					Insira aqui a designação da entidade jurídica registada							
Número do documento: P14S					Título do documento: **Política de Retenção e Eliminação de Dados**							
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 6.1.3, 8	Abrange o tratamento de riscos, os controlos operacionais e os requisitos de retenção
ISO/IEC 27002:2022	Controlo 5	Orientações sobre períodos de retenção e métodos de destruição segura
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Retenção de registos de auditoria, sanitização de suportes e limites/aplicação da retenção de dados
Diretiva NIS2 da UE	Artigo 21(2)(a)	Exige uma política de gestão do ciclo de vida adequada ao risco
DORA da UE	Artigo 5(1)	Gestão do risco das TIC: disponibilidade e remoção de dados
COBIT 2019	BAI03.04, DSS01	Controlos do ciclo de vida da informação, eliminação segura
RGPD da UE	Artigos 5(1)(e), 17	Os dados não devem ser conservados por mais tempo do que o necessário; direito ao apagamento

1. Finalidade

1.1 A finalidade desta política é definir as regras aplicáveis à retenção e eliminação segura da informação num contexto de PME. Garante que os registos são conservados apenas durante o período exigido por lei, por obrigação contratual ou por necessidade do negócio, sendo posteriormente destruídos de forma segura.

1.2 Esta política visa reduzir o risco da informação, gerir a exposição jurídica e limitar o armazenamento de dados redundantes ou obsoletos. Contribui para assegurar a conformidade com a ISO/IEC 27001 e com referenciais de privacidade como o RGPD da UE, minimizando a retenção não autorizada de informação pessoal ou sensível.

1.3 Um quadro de retenção e eliminação bem estruturado reduz custos operacionais, melhora o desempenho dos sistemas e aumenta a capacidade de demonstrar conformidade em auditoria. Para PME com capacidade de TI limitada, constitui uma forma prática de gerir de forma responsável os ativos de informação digitais e físicos.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os registos, ficheiros, logs, comunicações e conjuntos de dados criados, recolhidos, tratados ou armazenados pela organização

2.1.2 Todos os trabalhadores, contratados e prestadores de serviços externos que tratem dados da organização

2.1.3 Todos os formatos de dados (por exemplo, papel, eletrónico, imagem, áudio ou log) e todos os suportes de armazenamento (por exemplo, discos locais, serviços na nuvem, servidores de correio eletrónico, cópias de segurança)

2.2 O âmbito inclui:

2.2.1 Documentos do negócio (por exemplo, faturas, contratos, relatórios de projeto)

2.2.2 Registos operacionais (por exemplo, logs, histórico de acessos, snapshots de cópias de segurança)

2.2.3 Dados pessoais (por exemplo, ficheiros de RH, comunicações com clientes, registos de suporte)

2.2.4 Dados alojados internamente, externamente ou em sistemas híbridos

2.2.5 Dados arquivados e cópias de segurança, quer ativos quer inativos

2.3 Todas as fases do ciclo de vida dos dados estão incluídas no âmbito, desde a criação até à eliminação autorizada.

3. Objetivos

3.1 Definir regras de retenção consistentes com base em critérios legais, operacionais e regulamentares.

3.2 Prevenir a eliminação prematura de registos críticos e eliminar a acumulação desnecessária de dados.

3.3 Assegurar a eliminação segura e irreversível dos dados quando a retenção deixar de ser necessária.

3.4 Atribuir responsabilidades pela aplicação das decisões de retenção e eliminação, tendo em conta as limitações de recursos de uma PME.

3.5 Disponibilizar documentação apta para auditoria, de modo a demonstrar diligência devida ao abrigo da ISO 27001, do RGPD, da Diretiva NIS2 da UE e de outros referenciais.

3.6 Promover o tratamento seguro dos dados ao longo do seu ciclo de vida, sem impor encargos técnicos desnecessários ao pessoal não especializado.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Aprova esta política e assume a respetiva titularidade.

4.1.2 Assegura que os procedimentos de retenção e eliminação são implementados de forma consistente com o risco jurídico e o risco do negócio.

4.1.3 Autoriza exceções e medidas de preservação legal, quando necessário.

4.1.4 Determina revisões da política e aprova atualizações com base em alterações do negócio ou regulamentares.

4.2 Responsável designado pelos dados

4.2.1 É designado por categoria de dados (por exemplo, dados financeiros, de RH ou registos de clientes).

4.2.2 Classifica os registos e determina a retenção adequada com base na política e na orientação jurídica.

4.2.3 Autoriza a eliminação quando os requisitos de retenção estiverem cumpridos.

4.2.4 Apoia as auditorias internas, fornecendo contexto sobre a fundamentação da retenção e os eventos de eliminação.

[... 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 deve ser revista pelo menos uma vez por ano, ou quando ocorrer:

9.1.1 Alterações à legislação aplicável (por exemplo, privacidade de dados, reporte financeiro)

9.1.2 Adoção de novos sistemas ou processos que afetem o ciclo de vida dos dados

9.1.3 Constatações de auditoria ou incidentes que revelem lacunas nas práticas de retenção

9.2 As revisões devem assegurar que o Registo de Retenção permanece completo e reflete todas as principais categorias de registos.

9.3 As atualizações da política devem ser aprovadas pelo GM e comunicadas ao pessoal afetado. A versão mais recente deve estar acessível e sujeita a controlo de versões.

10. Políticas relacionadas e ligações

10.1 P2S – Política de Papéis e Responsabilidades de Governação: Define a titularidade da política e a autoridade para exceções.

10.2 P13S – Política de Classificação e Rotulagem de Dados: Determina a forma como as regras de retenção se alinham com a classificação dos dados.

10.3 P12S – Política de Gestão de Ativos: Rege os suportes de armazenamento que contêm dados sujeitos a retenção e eliminação.

10.4 P17S – Política de Proteção de Dados e Privacidade: Assegura a minimização de dados e suporta o tratamento lícito ao abrigo do RGPD da UE.

10.5 P30S – Política de Resposta a Incidentes: É ativada quando falhas na eliminação ou na retenção resultam em potencial exposição de dados.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1.3: Exige o tratamento de riscos relacionados com a informação, incluindo riscos de retenção.

11.1.2 Cláusula 8.1: Define controlos operacionais do ciclo de vida.

11.2 ISO/IEC 27002

11.2.1 Controlo 5.33: Orientações para a definição de períodos de retenção e métodos de destruição segura.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Exige a retenção de registos de auditoria.

11.3.2 MP-6: Define procedimentos de sanitização de suportes.

11.3.3 SI-12: Trata os limites de retenção de dados e a respetiva aplicação.

11.4 RGPD da UE

11.4.1 Artigo 5(1)(e): Os dados devem ser conservados apenas durante o período necessário.

11.4.2 Artigo 17: O direito ao apagamento aplica-se quando os dados deixam de estar legalmente retidos.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(a): Exige políticas organizacionais adequadas ao risco, incluindo a gestão do ciclo de vida.

11.6 DORA da UE

11.6.1 Artigo 5(1): A gestão do risco das TIC inclui a disponibilidade e remoção de dados.

11.7 COBIT 2019

11.7.1 BAI03.04: Exige controlos do ciclo de vida da informação.

11.7.2 DSS01.06: Procedimentos de eliminação segura como parte da salvaguarda dos ativos de informação.