					Insira aqui a designação da entidade jurídica registada							
Número do documento: P01S					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**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 5.1, 5.2, 5.3, 6.1, 6.2, 8	Especifica o compromisso da gestão, os requisitos da política, a atribuição de funções, a avaliação de riscos e o controlo operacional
ISO/IEC 27002:2022	Controlos 5.1–5	Especifica a definição de políticas de segurança da informação documentadas, a atribuição de funções, a segregação de funções e as responsabilidades da gestão
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Requisitos para o plano do programa de segurança, a política de planeamento, a avaliação e autorização e o controlo de acesso
RGPD da UE (2016/679)	Artigo 5(2), Artigo 32	Princípio da responsabilização e medidas de segurança do tratamento, em especial no que respeita a funções documentadas
Diretiva NIS2 da UE (2022/2555)	Artigo 21(2)(a)	Exige medidas de gestão de riscos, bem como funções e responsabilidades para o risco cibernético
DORA da UE (2022/2554)	Artigo 9, Artigo 10	Exige a atribuição de funções para a gestão do risco de TIC e para a continuidade do negócio
COBIT 2019	EDM03, APO13, DSS05	Assegura a otimização do risco, a gestão da segurança e a gestão dos serviços de segurança através de uma atribuição clara de funções

1. Finalidade

1.1 Esta política demonstra o compromisso da organização com a proteção da informação dos clientes e do negócio, definindo de forma clara responsabilidades e medidas práticas de segurança, adequadas a organizações sem equipas de TI dedicadas.

1.2 Assegura que todos os trabalhadores, prestadores de serviços e fornecedores de serviços cumprem regras obrigatórias, permitindo o cumprimento integral dos requisitos de certificação ISO/IEC 27001.

1.3 Esta política permite à organização reforçar a confiança dos clientes, demonstrando de forma clara como a sua informação é protegida através de responsabilidades definidas, processos estruturados e responsabilização efetiva.

2. Âmbito

2.1 Esta política aplica-se a todas as pessoas que acedem ou gerem os dados e sistemas da organização, incluindo:

2.1.1 Proprietários do negócio e diretores-gerais

2.1.2 Trabalhadores, prestadores de serviços e estagiários

2.1.3 Prestadores externos de serviços de TI ou consultores

2.2 Abrange todos os tipos de informação, sistemas e serviços, incluindo:

2.2.1 Registos do negócio, dados de clientes, palavras-passe e mensagens de correio eletrónico

2.2.2 Equipamento de TI, incluindo computadores portáteis e telemóveis

2.2.3 Serviços na nuvem utilizados para armazenamento de ficheiros, comunicação ou finanças

2.2.4 Documentos físicos armazenados em instalações de escritório

2.3 A política aplica-se a todos os ambientes de trabalho — presenciais, remotos e em nuvem — e inclui todos os dispositivos e aplicações informáticas utilizados para tratar ou armazenar informação do negócio.

3. Objetivos

3.1 Atribuir responsabilidade clara: assegurar que existe sempre uma pessoa responsável pela segurança da informação. Regra geral, trata-se do Diretor-Geral (GM) ou da pessoa por este formalmente designada.

3.2 Proteger a informação de clientes e do negócio: estabelecer salvaguardas fiáveis e consistentes para prevenir a utilização indevida, perda ou furto de dados sensíveis, incluindo registos de clientes e informação financeira.

3.3 Apoiar a certificação ISO/IEC 27001: permitir que a organização demonstre o cumprimento integral dos requisitos da ISO/IEC 27001, assegurando preparação para auditoria e elegibilidade para certificação sem exigir infraestruturas complexas.

3.4 Integrar a segurança nas operações do negócio: incorporar a segurança da informação nas tarefas e decisões diárias em toda a organização.

3.5 Reforçar a sensibilização e a cultura de segurança: assegurar que cada trabalhador compreende e aplica as práticas de segurança, como a utilização de palavras-passe fortes e a notificação de atividade suspeita.

4. Funções e responsabilidades

4.1 Diretor-Geral (GM) ou proprietário do negócio

4.1.1 Detém a responsabilidade integral pela segurança da informação.

4.1.2 Aprova e mantém a presente política.

4.1.3 Assegura que todas as principais atividades de segurança são executadas diretamente ou delegadas por escrito.

4.1.4 Verifica que quaisquer atividades de segurança delegadas, como a gestão de acessos ou a resposta a incidentes, são executadas de forma eficaz.

4.1.5 Atua como ponto de contacto por defeito para todas as matérias internas e externas relacionadas com segurança, incluindo auditorias e pedidos de clientes.

4.1.6 Deve monitorizar o progresso face a estes objetivos durante a revisão anual. Os objetivos devem ser mensuráveis sempre que possível (por exemplo, percentagem de pessoal com formação concluída, número de incidentes reportados, entre outros) e revistos com base em constatações de segurança e alterações no risco.

4.2 Trabalhador designado (quando aplicável)

4.2.1 Pode apoiar o Diretor-Geral (GM) na gestão de atividades diárias, como a criação de contas de utilizador, a remoção de acessos de pessoas que cessaram funções ou a coordenação com o prestador de serviços de TI.

4.2.2 Deve ser formalmente designado e dispor de autoridade e meios suficientes para executar as tarefas.

4.2.3 Reporta quaisquer problemas ao Diretor-Geral (GM).

[... 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 (GM) pelo menos uma vez por ano, para assegurar o cumprimento contínuo dos requisitos de certificação ISO/IEC 27001, de alterações regulamentares (como o RGPD da UE, a Diretiva NIS2 da UE e o DORA da UE) e das necessidades evolutivas do negócio.

9.2 Revisões intercalares

9.2.1 Devem ocorrer revisões adicionais sempre que existam alterações significativas, tais como:

9.2.1.1 Incidentes de segurança graves ou violações

9.2.1.2 Introdução de novos processos de negócio ou tecnologias (por exemplo, novo software, plataformas de trabalho remoto ou serviços na nuvem)

9.2.1.3 Alterações a requisitos legais ou regulamentares que afetem o tratamento da informação

9.3 Documentação das alterações

9.3.1 Todas as revisões e alterações à política devem ser formalmente documentadas, indicando claramente a data, a natureza das revisões e a aprovação do Diretor-Geral (GM).

9.3.2 Deve ser mantido de forma segura um registo histórico das versões da política para demonstrar a sua evolução e o cumprimento durante auditorias.

9.4 Comunicação das atualizações

9.4.1 Quaisquer alterações a esta política devem ser comunicadas prontamente a todos os trabalhadores, prestadores de serviços e terceiros relevantes.

9.4.2 As versões atualizadas da política devem estar facilmente acessíveis a todo o pessoal afetado (por exemplo, disponibilizadas por via eletrónica ou afixadas fisicamente no local de trabalho).

10. Políticas relacionadas e articulações

10.1 Esta política articula-se estreitamente com outras políticas do conjunto de políticas SME da organização, em particular:

10.1.1 P2S – Política de Funções e Responsabilidades de Governação: clarifica a atribuição de deveres e responsabilidades de segurança.

10.1.2 P4S – Política de Controlo de Acesso: define o tratamento seguro do acesso à informação da empresa.

10.1.3 P8S – Política de Sensibilização e Formação em Segurança da Informação: fornece orientações essenciais para a formação e sensibilização do pessoal.

10.1.4 P17S – Política de Proteção de Dados e Privacidade: assegura o cumprimento do RGPD e de outras leis de proteção de dados.

10.1.5 P30S – Política de Resposta a Incidentes: descreve em detalhe as ações exigidas em resposta a incidentes de segurança.

10.2 Estas políticas associadas fornecem orientações operacionais claras e devem ser implementadas de forma conjunta para alcançar o cumprimento integral dos requisitos de certificação ISO/IEC 27001.

11. Normas e referenciais

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.1 – Liderança e compromisso: exige o compromisso da Alta Direção e a responsabilização pela eficácia da segurança da informação na organização.

11.1.2 Cláusula 5.2 – Política de Segurança da Informação: exige políticas claras e documentadas alinhadas com a estratégia organizacional e os requisitos de conformidade.

11.1.3 Cláusula 5.3 – Funções e responsabilidades organizacionais: define a atribuição clara de responsabilidades de segurança da informação em toda a organização, essencial para uma governação eficaz e para a conformidade em auditoria.

11.1.4 Cláusula 6.1 – Ações para tratar riscos e oportunidades: assegura que os riscos para a segurança da informação são identificados, avaliados e tratados de forma sistemática.

11.1.5 Cláusula 8.1 – Planeamento e controlo operacional: exige que a organização planeie e implemente os processos necessários para cumprir os objetivos de segurança da informação e gerir eficazmente os riscos associados.

11.2 ISO/IEC 27002:2022 Controlos 5.1–5

11.2.1 Anexo A Controlo 5.1 – Políticas para a segurança da informação: especifica a definição e comunicação de políticas de segurança da informação documentadas.

11.2.2 Anexo A Controlo 5.2 – Funções de segurança da informação: clarifica e atribui formalmente funções e responsabilidades de segurança da informação às partes relevantes.

11.2.3 Anexo A Controlo 5.3 – Segregação de funções: impõe uma separação clara de funções para reduzir conflitos de interesse e riscos de fraude na gestão de informação sensível.

11.2.4 Anexo A Controlo 5.4 – Responsabilidades da gestão: exige que a gestão demonstre compromisso com a segurança da informação através de supervisão ativa e afetação de recursos.

11.2.5 Reforça a necessidade de políticas, funções, responsabilidades e estruturas de governação da segurança da informação claramente documentadas, assegurando gestão consistente e rastreabilidade para auditoria em toda a organização.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plano do programa de segurança da informação: exige estratégias e políticas documentadas de governação da segurança da informação, fornecendo um referencial para implementação e gestão consistentes.

11.3.2 PL-1 – Política de planeamento da segurança: exige uma política de planeamento da segurança aplicável a toda a organização para orientar a operação segura e o alinhamento estratégico das atividades de segurança da informação.

11.3.3 CA-1 – Política de avaliação e autorização de segurança: requer funções de avaliação e autorização claramente definidas para assegurar eficácia contínua e conformidade com os requisitos de segurança da informação.

11.3.4 AC-1 – Política de controlo de acesso: exige que as organizações definam, documentem e apliquem claramente as práticas e responsabilidades de gestão de acessos.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 5(2) – Princípio da responsabilização: exige que as organizações demonstrem conformidade com os princípios de proteção de dados, incluindo funções e políticas documentadas para responsabilidades de proteção de dados.

11.4.2 Artigo 32 – Segurança do tratamento: exige a implementação de medidas técnicas e organizativas adequadas, incluindo responsabilidades de segurança claras, para proteger os dados pessoais contra violações e acessos não autorizados.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(a) – Medidas de gestão de riscos: exige mecanismos de governação claros, incluindo funções e responsabilidades definidas para a segurança da informação, essenciais para gerir eficazmente os riscos cibernéticos.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 9 – Gestão do risco de TIC: exige que as organizações atribuam claramente funções e responsabilidades relacionadas com a gestão do risco de TIC, reforçando a resiliência e a preparação para a continuidade do negócio.

11.6.2 Artigo 10 – Continuidade de negócio das TIC: exige responsabilização clara e funções estruturadas para manter a resiliência e a continuidade das TIC, assegurando que as organizações conseguem responder de forma fiável a interrupções.

11.7 COBIT 2019

11.7.1 EDM03 – Assegurar a otimização do risco: enfatiza a definição clara de responsabilização e funções na gestão dos riscos organizacionais, proporcionando uma governação sólida e supervisão eficaz dos riscos de segurança da informação.

11.7.2 APO13 – Gerir a segurança: exige que as organizações estabeleçam e comuniquem claramente as responsabilidades de gestão da segurança, assegurando o alinhamento com os objetivos do negócio e os requisitos regulamentares.

11.7.3 DSS05 – Gerir serviços de segurança: requer funções estruturadas e responsabilidades claras na gestão de serviços de segurança, permitindo implementação consistente e verificação da conformidade.