					Insira aqui a designação da entidade jurídica registada							
Número do documento: P13S					Título do documento: **Política de Classificação e Rotulagem 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 5.3, 8	
ISO/IEC 27002:2022	Controlos 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Diretiva NIS2 da UE	Artigo 21(2)(a)	
DORA da UE	Artigo 5(8)	
COBIT 2019	BAI03.05, DSS05.02	
RGPD da UE	Artigos 5, 32	

1. Finalidade

1.1 Esta política define como toda a informação tratada pela organização deve ser classificada e rotulada, para garantir que a sua Confidencialidade, Integridade e Disponibilidade são mantidas ao longo do respetivo ciclo de vida.

1.2 Esta política assegura um tratamento de dados consistente, mediante a atribuição de níveis de proteção adequados à informação, com base na sua sensibilidade, impacto no negócio ou obrigações legais.

1.3 A classificação e a rotulagem ajudam a reduzir o risco de divulgação acidental, acesso não autorizado ou tratamento inadequado de dados sensíveis, em especial em PME que possam depender de sistemas mais simples e de controlos menos formalizados.

1.4 Esta política é crítica para a certificação ISO/IEC 27001 e para a conformidade regulamentar, em particular no âmbito da legislação de proteção de dados, como o RGPD da UE, e de referenciais de cibersegurança, como a Diretiva NIS2 da UE e o DORA da UE.

2. Âmbito

2.1 Esta política aplica-se a todos os dados da organização, independentemente do formato ou da localização, incluindo:

2.1.1 Documentos eletrónicos, folhas de cálculo, mensagens de correio eletrónico, formulários, imagens e ficheiros digitalizados

2.1.2 Documentos físicos, tais como registos impressos, relatórios, faturas e notas

2.1.3 Dados armazenados ou tratados em serviços na nuvem, em servidores locais, suportes amovíveis ou dispositivos pessoais utilizados para fins profissionais

2.1.4 Dados temporários ou transitórios gerados durante as operações do negócio (por exemplo, registos, ficheiros de cache, mensagens de correio eletrónico)

2.2 Todo o pessoal, contratados, trabalhadores temporários e prestadores de serviços externos com acesso aos dados da organização devem cumprir esta política.

2.3 Esta política aplica-se a todo o ciclo de vida dos dados — desde a criação e armazenamento, passando pelo acesso e transferência, até ao arquivo ou eliminação.

3. Objetivos

3.1 Definir um esquema de classificação simples e aplicável, que possa ser facilmente compreendido e utilizado em toda a organização.

3.2 Exigir que cada ativo de dados seja classificado de acordo com a sua sensibilidade e rotulado em conformidade, para orientar o respetivo tratamento, armazenamento e acesso.

3.3 Assegurar que as práticas de rotulagem de dados são integradas nos fluxos de trabalho do negócio, como a integração de colaboradores, o arranque de projetos e a configuração de sistemas.

3.4 Reduzir o risco de violações de dados através da aplicação de controlos de tratamento adequados ao nível de classificação (por exemplo, cifragem, restrição de acesso).

3.5 Assegurar a conformidade com a legislação de privacidade e segurança da informação, demonstrando que os dados sensíveis (por exemplo, pessoais, financeiros ou proprietários) estão devidamente rotulados e geridos.

3.6 Estabelecer a responsabilização pelas decisões de classificação e assegurar revisões e atualizações periódicas com base na evolução das necessidades do negócio e dos requisitos legais.

4. Papéis e responsabilidades

4.1 Diretor-Geral (DG)

4.1.1 É o responsável por esta política e aprova o esquema de classificação.

4.1.2 Exerce supervisão para assegurar que as responsabilidades de classificação são delegadas e cumpridas.

4.1.3 Deve rever e autorizar quaisquer exceções aos requisitos de classificação ou rotulagem.

4.1.4 Assegura que as práticas de tratamento de dados cumprem os requisitos legais aplicáveis, incluindo o RGPD da UE e o DORA da UE.

4.2 Proprietário da informação / Gestor de dados

4.2.1 Atribui uma classificação inicial a cada novo conjunto de dados ou ativo de informação no momento da sua criação ou aquisição.

4.2.2 Assegura a aplicação de rótulos visíveis, quando aplicável (por exemplo, cabeçalhos, rodapés, marcas de água, nomes de pastas).

4.2.3 Revê periodicamente as classificações para verificar a sua relevância, exatidão e eventuais alterações necessárias (por exemplo, após desclassificação ou publicação).

4.2.4 Trabalha com o Responsável de TI para aplicar proteções técnicas com base na classificação (por exemplo, direitos de acesso, cifragem).

[... 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 DG e pelo Gestor de dados para assegurar que reflete:

9.1.1 Alterações nas operações do negócio ou nos tipos de dados

9.1.2 Novos requisitos regulamentares (por exemplo, privacidade de dados ou supervisão financeira)

9.1.3 Evoluções tecnológicas que afetem as capacidades de rotulagem ou classificação

9.2 A revisão deve incluir atualizações às categorias de classificação, às ferramentas ou práticas de rotulagem e ao conteúdo de sensibilização e formação.

9.3 As revisões da política devem ser aprovadas pelo DG e comunicadas a todo o pessoal. Deve ser mantido um registo de versões para efeitos de auditoria.

10. Políticas relacionadas e articulações

10.1 P2S – Política de Papéis e Responsabilidades de Governação: Atribui a responsabilização pela titularidade e aplicação das políticas.

10.2 P4S – Política de Controlo de Acesso: Alinha o acesso aos sistemas com os níveis de classificação dos dados.

10.3 P12S – Política de Gestão de Ativos: Permite acompanhar os ativos físicos e digitais que armazenam dados classificados.

10.4 P17S – Política de Proteção de Dados e Privacidade: Regula a proteção dos dados pessoais, muitos dos quais são classificados como Confidenciais.

10.5 P30S – Política de Resposta a Incidentes: Define as vias de escalonamento e os procedimentos de resposta em caso de violações de classificação ou exposição de dados.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.3: Exige responsabilidades claramente definidas para o tratamento e a proteção de dados.

11.1.2 Cláusula 8.1: Exige planeamento e controlos operacionais, incluindo os associados à categorização de dados.

11.2 ISO/IEC 27002

11.2.1 Controlo 5.12: Fornece orientações sobre a classificação da informação com base no risco e nos requisitos regulamentares.

11.2.2 Controlo 5.13: Detalha mecanismos práticos de rotulagem e regras de tratamento associadas.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: Exige a marcação da informação para assegurar que as medidas de proteção estão alinhadas com a classificação.

11.3.2 MP-3 / MP-5: Fornecem orientações sobre a rotulagem e o controlo de suportes e saídas.

11.4 RGPD da UE

11.4.1 Artigos 5 e 32: Exigem minimização de dados e integridade através de salvaguardas adequadas de classificação e tratamento.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(a): Exige controlos técnicos e organizativos para a proteção de dados com base no risco.

11.6 DORA da UE

11.6.1 Artigo 5(8): Exige que as entidades classifiquem os ativos de dados como parte do respetivo programa de gestão do risco das TIC.

11.7 COBIT 2019

11.7.1 BAI03.05: Requer a classificação da informação e proteção ajustada ao risco.

11.7.2 DSS05.02: Abrange a aplicação de controlos baseados na classificação e a respetiva monitorização.