					Insira aqui a designação da entidade jurídica registada							
Número do documento: P16S					Título do documento: **Política de Mascaramento de Dados e Pseudonimização**							
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**

Aviso legal (direitos de autor e restrições de utilização)

(C) 2025 Clarysec LLC. All rights reserved.

Este documento é propriedade intelectual da Clarysec LLC. Nenhuma parte deste documento pode ser copiada, reutilizada, distribuída ou modificada para fins comerciais ou de implementação sem autorização prévia, expressa e por escrito.

A utilização não autorizada é estritamente proibida e pode dar origem a ações legais.

Para efeitos de licenciamento, contacte: info@clarysec.com

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 6.1.3, Cláusula 8	Riscos de segurança da informação e controlos necessários, incluindo mascaramento e pseudonimização
ISO/IEC 27002:2022	Controlos 8.11, 8.12	Orientações sobre mascaramento e prevenção de fugas de dados
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Ofuscação de dados e tecnologias de reforço da privacidade
Diretiva NIS2 da UE	Artigo 21(2)(c)	Medidas técnicas proporcionadas, incluindo a pseudonimização como controlo
DORA da UE	Artigo 10(1)	Controlos de risco das TIC, incluindo salvaguardas de transformação
COBIT 2019	DSS05.01, DSS06	Proteção de dados e técnicas de ofuscação/pseudonimização
RGPD da UE	Artigos 4(5), 5(1)(c), 32	Minimização de dados e pseudonimização como controlo técnico

1. Finalidade

1.1. A presente política estabelece requisitos obrigatórios para a utilização de mascaramento de dados e pseudonimização, com o objetivo de proteger dados sensíveis, pessoais e confidenciais em pequenas e médias empresas (PME).

1.2. Estas técnicas são obrigatórias sempre que os dados reais não sejam necessários, nomeadamente em cenários de desenvolvimento, análise de dados ou utilização por prestadores de serviços terceiros, contribuindo para reduzir os riscos de exposição, utilização indevida ou violação de dados.

1.3. A presente política suporta diretamente o cumprimento dos requisitos de certificação ISO/IEC 27001:2022, bem como de obrigações regulamentares europeias, incluindo o RGPD da UE, a Diretiva NIS2 da UE e a DORA da UE.

1.4. Ao transformar os dados antes da sua utilização fora do contexto original de negócio, a organização limita a sua exposição a responsabilidades e reforça a capacidade de demonstrar diligência devida em matéria de privacidade e segurança.

2. Âmbito

2.1. A presente política aplica-se a todos os dados estruturados ou não estruturados classificados como pessoais, confidenciais ou sensíveis, quer sejam armazenados ou tratados:

2.1.1. Em ambientes de produção, teste ou desenvolvimento

2.1.2. Em dispositivos locais, servidores ou plataformas na nuvem

2.1.3. Por pessoal interno, contratados ou prestadores de serviços terceiros

2.2. Abrange igualmente todas as ferramentas de transformação de dados (mascaramento, tokenização, pseudonimização), sejam de código aberto, comerciais ou desenvolvidas internamente.

2.3. Os casos de utilização abrangidos por esta política incluem:

2.3.1. Preparação de conjuntos de dados para teste ou desenvolvimento

2.3.2. Exportação de dados para sistemas de análise

2.3.3. Acesso de fornecedores ou consultores a sistemas operacionais

2.3.4. Minimização de dados pessoais do titular dos dados para reduzir o risco de tratamento

3. Objetivos

3.1. Assegurar que dados pessoais ou sensíveis reais nunca sejam expostos em ambientes com menor nível de segurança quando tal não seja essencial.

3.2. Tornar obrigatória a utilização de técnicas de mascaramento ou pseudonimização sempre que identificadores reais não sejam estritamente necessários para a execução da tarefa.

3.3. Prevenir o acesso não autorizado ou a utilização indevida de dados, impondo controlos de transformação antes da transferência ou do tratamento dos dados.

3.4. Garantir que todos os processos de mascaramento e pseudonimização sejam rastreáveis, auditáveis e executados através de ferramentas aprovadas.

3.5. Cumprir as normas legais e regulamentares aplicáveis que exijam minimização de dados, confidencialidade e salvaguardas de transformação.

4. Papéis e responsabilidades

4.1. Diretor-Geral (GM)

4.1.1. É o responsável por esta política e aprova-a

4.1.2. Assegura que todos os departamentos e prestadores cumprem os requisitos de transformação

4.1.3. Revê exceções, avaliações de risco e registos de transformação

4.1.4. Coordena ações jurídicas, operacionais ou dirigidas a fornecedores em caso de violações

4.2. Prestador de suporte de TI / TI interna

4.2.1. Seleciona e gere as ferramentas de mascaramento ou pseudonimização

4.2.2. Assegura a aplicação de métodos de transformação adequados com base no tipo de dados

4.2.3. Mantém registos dos conjuntos de dados transformados e dos procedimentos de gestão de chaves

4.2.4. Assegura que o mascaramento ocorre antes da utilização para testes, por fornecedores ou para análise de dados

[... 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. A presente política deve ser revista pelo menos uma vez por ano pelo Diretor-Geral (GM), para assegurar que reflete:

9.1.1.1. Atualizações da regulamentação aplicável (por exemplo, RGPD da UE, DORA da UE)

9.1.1.2. Novos sistemas de negócio ou trocas de dados com terceiros

9.1.1.3. Conclusões de auditorias ou incidentes que envolvam utilização de dados sem mascaramento

9.2. Revisões intercalares

9.2.1. Devem igualmente ocorrer revisões quando:

9.2.1.1. São introduzidas novas aplicações ou plataformas que tratem dados sensíveis

9.2.1.2. Um incidente grave revele lacunas nos controlos de transformação em vigor

9.2.1.3. Alterações nos níveis de classificação afetem os procedimentos de tratamento de dados

9.3. Controlo de versões e gestão de alterações

9.3.1. Todas as alterações às políticas devem:

9.3.1.1. Ser aprovadas pelo Diretor-Geral (GM) e documentadas num registo de alterações

9.3.1.2. Ser claramente comunicadas aos trabalhadores e prestadores de serviços afetados

9.3.1.3. Ser arquivadas de forma segura, com acesso restrito a versões desatualizadas

10. Políticas relacionadas e interligações

10.1. A presente política deve ser aplicada em conjunto com as seguintes políticas SME, para assegurar uma proteção consistente e obrigatória dos dados sensíveis:

10.1.1. P13S – Política de Classificação e Rotulagem de Dados: Define os níveis de classificação (por exemplo, Confidencial – Pessoal) que determinam quando o mascaramento ou a pseudonimização devem ser aplicados. Esta política estabelece regras de transformação com base nos níveis de sensibilidade dos dados.

10.1.2. P14S – Política de Retenção e Eliminação de Dados: Assegura que os conjuntos de dados transformados, incluindo cópias de segurança que contenham dados mascarados ou pseudonimizados, são retidos e eliminados de acordo com as regras aplicáveis, incluindo a eliminação das chaves de correspondência quando deixem de ser necessárias.

10.1.3. P17S – Política de Proteção de Dados e Privacidade: Alinha as práticas de transformação com obrigações de privacidade mais amplas, incluindo requisitos do RGPD da UE relativos à minimização de dados e à utilização da pseudonimização como salvaguarda para o tratamento de dados pessoais.

10.1.4. P30S – Política de Resposta a Incidentes: Abrange os procedimentos de comunicação e escalonamento em caso de divulgação não autorizada de dados, incluindo utilização indevida ou reversão de dados mascarados ou pseudonimizados.

10.1.5. P2S – Política de Papéis e Responsabilidades de Governação: Atribui a responsabilização global pela implementação da política, aceitação do risco e aprovação de exceções, principalmente ao Diretor-Geral (GM).

10.2. Estas políticas formam um quadro integrado de proteção de dados, assegurando que os esforços de mascaramento e pseudonimização suportam a certificação ISO 27001 e o cumprimento regulamentar transversal.

11. Normas e quadros de referência

11.1. ISO/IEC 27001

11.1.1. Cláusula 6.1.3: Exige o tratamento dos riscos de segurança da informação, incluindo a mitigação da exposição através de técnicas de transformação de dados.

11.1.2. Cláusula 8.1: Exige a implementação dos controlos necessários para cumprir os objetivos de segurança, incluindo pseudonimização e mascaramento.

11.2. ISO/IEC 27002

11.2.1. Controlo 8.11: Fornece orientações sobre o mascaramento de dados sensíveis em sistemas de teste e desenvolvimento.

11.2.2. Controlo 8.12: Apresenta estratégias para prevenir fugas de dados através de práticas controladas de transformação e acesso.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Assegura a confidencialidade da informação através da ofuscação de dados.

11.3.2. SC-28: Protege a informação em repouso e em utilização.

11.3.3. PT-2/PT-3: Promovem a utilização de tecnologias de reforço da privacidade, incluindo a pseudonimização, no tratamento de informações de identificação pessoal.

11.4. RGPD da UE

11.4.1. Artigo 4(5): Define juridicamente a pseudonimização e exige controlos sobre chaves de correspondência e identificadores.

11.4.2. Artigo 5(1)(c): Sustenta os princípios de minimização de dados através do mascaramento.

11.4.3. Artigo 32: Reconhece a pseudonimização como um controlo técnico que reduz os riscos de privacidade.

11.5. Diretiva NIS2 da UE

11.5.1. Artigo 21(2)(c): Exige medidas técnicas proporcionadas para minimizar o risco de segurança dos dados, incluindo a pseudonimização como parte do controlo do risco.

11.6. DORA da UE

11.6.1. Artigo 10(1): Exige controlos de risco relacionados com as TIC que incluam salvaguardas de transformação de dados para continuidade e confidencialidade durante a subcontratação e o desenvolvimento de sistemas.

11.7. COBIT 2019

11.7.1. DSS05.01: Exige a proteção dos ativos de informação, incluindo transformação sempre que possível.

11.7.2. DSS06.06: Requer técnicas adequadas de ofuscação e pseudonimização para limitar a exposição de dados em ambientes de menor confiança.