					Insira aqui a designação da entidade jurídica registada							
Número do documento: P14					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, 8.1	
ISO/IEC 27002:2022	Controlos 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
RGPD da UE	Artigos 5(1)(e), 17, 32	
Diretiva NIS2 da UE	Artigo 21(2)(a-e)	
DORA da UE	Artigos 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Finalidade

1.1 A finalidade desta política é definir os requisitos organizacionais para a retenção de dados e a eliminação segura em todas as fases do ciclo de vida da informação. Esta política assegura o cumprimento das obrigações legais, regulamentares e contratuais aplicáveis e evita a acumulação desnecessária ou arriscada de dados.

1.2 Esta política apoia a implementação da ISO/IEC 27001:2022 ao impor controlos sobre a duração da conservação dos dados e sobre práticas de eliminação irreversível. Permite a documentação rastreável dos registos, impõe a retenção alinhada com a classificação da informação e assegura a capacidade de demonstrar conformidade em auditorias, inspeções regulatórias e processos de discovery.

1.3 Visa ainda preservar a Confidencialidade, Integridade e Disponibilidade dos dados, minimizando simultaneamente o risco de negócio, as ineficiências operacionais e a exposição a violações de privacidade resultantes de retenção ou destruição inadequadas.

2. Âmbito

2.1 Esta política aplica-se a todos os ativos de informação físicos e digitais detidos, tratados ou conservados pela organização, incluindo os que se encontrem sob o controlo de terceiros, filiais ou prestadores de serviços de outsourcing.

2.2 O âmbito inclui, sem caráter limitativo:

2.2.1 Documentos, ficheiros e registos (digitais e em papel)

2.2.2 Bases de dados e arquivos

2.2.3 Mensagens de correio eletrónico e registos de mensagens instantâneas

2.2.4 Cópias de segurança, registos de sistema e trilhos de auditoria

2.2.5 Código-fonte, dados de aplicações e ativos alojados na cloud

2.2.6 Suportes amovíveis e hardware em fim de vida que contenham dados

2.3 A política rege tanto os registos operacionais como os conjuntos de dados regulados (por exemplo, informação financeira, jurídica, de recursos humanos, relativa a clientes e relevante para auditoria), independentemente da localização de armazenamento ou do sistema.

2.4 Aplica-se a todos os departamentos organizacionais e a todos os colaboradores, prestadores de serviços e fornecedores envolvidos na criação, armazenamento, gestão ou eliminação de dados.

3. Objetivos

3.1 Assegurar que os dados são conservados apenas pelo período legal, contratual ou operacionalmente necessário e eliminados de forma segura quando deixem de ser necessários.

3.2 Prevenir a eliminação prematura, não autorizada ou acidental de registos necessários para operações em curso, conformidade, litígios ou fins de auditoria.

3.3 Estabelecer e aplicar calendários de retenção consistentes com base na classificação da informação, no tipo de ativo, na legislação aplicável e na exposição ao risco.

3.4 Salvaguardar a privacidade e a confidencialidade dos dados durante o respetivo período de retenção e no momento da eliminação, incluindo o exercício dos direitos do titular dos dados (por exemplo, apagamento ao abrigo do artigo 17.º do RGPD da UE).

3.5 Assegurar que todos os métodos de eliminação de dados são irreversíveis, devidamente documentados e conformes com normas reconhecidas, como a NIST SP 800-88.

3.6 Minimizar ineficiências operacionais, custos adicionais e exposição jurídica causados por retenção excessiva ou por dados legados não rastreados.

3.7 Apoiar os objetivos de continuidade do negócio e de recuperação de desastre através de uma governação integrada da retenção de cópias de segurança e de práticas de arquivo de dados defensáveis.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova esta política e assegura financiamento, recursos e integração adequados na gestão do risco empresarial e nos programas de conformidade.

4.1.2 Detém a responsabilidade global pelo cumprimento legal e regulamentar relacionado com a retenção de dados e a eliminação segura.

4.2 Chief Information Security Officer (CISO)

4.2.1 É o proprietário desta política e responsável por definir e rever a governação da retenção e eliminação em alinhamento com o SGSI.

4.2.2 Assegura que os requisitos de retenção e eliminação orientados pela classificação da informação são implementados nas unidades de negócio e nos sistemas técnicos.

4.2.3 Monitoriza o cumprimento da política e determina ações corretivas sempre que necessário.

[... 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 anualmente ou quando se verifique qualquer uma das seguintes condições:

9.1.1 Alterações à legislação ou regulamentação aplicáveis que afetem a retenção de dados (por exemplo, atualizações ao RGPD da UE, códigos fiscais, DORA da UE)

9.1.2 Revisões do quadro de classificação ou dos processos de negócio com impacto nas fases do ciclo de vida dos dados

9.1.3 Introdução de novos sistemas de TI, plataformas de arquivo ou tecnologias de eliminação de suportes

9.1.4 Constatações de auditoria interna ou recomendações regulatórias que evidenciem lacunas nas práticas de retenção ou eliminação

9.2 A revisão deve ser conduzida pelo CISO e pelo Encarregado da Proteção de Dados (EPD), com contributos das áreas Jurídica, de Conformidade, de TI e das unidades de negócio.

9.3 O Calendário Mestre de Retenção de Dados (MDRS) e o Registo de Eliminação devem ser revistos em paralelo para assegurar que:

9.3.1 Os calendários permanecem exatos e refletem as necessidades operacionais, legais e regulamentares

9.3.2 A documentação de eliminação está completa e auditável

9.3.3 Os registos de preservação legal são validados e levantados quando adequado

9.4 Quaisquer atualizações à política devem:

9.4.1 Ser formalmente versionadas e conservadas no repositório documental do SGSI

9.4.2 Incluir um histórico de revisões e a respetiva justificação da alteração

9.4.3 Ser aprovadas pela Alta Direção

9.4.4 Ser comunicadas ao pessoal relevante com materiais de formação ou orientação atualizados

9.5 Sempre que ocorram alterações materiais à política, os colaboradores afetados devem concluir formação direcionada no prazo de 30 dias após a publicação, para assegurar a continuidade da conformidade.

9.6 Políticas relacionadas e ligações

10. Políticas relacionadas e ligações

10.1.1 P4 - Política de Controlo de Acesso: assegura que apenas pessoas autorizadas acedem aos dados durante o respetivo período de retenção e que os dados expirados ficam restringidos enquanto aguardam eliminação.

10.1.2 P12 - Política de Gestão de Ativos: identifica quais os ativos que contêm dados sujeitos a eliminação programada e acompanha o respetivo ciclo de vida desde a aquisição até à destruição.

10.1.3 P13 - Política de Classificação e Rotulagem da Informação: orienta as decisões de classificação que influenciam diretamente a duração da retenção e o método de eliminação exigido.

10.1.4 P15 - Política de Cópias de Segurança e Restauro: define períodos de retenção e procedimentos de eliminação para suportes de cópias de segurança e ativos de dados replicados.

10.1.5 P18 - Política de Controlos Criptográficos: suporta o apagamento criptográfico para efeitos de eliminação e impõe a cifragem durante a conservação dos dados até à destruição.

10.1.6 P30 - Política de Resposta a Incidentes: é acionada nos casos em que a eliminação inadequada resulte em potencial perda de dados, incidente de segurança ou incumprimento regulamentar.

10.2 Cada política associada desempenha um papel na aplicação de um modelo coerente de governação de dados nas vertentes de classificação, controlo do ciclo de vida, acesso e capacidade de demonstrar conformidade em auditoria.

11. Normas e quadros de referência

11.1 Esta política está alinhada com normas e quadros regulamentares globalmente reconhecidos que definem práticas seguras, conformes e eficientes para o ciclo de vida dos dados.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 6.1.3 - Plano de tratamento de riscos: apoia a mitigação de riscos associados à retenção excessiva, a violações de dados ou a falhas de eliminação.

11.2.2 Cláusula 8.1 - Planeamento e controlo operacional: estabelece controlos do ciclo de vida que regem armazenamento, arquivo e destruição.

11.3 ISO/IEC 27002:2022 - Controlos 5.10, 5.12, 5.30, 5: fornecem orientação prática sobre utilização aceitável dos dados, justificação da retenção, eliminação controlada e manutenção defensável de registos, em alinhamento com a tolerância ao risco da organização.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Retenção de registos de auditoria: assegura armazenamento suficiente de registos de auditoria e evidência de conformidade.

11.4.2 MP-6 - Sanitização de suportes: exige métodos de destruição seguros e documentados para suportes físicos e eletrónicos.

11.4.3 SI-12 - Tratamento da informação: impõe o tratamento adequado dos dados em alinhamento com os controlos de retenção e eliminação.

11.4.4 PL-2 - Plano de segurança e privacidade do sistema: exige documentação específica do sistema relativa ao tratamento do ciclo de vida dos dados e às disposições de eliminação segura.

11.5 RGPD da UE (2016/679):

11.5.1 Artigo 5(1)(e) - Minimização de dados e limitação da conservação: exige que os dados não sejam conservados por mais tempo do que o necessário.

11.5.2 Artigo 17 - Direito ao apagamento ("direito a ser esquecido"): exige a eliminação célere e permanente de dados pessoais mediante pedido válido.

11.5.3 Artigo 32 - Segurança do tratamento: reforça a proteção dos dados durante a retenção e exige a destruição segura de registos expirados.

11.6 Diretiva NIS2 da UE (2022/2555):

11.6.1 Artigo 21(2)(a-e): exige que as entidades adotem políticas e medidas técnicas para o tratamento seguro dos dados, incluindo limitações de armazenamento e métodos de eliminação.

11.7 DORA da UE (2022/2554):

11.7.1 Artigo 5 - Governação e controlo: determina uma gestão estruturada do risco das TIC, incluindo o tratamento seguro do ciclo de vida da informação.

11.7.2 Artigo 9 - Quadro de gestão do risco das TIC: exige políticas para retenção de dados, destruição e cumprimento legal/regulamentar das operações digitais.

11.8 COBIT 2019:

11.8.1 DSS01 - Operações geridas: apoia o acompanhamento da retenção e a consistência entre sistemas de dados.

11.8.2 DSS05 - Gerir Serviços de Segurança: assegura a proteção dos dados armazenados e arquivados até à respetiva eliminação segura.

11.8.3 MEA03 - Monitorizar, Avaliar e Analisar a Conformidade: permite a auditoria da aplicação da retenção, dos procedimentos de eliminação e do cumprimento regulamentar.