					Insira aqui a designação da entidade jurídica registada							
Número do documento: P18S					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	
NIST SP 800-53 Rev. 5	SC-12 a SC-17	
Diretiva NIS2 da UE	Artigos 21(2)(d), 21(2)(e)	
DORA da UE	Artigos 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
RGPD da UE	Artigos 32(1)(a), 34	

1. Finalidade

1.1 Esta política define requisitos obrigatórios para a utilização de cifragem e de controlos criptográficos com vista à proteção da confidencialidade, integridade e autenticidade dos dados empresariais e dos dados pessoais.

1.2 Assegura que as ferramentas criptográficas são utilizadas adequadamente em sistemas, dispositivos e serviços na nuvem no contexto de uma pequena empresa.

1.3 Esta política apoia diretamente a certificação ISO/IEC 27001:2022 e contribui para o cumprimento, pela organização, das obrigações legais decorrentes do RGPD da UE, da Diretiva NIS2 da UE e do Regulamento DORA da UE.

1.4 Os controlos criptográficos abrangidos incluem a cifragem de dados, a gestão de certificados, o tratamento seguro de chaves e as cópias de segurança cifradas.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os trabalhadores, prestadores de serviços e terceiros que tratem dados da organização

2.1.2 Todos os sistemas empresariais, terminais e plataformas na nuvem utilizados para armazenar, transmitir ou aceder a informação confidencial

2.1.3 Todos os registos pessoais, financeiros, jurídicos ou sensíveis classificados ao abrigo da política de classificação da informação da organização

2.1.4 Qualquer controlo criptográfico, incluindo métodos de cifragem, chaves, palavras-passe, certificados e módulos de segurança

2.2 A política abrange dados em repouso, dados em trânsito e dados em utilização. Regula igualmente a cifragem utilizada em cópias de segurança, correio eletrónico, transferências externas de dados e sítios Web acessíveis ao público.

3. Objetivos

3.1 Assegurar que os dados sensíveis e regulamentados são protegidos em permanência através de medidas criptográficas adequadas

3.2 Definir responsabilidades pela seleção de ferramentas de cifragem, configuração e gestão de chaves

3.3 Prevenir o acesso não autorizado, a adulteração ou a fuga de dados através da aplicação de controlos seguros de transmissão e armazenamento

3.4 Cumprir os requisitos legais e regulamentares que imponham a cifragem de dados pessoais e empresariais

3.5 Manter a segurança operacional e a disponibilidade através de uma gestão eficaz de certificados e chaves criptográficas

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Aprova esta política e assegura a aplicação dos requisitos criptográficos

4.1.2 Revê exceções, notificações de violação de dados e o cumprimento, por parte dos fornecedores, das cláusulas de cifragem

4.1.3 Assegura que os serviços externalizados ou alojados na nuvem cumprem os requisitos de cifragem aplicáveis

4.2 Prestador de serviços de TI / administrador interno de TI

4.2.1 Implementa e mantém soluções de cifragem (por exemplo, cifragem integral de disco, certificados SSL/TLS e VPN)

4.2.2 Gere o ciclo de vida das chaves criptográficas e as ferramentas de armazenamento seguro

4.2.3 Configura e monitoriza a cifragem para proteção de cópias de segurança, sítios Web e dispositivos

[... 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 menos uma vez por ano pelo Diretor-Geral, em articulação com o prestador de serviços de TI e o Responsável pela Privacidade.

9.2 Fatores desencadeadores de revisão intercalar

9.2.1 Devem igualmente ser efetuadas revisões se:

9.2.1.1 As normas ou protocolos criptográficos mudarem (por exemplo, descontinuação de um algoritmo)

9.2.1.2 Forem introduzidos novos sistemas ou serviços na nuvem

9.2.1.3 Uma violação ou incidente envolver uma chave ou certificado comprometido

9.2.1.4 Atualizações legais ou regulamentares afetarem os requisitos de cifragem

9.3 Controlo de versões e comunicação

9.3.1 Todas as alterações à política devem ser documentadas num registo de versões

9.3.2 Os trabalhadores devem ser notificados das atualizações e as versões anteriores devem ser arquivadas

9.3.3 A versão aprovada mais recente deve ser armazenada no repositório central de políticas

10. Políticas relacionadas e ligações

10.1 Esta política deve ser aplicada em conjunto com as seguintes políticas SME:

10.1.1 P12S – Política de Gestão de Ativos: Assegura que a cifragem é aplicada aos ativos classificados durante o armazenamento, transferência e eliminação.

10.1.2 P14S – Política de Retenção e Eliminação de Dados: Define os períodos de retenção e exige o armazenamento cifrado dos dados até à sua eliminação segura.

10.1.3 P17S – Política de Proteção de Dados e Privacidade: Alinha a cifragem com os princípios de proteção de dados e as expectativas regulamentares ao abrigo do artigo 32.º do RGPD.

10.1.4 P22S – Política de Registo e Monitorização: Exige o registo da utilização de chaves, falhas de cifragem e expiração de certificados para efeitos de auditoria.

10.1.5 P30S – Política de Resposta a Incidentes: Detalha os procedimentos de escalonamento, contenção e notificação quando a cifragem falha ou as chaves são comprometidas.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Exige a implementação de controlos operacionais, incluindo cifragem, para gerir riscos de segurança.

11.2 ISO/IEC 27002

11.2.1 Controlo 8.24 – Descreve os requisitos para a aplicação da cifragem para assegurar a confidencialidade e a integridade.

11.2.2 Controlo 8.25 – Define a gestão segura de chaves criptográficas e certificados.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Estabelece requisitos para o estabelecimento e a validação de chaves criptográficas.

11.3.2 SC-13 – Define requisitos para a utilização de proteção criptográfica.

11.3.3 SC-17 – Abrange a infraestrutura de chave pública (PKI) e a gestão do ciclo de vida dos certificados.

11.3.4 SC-28 – Exige a cifragem de dados em repouso.

11.3.5 SC-12 a SC-17 (família) – Assegura que as proteções criptográficas são implementadas adequadamente em todos os sistemas.

11.4 RGPD da UE

11.4.1 Artigo 32(1)(a) – Exige que as organizações implementem medidas técnicas, como a cifragem, para assegurar a confidencialidade dos dados.

11.4.2 Artigo 34 – Estabelece que a cifragem pode isentar as organizações da notificação de violações de dados se os dados forem ininteligíveis para pessoas não autorizadas.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(d) – Exige cifragem eficaz para proteger sistemas e comunicações.

11.5.2 Artigo 21(2)(e) – Reforça a proteção de dados e a mitigação de ciberameaças através da cifragem.

11.6 DORA da UE

11.6.1 Artigo 6(2)(d) – Exige que os sistemas de TIC mantenham canais de comunicação seguros e cifragem.

11.6.2 Artigo 9(2)(f) – Obriga as entidades financeiras a utilizarem cifragem robusta para salvaguardar comunicações digitais e trocas de dados.

11.7 COBIT 2019

11.7.1 DSS05.01 – Determina a proteção de informação sensível através de cifragem e protocolos criptográficos.

11.7.2 APO13.02 – Exige a implementação eficaz de controlos de segurança, incluindo salvaguardas criptográficas, como parte do planeamento da segurança da informação.