					Insira aqui a designação da entidade jurídica registada							
Número do documento: P18					Título do documento: **Política de Controlos Criptográficos**							
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	Cláusula 8	-
ISO/IEC 27002:2022	Controlos 8.24, 8.25, 8	-
NIST SP 800-53 Rev. 5	SC-12 a SC-17, SC-28, SC-28(1), SC-12(3)	-
RGPD da UE	Artigo 32, Artigos 33–34, Considerando 83	-
Diretiva NIS2 da UE	Artigo 21(2)(d)	-
DORA da UE	Artigos 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA03	-

1. Finalidade

1.1 Esta política define requisitos obrigatórios para a utilização segura e conforme de controlos criptográficos em toda a organização, de modo a assegurar a confidencialidade, integridade, disponibilidade e autenticidade da informação sensível e regulada.

1.2 A utilização de criptografia sustenta a confiança nas operações de segurança da informação, suporta comunicações seguras, reforça o controlo de acesso e permite a conformidade regulamentar através de práticas eficazes de cifragem e gestão de chaves.

1.3 Esta política está alinhada com a Cláusula 8.1 da ISO/IEC 27001:2022 e com o Controlo 8.24 do Anexo A, e suporta obrigações legais e operacionais ao abrigo do Artigo 32 do RGPD da UE, do Artigo 6(2)(d) do DORA da UE e do Artigo 21 da Diretiva NIS2 da UE. Suporta igualmente os objetivos do COBIT 2019 relativos aos serviços de segurança e à proteção dos ativos de informação.

2. Âmbito

2.1 Esta política aplica-se a todas as unidades organizacionais, funções de negócio, colaboradores e prestadores de serviços terceiros envolvidos na utilização, administração ou implementação de ferramentas e métodos criptográficos.

2.2 Os ambientes abrangidos incluem sistemas de produção, desenvolvimento, pré-produção, cópias de segurança e recuperação de desastre, nos quais dados sensíveis sejam transmitidos, tratados ou armazenados.

2.3 O âmbito inclui todos os componentes criptográficos e casos de uso, incluindo, sem limitação:

2.3.1 Cifragem simétrica e assimétrica

2.3.2 Assinaturas digitais e certificados

2.3.3 Algoritmos de hash

2.3.4 Geração, distribuição e destruição segura de chaves

2.3.5 Transport Layer Security (TLS), cifragem integral de disco e cifragem ao nível da API

2.3.6 Elementos seguros, tais como Hardware Security Modules (HSM), Trusted Platform Modules (TPM) e sistemas de gestão de chaves (KMS)

2.4 Esta política rege a utilização de criptografia relativamente a:

2.4.1 Dados classificados como Confidencial, Altamente Confidencial ou Regulados

2.4.2 Autenticação e verificação de identidade digital

2.4.3 Comunicações seguras com partes externas

2.4.4 Custódia de chaves e mecanismos de controlo dual

3. Objetivos

3.1 Assegurar que as tecnologias criptográficas são selecionadas, aprovadas, implementadas e mantidas em conformidade com o risco de negócio, as normas internacionais e os requisitos regulamentares.

3.2 Estabelecer uma estrutura de governação normalizada para a gestão de serviços criptográficos, incluindo responsabilização clara pela implementação, validação e gestão de exceções.

3.3 Prevenir a utilização não autorizada, a configuração incorreta ou a obsolescência de algoritmos criptográficos e de controlos, através de um processo formal de aprovação e revisão.

3.4 Assegurar que os controlos criptográficos são incorporados na fase de conceção dos sistemas e validados regularmente para prevenir a exposição de dados, o compromisso de chaves ou a degradação de protocolos.

3.5 Aplicar a gestão do ciclo de vida de todas as chaves criptográficas, incluindo geração, armazenamento, utilização, rotação, revogação e destruição segura.

3.6 Cumprir regulamentos internacionais e regionais que imponham cifragem e tratamento seguro de dados, incluindo o RGPD da UE, o DORA da UE, a Diretiva NIS2 da UE e o COBIT 2019.

4. Papéis e responsabilidades

4.1 Responsável pela Segurança da Informação / Diretor de Segurança da Informação

4.1.1 É responsável por esta política e assegura o seu alinhamento com o SGSI e com o Controlo 8.24 do Anexo A da ISO/IEC 27001.

4.1.2 Aprova a utilização de algoritmos e controlos criptográficos e assegura o respetivo cumprimento em toda a organização.

4.2 Responsável pelas Operações Criptográficas / Arquiteto de Segurança

4.2.1 Gere as operações diárias e a administração dos sistemas criptográficos.

4.2.2 Mantém a Lista de Métodos Criptográficos Aprovados (ACML) e o Registo de Gestão de Chaves.

4.2.3 Realiza revisões de arquitetura criptográfica e avalia novas tecnologias criptográficas.

[... 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 pelo Responsável pela Segurança da Informação e pelo Responsável pelas Operações Criptográficas.

9.2 Os fatores desencadeadores de revisão incluem:

9.2.1 Descoberta de vulnerabilidades criptográficas (por exemplo, downgrade de algoritmos, ataques quânticos)

9.2.2 Alterações regulamentares que exijam normas de cifragem atualizadas

9.2.3 Constatações operacionais ou de auditoria que revelem lacunas na política

9.2.4 Atualizações de ferramentas criptográficas ou alterações de arquitetura

9.3 As atualizações devem estar sujeitas a controlo de versões no Registo de Documentos do SGSI e ser comunicadas a:

9.3.1 Todos os administradores com funções de acesso criptográfico

9.3.2 Equipas de desenvolvimento e responsáveis de DevSecOps

9.3.3 Fornecedores terceiros sujeitos a obrigações contratuais de cifragem

9.4 A equipa do SGSI deve assegurar que as versões substituídas são arquivadas e deixam de ser referenciadas nos procedimentos operacionais.

10. Políticas relacionadas e interligações

10.1 P1 - Política de Segurança da Informação. Fornece a governação de base para todas as medidas de segurança, incluindo a aplicação de controlos criptográficos, a proteção de ativos e as comunicações seguras.

10.2 P4 - Política de Controlo de Acesso. Assegura que o acesso lógico a material criptográfico e a sistemas de gestão de cifragem é estritamente limitado com base no princípio do menor privilégio e na segregação de funções.

10.3 P6 - Política de Gestão de Riscos. Suporta a avaliação dos riscos associados aos controlos criptográficos e documenta a estratégia de tratamento de riscos para exceções, obsolescência de algoritmos ou cenários de compromisso de chaves.

10.4 P12 - Política de Gestão de Ativos. Determina a classificação de dados sensíveis e de ativos de hardware, o que define diretamente os requisitos criptográficos e as obrigações de custódia de chaves.

10.5 P13 - Política de Classificação e Rotulagem de Dados. Define os níveis de classificação (por exemplo, Confidencial, Regulado) que desencadeiam requisitos específicos de cifragem em trânsito e em repouso.

10.6 P14 - Política de Retenção e Eliminação de Dados. Especifica procedimentos para a eliminação segura de suportes de armazenamento cifrados e de material criptográfico no fim da vida útil.

10.7 P30 - Política de Resposta a Incidentes (P30). Define a estratégia de resposta da organização para o compromisso de chaves, a utilização indevida de certificados ou a suspeita de vulnerabilidades algorítmicas, incluindo revogação rápida e notificação de violações.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 - Planeamento e controlo operacional: impõe controlos técnicos de segurança, incluindo medidas criptográficas, como parte das salvaguardas operacionais.

11.2 ISO/IEC 27002:2022

11.2.1 Controlos 8.24, 8.25, 8: fornece orientações de implementação sobre os objetivos dos controlos criptográficos, seleção de algoritmos, aplicação de protocolos e gestão do ciclo de vida dos certificados.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - Estabelecimento de chaves criptográficas: assegura a geração e a troca seguras de chaves de cifragem. A P18 define como as chaves simétricas e assimétricas devem ser geradas e trocadas com recurso a algoritmos e protocolos aprovados.

11.3.2 SC-13 - Proteção criptográfica: impõe a utilização de criptografia para proteger a confidencialidade e a integridade da informação. A P18 aplica cifragem em repouso e em trânsito com base na classificação dos dados, com normas algorítmicas alinhadas com a NIST FIPS 140-3.

11.3.3 SC-17 - Certificados da Infraestrutura de Chave Pública (PKI): requer a implementação de PKI para suportar autenticação e assinaturas digitais. A P18 define a utilização de PKI para proteger comunicações, identidades de sistemas e acessos administrativos.

11.3.4 SC-28, SC-28(1) - Proteção da informação em repouso e em trânsito: requer a cifragem dos dados quando armazenados ou transmitidos através de redes não confiáveis. A P18 especifica a aplicação de TLS, túneis VPN, cifragem integral de disco e métodos de armazenamento seguro para dados sensíveis.

11.3.5 SC-12(3) - Geração de chaves simétricas para armazenamento e distribuição seguros: centra-se na geração e tratamento seguros de chaves simétricas. A P18 exige a utilização de geradores robustos de números aleatórios, políticas de rotação de chaves e cofres de chaves seguros para operações criptográficas.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 32 - Segurança do tratamento: recomenda expressamente a cifragem como medida de redução de risco para dados pessoais.

11.4.2 Considerando 83: reforça a cifragem como controlo para prevenir o acesso não autorizado a dados.

11.4.3 Artigos 33 e 34: a cifragem pode isentar as organizações de notificações obrigatórias de violação, quando eficaz.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(d): exige medidas técnicas e organizativas, incluindo proteções criptográficas, para manter a disponibilidade e a integridade dos serviços.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 6(2)(d): as instituições financeiras devem proteger os dados, incluindo através de cifragem forte da informação crítica.

11.6.2 Artigo 11(1)(c): impõe controlos seguros de tratamento de dados para prestadores de serviços terceiros de TIC.

11.7 COBIT 2019

11.7.1 DSS05.01 - Proteger ativos de informação: exige a utilização de cifragem e gestão de chaves para salvaguardar dados contra acessos não autorizados.

11.7.2 DSS06.06 - Testes de segurança geridos: recomenda a validação da conformidade criptográfica como parte das avaliações de vulnerabilidades.

11.7.3 MEA03 - Monitorizar, Avaliar e Analisar a Conformidade: impõe a garantia contínua da eficácia dos controlos criptográficos.