.1 É responsável, em última instância, pela implementação e supervisão desta política.

4.1.2 Aprova todos os papéis, responsabilidades e decisões de delegação em matéria de segurança.

4.1.3 Monitoriza o cumprimento e toma as decisões finais sobre exceções à política e escalonamentos.

4.2 Coordenador de Segurança Designado (se aplicável)

4.2.1 Pode ser um trabalhador ou um consultor de confiança.

4.2.2 Esta função pode ser assumida pelo Diretor-Geral ou por um prestador externo no contexto de microempresa.

4.2.3 Apoia a execução diária do controlo de acessos, da resposta a incidentes e de tarefas técnicas básicas de segurança.

4.2.4 Reporta diretamente ao Diretor-Geral quaisquer questões ou riscos de segurança.

[... 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 pelo Diretor-Geral a cada 12 meses para assegurar que continua a refletir as obrigações legais, as necessidades operacionais e os requisitos de certificação ISO/IEC 27001.

9.2 Revisões intercalares

9.2.1 Devem igualmente ocorrer revisões quando:

9.2.1.1 Existam alterações organizacionais significativas

9.2.1.2 Seja integrado um novo prestador

9.2.1.3 Ocorra um incidente de segurança grave

9.2.1.4 Regulamentos como o RGPD da UE, a Diretiva NIS2 da UE ou o Regulamento DORA da UE sejam atualizados

9.3 Controlo de versões e documentação

9.3.1 Todas as revisões devem incluir:

9.3.1.1 Data da revisão

9.3.1.2 Resumo de quaisquer alterações

9.3.1.3 Assinatura ou aprovação documentada pelo Diretor-Geral

9.3.1.4 Versões anteriores arquivadas para referência de auditoria

9.4 Comunicação de alterações

9.4.1 Todas as atualizações da política devem ser comunicadas prontamente ao pessoal e aos prestadores através de correio eletrónico, portais internos ou memorandos formais.

10. Políticas relacionadas e articulações

10.1 Esta política deve ser implementada em conjunto com as seguintes políticas PME, para garantir plena eficácia:

10.1.1 P4S – Política de controlo de acessos: Define como o acesso é concedido, gerido e revogado, estando diretamente ligada às funções atribuídas e à supervisão.

10.1.2 P8S – Política de sensibilização e formação em segurança da informação: Reforça as responsabilidades e expectativas específicas de cada função.

10.1.3 P17S – Política de proteção de dados e privacidade: Define os deveres legais ao abrigo do RGPD da UE, atribuídos aos papéis definidos nesta política de governação.

10.1.4 P30S – Política de resposta a incidentes: Exige responsabilidades definidas para a notificação, o escalonamento e a resolução de incidentes.

10.2 Em conjunto, estas políticas permitem uma aplicação coerente, responsabilização interna e conformidade externa.

11. Normas e referenciais aplicáveis

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.3 – Papéis, responsabilidades e autoridades organizacionais: Exige que os papéis sejam claramente atribuídos e apoiados pela Alta Direção.

11.2 ISO/IEC 27002

11.2.1 Controlos 5.2–5.4: Exigem documentação clara dos papéis de segurança da informação, segregação de funções e supervisão pela gestão.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Estabelece um programa global de segurança da informação com responsabilidades definidas.

11.3.2 PL-1 a PL-4: Exigem controlos de planeamento, incluindo definição de políticas e atribuições documentadas de funções.

11.3.3 CA-1: Exige papéis definidos para avaliação e autorização.

11.3.4 AC-1: Relaciona o controlo de acesso baseado em funções (RBAC) com as responsabilidades de governação atribuídas.

11.4 RGPD da UE

11.4.1 Artigo 5(2) – Responsabilização: Exige que as organizações demonstrem conformidade através de papéis e responsabilidades.

11.4.2 Artigo 32 – Segurança do tratamento: Salienta a atribuição clara de deveres para proteger os dados pessoais.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(a): Exige estruturas de governação que incluam papéis formalizados para a gestão do risco cibernético e de incidentes.

11.6 Regulamento DORA da UE

11.6.1 Artigos 9 e 10: Exigem que as entidades financeiras atribuam e supervisionem de forma clara as responsabilidades relacionadas com as TIC e a segurança.

11.7 COBIT 2019

11.7.1 EDM03 – Ensure Risk Optimization: Exige papéis bem definidos e vias de escalonamento para a gestão do risco de segurança.

11.7.2 APO13 – Manage Security: Atribui deveres estratégicos e operacionais de segurança a indivíduos e funções.

11.7.3 DSS05 – Manage Security Services: Exige estrutura e rastreabilidade nas responsabilidades por serviços de segurança internos e externos.