					Insira aqui a designação da entidade jurídica registada							
Número do documento: P12					Título do documento: **Política de Gestão de Ativos**							
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 os requisitos organizacionais obrigatórios para identificar, classificar, gerir e proteger os ativos de informação ao longo do respetivo ciclo de vida. Suporta a governação transversal dos ativos de hardware, software, dados, cloud e ativos de informação intangíveis, incluindo ambientes móveis, remotos e geridos por terceiros.

1.2 A finalidade desta política é assegurar visibilidade completa sobre o panorama de ativos de informação da organização, permitindo a aplicação eficaz de controlos de segurança, a atribuição de propriedade, o alinhamento com requisitos de conformidade e o descomissionamento ou a eliminação responsável.

1.3 A política está alinhada com o Anexo A.5.9 da ISO/IEC 27001:2022, ao exigir a manutenção de um inventário centralizado da informação e dos ativos associados. Assegura a responsabilização ao associar cada ativo a um proprietário e ao aplicar proteção orientada pela classificação, com base na sensibilidade para o negócio e nos requisitos regulamentares.

2. Âmbito

2.1 Esta política aplica-se a todos os trabalhadores, prestadores de serviços, terceiros e prestadores de serviços geridos que gerem, utilizem, acedam, armazenem ou tratem ativos de informação detidos ou controlados pela organização.

2.2 O âmbito inclui todas as categorias de ativos, tais como:

2.2.1 Ativos físicos: computadores portáteis, computadores de secretária, dispositivos móveis, suportes amovíveis, impressoras, equipamentos de rede

2.2.2 Ativos digitais: software, aplicações, imagens de sistema, bases de dados, dados de cópias de segurança, chaves de cifragem

2.2.3 Ativos de informação: dados estruturados e não estruturados, relatórios, mensagens de correio eletrónico, propriedade intelectual

2.2.4 Ativos cloud e virtuais: ambientes IaaS, SaaS e PaaS, máquinas virtuais, contentores

2.2.5 Ativos lógicos: nomes de domínio, licenças, contas de utilizador, configurações de referência

2.3 A política rege igualmente os ativos utilizados em contextos de trabalho remoto, híbrido ou externalizado, assegurando proteção e visibilidade mesmo quando os ativos não se encontrem fisicamente nas instalações da organização.

3. Objetivos

3.1 Manter um inventário completo, exato e atualizado de todos os ativos de informação da organização, com atributos de propriedade, classificação e localização definidos.

3.2 Atribuir proprietários de ativos responsáveis pela classificação, tratamento e proteção dos ativos sob o seu controlo, em conformidade com as políticas de governação de dados e de segurança.

3.3 Aplicar classificação e rotulagem adequadas a todos os ativos com base na sensibilidade, criticidade e requisitos regulamentares.

3.4 Proteger os ativos de acordo com a sua classificação e exposição ao risco associada, incluindo armazenamento, acesso, transmissão e eliminação.

3.5 Assegurar procedimentos de devolução de ativos e eliminação segura aquando da cessação da relação laboral, cessação contratual ou conclusão do ciclo de vida do ativo.

3.6 Apoiar a conformidade regulamentar com referenciais como a ISO/IEC 27001, o RGPD da UE, a Diretiva NIS2 da UE, o DORA da UE e o COBIT 2019 através de uma gestão estruturada de ativos e da rastreabilidade para efeitos de auditoria.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova a Política de Gestão de Ativos e assegura a afetação dos recursos necessários à sua implementação integral.

4.1.2 Assume a responsabilidade última por assegurar que os ativos da organização são protegidos e geridos em conformidade com as obrigações regulamentares e contratuais.

4.2 Diretor de Segurança da Informação (CISO)

4.2.1 É o responsável pela Política de Gestão de Ativos e assegura a sua integração com o Sistema de Gestão da Segurança da Informação (SGSI) da organização.

4.2.2 Revê exceções e desvios a esta política e assegura a aplicação de estratégias de mitigação baseadas no risco.

4.2.3 Supervisiona auditorias periódicas à classificação de ativos, à integridade do inventário e ao cumprimento do ciclo de vida dos ativos.

[... 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, ou em resposta a:

9.1.1 Alterações às obrigações legais ou regulamentares que afetem a classificação de ativos ou os requisitos de inventário

9.1.2 Introdução de novas categorias de ativos ou plataformas de gestão (por exemplo, CMDB nativas de cloud)

9.1.3 Constatações de auditoria interna ou incidentes de segurança que envolvam má gestão de ativos

9.1.4 Reestruturação organizacional que afete a propriedade ou os controlos do ciclo de vida

9.2 O processo de revisão deve ser iniciado pelo Gestor de Ativos de TI e coordenado com o Diretor de Segurança da Informação, a área de Aquisição, a área Jurídica e os responsáveis de departamento afetados.

9.3 As revisões intercalares também podem ser desencadeadas por:

9.3.1 Aquisição ou alienação de unidades de negócio

9.3.2 Alterações de fornecedores que afetem ativos geridos por terceiros

9.3.3 Renovações tecnológicas que envolvam descomissionamento ou provisionamento em massa

9.4 Todas as revisões a esta política devem:

9.4.1 Estar sujeitas a controlo de versões e ser armazenadas no repositório do SGSI

9.4.2 Ser aprovadas pela Alta Direção

9.4.3 Incluir um resumo das alterações e respetiva fundamentação

9.4.4 Ser comunicadas a todas as partes interessadas afetadas, incluindo procedimentos atualizados ou formação sobre sistemas, quando aplicável

10. Políticas relacionadas e articulações

10.1 Esta política funciona em conjunto com as seguintes políticas relacionadas e apoia a sua aplicação:

10.1.1 P4 - Política de Controlo de Acesso: Assegura que a visibilidade dos ativos está alinhada com os direitos de acesso e os mecanismos de controlo nos diversos sistemas e ambientes de dados.

10.1.2 P7 - Política de Admissão e Cessação: Rege o provisionamento atempado e a devolução de ativos físicos e lógicos durante as transições de pessoal.

10.1.3 P13 - Política de Classificação e Rotulagem de Dados: Estabelece regras obrigatórias de classificação para ativos, que determinam os procedimentos de rotulagem, tratamento e eliminação.

10.1.4 P14 - Política de Retenção e Eliminação de Dados: Define o calendário e os métodos de eliminação segura para ativos digitais e físicos que contenham informação.

10.1.5 P22 - Política de Registo e Monitorização: Permite a rastreabilidade do acesso e da utilização de ativos através de registos de sistemas, visibilidade de endpoints e análises comportamentais.

10.1.6 P30 - Política de Resposta a Incidentes (P30): Suporta a contenção rápida e a investigação de violações relacionadas com ativos, tais como computadores portáteis perdidos ou suportes de armazenamento sem rastreio.

10.2 Estas políticas formam uma estrutura de governação coesa que assegura que os ativos são geridos de forma segura, inventariados com exatidão e tratados adequadamente ao longo do respetivo ciclo de vida.

11. Normas e quadros de referência

11.1 Esta política está alinhada com normas de segurança da informação e referenciais regulamentares internacionalmente reconhecidos que exigem uma gestão robusta de ativos ao longo do ciclo de vida.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 8.1 - Exige que as organizações planeiem, implementem e controlem os processos necessários para cumprir os requisitos de segurança da informação, incluindo os relativos à gestão do ciclo de vida dos ativos.

11.3 ISO/IEC 27002:2022 - Controlos 5.9 a 5.11

11.3.1 Cláusula 5.9 - Inventário da Informação e de Outros Ativos Associados: Exige um inventário atualizado e completo de todos os ativos relevantes para o tratamento da informação.

11.3.2 Cláusula 5.10 - Utilização Aceitável da Informação e dos Ativos: Suportada por regras de utilização, propriedade e processos de devolução.

11.3.3 Cláusula 5.11 - Devolução de Ativos: Implementada através de procedimentos formais de entrega e descomissionamento.

11.3.4 Estes controlos estabelecem requisitos estruturados para identificar, rotular, manter e acompanhar os ativos da organização, com responsabilidades correspondentes para proprietários e custodiante ao longo do ciclo de vida.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Inventário de Componentes do Sistema: Refletido através da gestão centralizada de ativos, visibilidade em tempo real e ligação às configurações operacionais.

11.4.2 RA-3 - Avaliação de Riscos: Os inventários de ativos constituem elementos fundamentais para a modelação de ameaças e a avaliação de riscos.

11.4.3 MP-6 - Sanitização de suportes: Aplicada através de métodos de eliminação segura definidos nos controlos do ciclo de vida dos ativos e na Política de Eliminação de Dados.

11.5 RGPD da UE (2016/679):

11.5.1 Artigo 30 - Registos das atividades de tratamento: Exige que as organizações documentem sistemas, dispositivos e repositórios que armazenem ou tratem dados pessoais.

11.5.2 Artigo 32 - Segurança do Tratamento: Alinha-se com a avaliação de riscos baseada em ativos e com salvaguardas adequadas a ativos classificados e infraestruturas críticas.

11.6 Diretiva NIS2 da UE (2022/2555):

11.6.1 Artigo 21(2)(a, b): Exige visibilidade e inventário de ativos como base da análise de riscos, da proteção e da resposta a incidentes de cibersegurança.

11.6.2 Artigo 21(3): Reforça a necessidade de uma governação estruturada de ativos como parte integrante da cultura de segurança da organização.

11.7 DORA da UE (2022/2554):

11.7.1 Artigo 5 - Governação das TIC e controlo interno: Exige que as entidades financeiras controlem os ativos de TIC com requisitos claros de inventário, propriedade e proteção.

11.7.2 Artigo 9 - Quadro de gestão do risco das TIC: Estabelece que os processos de gestão de ativos devem suportar a mitigação de ameaças, o planeamento da continuidade e a resiliência dos serviços.

11.8 COBIT 2019:

11.8.1 BAI09 - Gerir Ativos: Diretamente alinhado com a identificação, classificação, utilização e eliminação estruturadas dos ativos empresariais.

11.8.2 DSS01 - Operações Geridas: Suporta a implementação de controlos que asseguram a proteção dos ativos e a governação operacional contínua.

11.8.3 MEA03 - Monitorizar, Avaliar e Analisar a Conformidade: Assegura a auditoria regular dos controlos de gestão de ativos e da sua eficácia no alinhamento regulamentar.