					Insira aqui a designação da entidade jurídica registada							
Número do documento: P13					Título do documento: **Política de Classificação e Rotulagem da Informação**							
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**

1. Finalidade

1.1 Esta política define o quadro formal para a classificação e rotulagem dos ativos de informação da organização com base na sua sensibilidade, exposição ao risco e obrigações regulamentares.

1.2 Assegura que toda a informação, quer esteja armazenada, em transmissão ou em tratamento, é claramente categorizada e rotulada de modo a comunicar o nível de proteção e os requisitos de tratamento aplicáveis.

1.3 Esta política impõe uma classificação estruturada, alinhada com as práticas de gestão de risco da organização, suportando os objetivos de Confidencialidade, Integridade e Disponibilidade da informação em formato digital e físico.

1.4 Este controlo é essencial para viabilizar o controlo de acesso baseado em funções, a demonstração de conformidade em auditoria, a partilha adequada de dados e a implementação eficaz de salvaguardas técnicas, como cifragem, cópias de segurança e monitorização.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os ativos de informação da organização, incluindo documentos, bases de dados, registos e comunicações

2.1.2 Todos os formatos de dados, incluindo digital, impresso, escrito ou verbal

2.1.3 Todos os ambientes: local, remoto, móvel e na nuvem

2.1.4 Todos os trabalhadores, prestadores de serviços, fornecedores e subcontratantes terceiros que criem, tratem ou armazenem informação da organização

2.2 O âmbito abrange conteúdos desenvolvidos internamente, dados obtidos externamente, dados pessoais sujeitos a obrigações legais de privacidade (por exemplo, RGPD da UE) e informação trocada com clientes, parceiros e reguladores.

2.3 Aplica-se a todos os sistemas utilizados para armazenar ou transmitir dados, incluindo aplicações empresariais, servidores de ficheiros, sistemas de correio eletrónico, plataformas na nuvem e repositórios de cópias de segurança.

3. Objetivos

3.1 Estabelecer um esquema de classificação normalizado, aplicável a toda a organização, com base no impacto da exposição ou comprometimento dos dados.

3.2 Assegurar que toda a informação é rotulada de forma visível e persistente para refletir o seu nível de classificação e os requisitos de tratamento aplicáveis.

3.3 Impor controlos de tratamento de dados e de acesso alinhados com a classificação, incluindo cifragem, registos, proteção da transmissão e calendarização da retenção.

3.4 Apoiar a conformidade com normas internacionais (ISO/IEC 27001, 27002), enquadramentos legais (RGPD da UE, Diretiva NIS2 da UE, DORA da UE) e políticas internas de risco.

3.5 Assegurar que todos os utilizadores compreendem as suas responsabilidades na proteção de dados, na aplicação de rótulos e no tratamento correto de informação classificada.

3.6 Manter a rastreabilidade entre o estado de classificação, os controlos associados e o inventário de ativos da organização para efeitos de auditoria e conformidade.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável pela política de classificação e rotulagem da informação e assegura o seu alinhamento com os requisitos regulamentares, contratuais e operacionais.

4.1.2 Aprova os níveis de classificação, as normas de rotulagem e as revisões da política.

4.1.3 Supervisiona o cumprimento da política através de auditorias, métricas e revisões de exceções.

4.1.4 Coordena a governação transversal com as equipas Jurídica, de Proteção de Dados e de Risco.

4.2 Proprietários da informação

4.2.1 São responsáveis por classificar os ativos de informação sob o seu controlo, utilizando o esquema de classificação da organização.

4.2.2 Aplicam os rótulos de classificação no momento da criação, atualização ou receção.

4.2.3 Revêm periodicamente a classificação dos ativos, em especial em resposta a alterações de sensibilidade, âmbito regulamentar ou valor para o negócio.

4.2.4 Asseguram que os dados sensíveis são tratados e rotulados de forma adequada ao longo de todo o seu ciclo de vida.

[... 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, pelo menos, anualmente para assegurar o alinhamento com:

9.1.1 Requisitos regulamentares em evolução (por exemplo, RGPD da UE, Diretiva NIS2 da UE, DORA da UE)

9.1.2 Atualizações das orientações de classificação da ISO/IEC 27001 ou 27002

9.1.3 Alterações organizacionais com impacto na sensibilidade ou titularidade dos dados

9.1.4 Alterações tecnológicas, incluindo novas plataformas de gestão documental ou de dados

9.2 O Diretor de Segurança da Informação (CISO) deve iniciar a revisão em colaboração com o Comité de Segurança da Informação, a assessoria jurídica e as unidades de negócio afetadas.

9.3 As revisões devem incluir:

9.3.1 A eficácia da imposição da classificação e a adesão dos utilizadores

9.3.2 Análise de incidentes ou exceções associados a classificação incorreta

9.3.3 Feedback dos utilizadores sobre ferramentas de rotulagem ou materiais de orientação

9.3.4 Benchmarking face a normas de classificação do setor

9.4 As atualizações da política devem estar sujeitas a controlo de versões, ser documentadas no repositório do SGSI e comunicadas a todo o pessoal relevante, com destaque para novas responsabilidades ou alterações de ferramentas.

9.5 As novas admissões devem tomar conhecimento da versão atual da política durante o processo de integração. Todos os trabalhadores devem concluir formação de reciclagem após alterações materiais à política.

10. Políticas relacionadas e ligações

10.1 Esta política é diretamente suportada por, e concretiza controlos descritos nas seguintes políticas relacionadas:

10.1.1 P4 - Política de controlo de acesso: O acesso à informação é regido por níveis de classificação; dados mais sensíveis exigem mecanismos de controlo de acesso e de autorização mais rigorosos.

10.1.2 P11 - Política de Gestão de Contas de Utilizador e Privilégios: Reforça a atribuição de privilégios com base no princípio da necessidade de conhecer, informado pelos níveis de classificação.

10.1.3 P12 - Política de Gestão de Ativos: Assegura que cada ativo no inventário inclui a sua classificação e rótulo, suportando rastreabilidade e responsabilização.

10.1.4 P14 - Política de Retenção e Eliminação de Dados: As regras de retenção e eliminação são determinadas pelo nível de classificação dos dados e pelos requisitos regulamentares de retenção.

10.1.5 P18 - Política de Controlos Criptográficos: Aplica normas de cifragem adequadas com base na classificação do ativo de informação.

10.1.6 P22 - Política de Registo e Monitorização: Permite a monitorização do acesso e da movimentação de informação classificada, assegurando auditabilidade e deteção de rotulagem incorreta ou utilização indevida.

10.2 Cada ligação assegura a proteção coerente da informação ao longo do seu ciclo de vida, desde a criação e classificação até ao tratamento seguro, armazenamento, transmissão e destruição final.

11. Normas e quadros de referência

11.1 Esta política está alinhada com normas internacionalmente reconhecidas e enquadramentos regulamentares aplicáveis à classificação e rotulagem de informação sensível.

11.2 ISO/IEC 27001

11.2.1 Cláusula 4.2 - Compreender as necessidades e expectativas das partes interessadas. Os requisitos de classificação decorrem frequentemente de obrigações legais, regulamentares ou contratuais impostas por partes interessadas (por exemplo, RGPD da UE, acordos de confidencialidade com clientes), que devem refletir-se na política.

11.2.2 Cláusula 6.1.3 - Tratamento de riscos de segurança da informação. A classificação afeta diretamente a seleção de controlos de tratamento de riscos, incluindo controlo de acesso, cifragem e retenção, com base na sensibilidade dos dados.

11.2.3 Cláusula 7.2 - Competência. A política determina que o pessoal responsável pela classificação e rotulagem deve receber formação, o que se enquadra nos requisitos de competência.

11.2.4 Cláusula 7.3 - Sensibilização. A política exige que todos os utilizadores conheçam os níveis de classificação e as suas responsabilidades no tratamento da informação, em alinhamento com as obrigações de sensibilização.

11.2.5 Cláusula 7.5 - Informação documentada. A própria política de classificação é um documento controlado, e os procedimentos, registos de formação e rótulos de classificação fazem parte da informação documentada.

11.2.6 Cláusula 8.1 - Planeamento e controlo operacional. A classificação e a rotulagem são processos operacionais incorporados na gestão do ciclo de vida dos dados, e esta cláusula assegura que essas atividades são planeadas, implementadas e controladas.

11.2.7 Cláusula 9.1 - Monitorização, medição, análise e avaliação. A política inclui disposições para monitorização do cumprimento da classificação, tendências de incidentes e eficácia do esquema de rotulagem.

11.2.8 Cláusula 10.1 - Não conformidade e ação corretiva. A política define respostas a classificações incorretas, incluindo ações corretivas como formação adicional, atualizações e tratamento de exceções.

11.3 ISO/IEC 27002:2022

11.3.1 Controlo 5.12 - Classificação da informação. Este controlo assegura que a informação é classificada com base na sua sensibilidade, valor e criticidade, precisamente o que esta política formaliza.

11.3.2 Controlo 5.13 - Rotulagem da informação. Este controlo exige a rotulagem adequada da informação de acordo com o respetivo nível de classificação, plenamente tratada nesta política.

11.3.3 Controlo 5.10 - Utilização aceitável da informação e de outros ativos associados. A política impõe a forma como os utilizadores devem tratar dados classificados, suportando diretamente a utilização aceitável e prevenindo o uso indevido.

11.3.4 Controlo 5.11 - Devolução de ativos. A classificação ajuda a assegurar que os dados sensíveis são identificados e devolvidos ou sujeitos a sanitização de dados de forma segura quando um trabalhador ou fornecedor cessa funções.

11.3.5 Controlo 5.9 - Inventário da informação e de outros ativos associados. A classificação está frequentemente associada ao inventário de ativos, o qual deve refletir o nível de classificação de cada item para suportar a atribuição adequada de controlos.

11.3.6 Controlo 5.14 - Transferência de informação. Os níveis de classificação influenciam os controlos sobre transferências internas e externas de dados (por exemplo, cifragem, aprovação, restrições de acesso).

11.3.7 Controlo 8.12 - Prevenção de fuga de dados. A imposição da classificação e da rotulagem apoia a prevenção da divulgação não autorizada e da perda de dados.

11.3.8 Controlo 8.11 - Mascaramento de dados. Determinados níveis de classificação (por exemplo, Confidencial, Restrito) podem exigir mascaramento quando os dados são utilizados em ambientes de teste e desenvolvimento ou em análises.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Política e procedimentos de proteção de sistemas e comunicações: Suporta políticas de classificação como parte da proteção global dos dados.

11.4.2 AC-16 - Atributos de segurança: Implementa a imposição de acesso com base em metadados de classificação e permissões do utilizador.

11.4.3 MP-3 / MP-5 - Marcação de suportes e proteção no transporte: Impõe a rotulagem e a proteção de dados em repouso e em trânsito com base na classificação.

11.5 RGPD da UE (2016/679)

11.5.1 Artigo 5 - Princípios da proteção de dados: Exige que os dados pessoais sejam tratados de forma segura e proporcional à sua sensibilidade.

11.5.2 Artigo 32 - Segurança do tratamento: Reforça a classificação como mecanismo de proteção de dados baseado no risco e de aplicação de medidas técnicas adequadas.

11.6 Diretiva NIS2 da UE (2022/2555)

11.6.1 Artigo 21(2)(a): Exige políticas de gestão de riscos de segurança da informação, incluindo controlos de classificação de ativos e dados.

11.6.2 Artigo 21(3): Incentiva a adoção de medidas que imponham o tratamento adequado dos dados, suportado por rotulagem baseada em classificação.

11.7 DORA da UE (2022/2554)

11.7.1 Artigo 5 - Governação e controlo: Exige quadros de governação que classifiquem ativos de dados para controlo do risco das TIC.

11.7.2 Artigo 9 - Gestão do risco das TIC: Impõe medidas técnicas e organizativas para ativos críticos de TIC, incluindo classificação e rotulagem.

11.8 COBIT 2019

11.8.1 DSS05.02 - Gerir serviços de segurança: Impõe classificações de segurança da informação para assegurar a proteção dos dados empresariais.

11.8.2 MEA03 - Monitorizar, avaliar e analisar a conformidade: Suporta auditoria e revisão regulares das práticas de classificação para assegurar o cumprimento da política e a maturidade.