| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insira aqui a designação da entidade jurídica registada | | | | | | | |
| Número do documento:<br>P12S | | | | | Título do documento:<br>**Política de Gestão de Ativos** | | | | | | | |
| Versão:<br>1.0 | | Data de entrada em vigor:<br>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 | Requisitos de gestão de ativos |
| ISO/IEC 27002:2022 | Controlo 5 | Controlos de gestão de ativos |
| NIST SP 800-53 Rev.5 | CM-8 | Inventário de ativos e componentes do sistema |
| Diretiva NIS2 da UE | Artigo 21(2)(a) | Inventário e acompanhamento de ativos para proteção dos sistemas de rede e informação |
| DORA da UE | Artigo 5(8) | Requisitos de inventário de ativos de TIC |
| COBIT 2019 | BAI | Gestão do ciclo de vida dos ativos de TI |
| RGPD da UE | Artigo 30 | Inventário das atividades de tratamento de dados |

## 1. Finalidade

1.1 Esta política define a forma como a organização identifica, inventaria, protege e retira de serviço os seus ativos de informação, incluindo componentes físicos e digitais.

1.2 O objetivo é reduzir os riscos operacionais e de segurança, assegurando visibilidade, responsabilização e tratamento seguro de todos os ativos da organização ao longo do respetivo ciclo de vida.

1.3 Um inventário de ativos fiável apoia o cumprimento regulamentar, a resposta a incidentes, o planeamento da continuidade e a gestão de riscos.

1.4 Esta política apoia igualmente a certificação ao abrigo da ISO/IEC 27001 e demonstra alinhamento com obrigações legais, financeiras e de cibersegurança ao abrigo de quadros como o RGPD da UE, a Diretiva NIS2 da UE e o DORA da UE.

1.5 Para pequenas e médias empresas (PME), uma abordagem simples, mas sistemática, à gestão de ativos é essencial para evitar dispositivos não geridos, perda de dados ou não conformidades de auditoria, especialmente quando operam com recursos técnicos limitados.

## 2. Âmbito

**2.1 Esta política aplica-se a todos os ativos detidos, alugados ou de qualquer outra forma geridos pela organização, incluindo os utilizados em:**

2.1.1 Trabalho em escritório

2.1.2 Regimes de trabalho remoto ou híbrido

2.1.3 Operações no terreno ou móveis

2.1.4 Ambientes cloud e externalizados

**2.2 Os tipos de ativos abrangidos incluem, entre outros:**

2.2.1 Hardware: computadores portáteis, computadores de secretária, monitores, telefones, tablets, unidades USB, routers, impressoras e suportes de cópia de segurança

2.2.2 Software: aplicações instaladas, ferramentas SaaS, sistemas operativos, ferramentas antivírus e licenças

2.2.3 Ativos de dados: repositórios de dados da organização, folhas de cálculo, registos de clientes e código-fonte

2.2.4 Credenciais e serviços digitais: nomes de domínio, certificados digitais, chaves de API, contas de correio eletrónico e credenciais de acesso à cloud

2.2.5 Dispositivos de acesso: chaves, cartões inteligentes, comandos de acesso e tokens biométricos

2.3 Todos os trabalhadores, prestadores de serviços e terceiros que tratem ativos da organização estão abrangidos pelo âmbito desta política.

2.4 A política rege igualmente ativos de curto prazo (por exemplo, computadores portáteis atribuídos a projetos específicos) e de longo prazo, bem como ativos partilhados utilizados por vários colaboradores.

**3. Objetivos**

3.1 Estabelecer e manter um inventário de ativos completo e exato de todos os ativos relevantes, continuamente atualizado.

3.2 Assegurar que cada ativo tem um proprietário designado responsável pela sua utilização, armazenamento e devolução.

3.3 Classificar os ativos com base na sensibilidade, no impacto no negócio ou na relevância regulamentar, permitindo níveis de proteção diferenciados.

3.4 Definir procedimentos claros para atribuição, reafetação, manutenção, comunicação de perda e retirada de serviço de ativos.

3.5 Assegurar que os ativos são tratados de forma segura ao longo do respetivo ciclo de vida e que a informação que armazenam é protegida ou sujeita a apagamento seguro aquando da eliminação.

3.6 Reduzir a probabilidade de incidentes de segurança causados por ativos organizacionais não rastreados, não devolvidos ou utilizados indevidamente.

3.7 Apoiar o cumprimento da legislação aplicável (por exemplo, o princípio da responsabilização do RGPD da UE) e das normas de certificação em cibersegurança.

**4. Papéis e responsabilidades**

**4.1 Diretor-Geral**

4.1.1 É responsável por esta política e por assegurar que as práticas de gestão de ativos são implementadas e cumpridas em toda a organização.

4.1.2 Revê e aprova atualizações ao inventário de ativos e autoriza a retirada de serviço ou a transferência de ativos, quando necessário.

4.1.3 Deve ser informado de qualquer perda, furto ou utilização indevida significativa de ativos.

**4.2 Responsável de TI ou fiel depositário de ativos designado**

4.2.1 Mantém o inventário de ativos (por exemplo, numa folha de cálculo, sistema de tickets do service desk ou ferramenta simplificada de inventário de ativos).

4.2.2 Atribui a propriedade dos ativos e acompanha alterações de estado (por exemplo, novo, em utilização, em reparação, retirado de serviço).

4.2.3 Verifica que todos os ativos atribuídos estão documentados e associados a uma pessoa ou unidade de negócio.

4.2.4 Assegura que os rótulos de classificação são aplicados e respeitados (por exemplo, Interno, Confidencial).

4.2.5 Coordena a recolha, a sanitização de dados e a desativação de ativos durante a cessação ou retirada de serviço.

4.2.6 Comunica ao Diretor-Geral quaisquer discrepâncias de ativos que permaneçam por resolver.

[ ... 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 uma vez por ano e sempre que:**

9.1.1 Sejam introduzidos novos tipos de tecnologia ou de ativos

9.1.2 Os procedimentos de acompanhamento de ativos sejam alterados (por exemplo, adoção de novas ferramentas ou plataformas)

9.1.3 Novas obrigações regulamentares afetem a rastreabilidade ou eliminação de ativos

9.1.4 Um incidente ou auditoria identifique uma lacuna nas práticas atuais de gestão de ativos

9.2 As revisões devem envolver o Diretor-Geral e o Responsável de TI e incluir atualizações aos procedimentos de tratamento de ativos, modelos de inventário e orientações de classificação.

9.3 Todas as atualizações devem ser documentadas e comunicadas ao pessoal afetado. Deve ser mantido um registo de alterações sujeito a controlo de versões.

**10. Políticas relacionadas e ligações**

10.1 P2S – Política de Papéis e Responsabilidades de Governação: atribui a responsabilização pela titularidade das políticas e pelas operações de TI.

10.2 P4S – Política de Controlo de Acesso: relaciona a utilização de ativos (por exemplo, computadores portáteis e dispositivos móveis) com os direitos de acesso dos utilizadores e a gestão de identidades.

10.3 P7S – Política de Admissão e Cessação: assegura que a atribuição e a recuperação de ativos estão integradas nos processos do ciclo de vida do pessoal.

10.4 P13S – Política de Classificação e Rotulagem de Dados: define regras para determinar se um ativo deve ser classificado como Interno ou Confidencial.

10.5 P30S – Política de Resposta a Incidentes: orienta os procedimentos de resposta quando um evento relacionado com ativos resulta numa violação de segurança ou de privacidade.

**11. Normas e quadros de referência**

**11.1 ISO/IEC 27001**

11.1.1 Cláusula 8.1: Exige controlos operacionais para gerir ativos e protegê-los ao longo da sua utilização.

**11.2 ISO/IEC 27002**

11.2.1 Controlo 5.9: Detalha como identificar, atribuir a propriedade, classificar e gerir ativos de forma segura.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 CM-8: Exige que as organizações desenvolvam e mantenham um inventário de componentes do sistema, incluindo hardware, software e ativos virtuais.

**11.4 RGPD da UE**

11.4.1 Artigo 30: Exige a documentação das atividades de tratamento de dados, o que depende de saber onde os dados estão armazenados e em que ativos.

**11.5 Diretiva NIS2 da UE**

11.5.1 Artigo 21(2)(a): Exige medidas técnicas e organizativas, incluindo o inventário e acompanhamento de ativos, para proteger os sistemas de rede e informação.

**11.6 DORA da UE**

11.6.1 Artigo 5(8): As entidades financeiras devem manter inventários detalhados de ativos de TIC como parte da gestão do risco das TIC.

**11.7 COBIT 2019**

11.7.1 BAI09: Especifica que os ativos de TI devem ser geridos ao longo de todo o seu ciclo de vida — desde a aquisição até à retirada de serviço — com propriedade e controlos claramente definidos.