| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insira aqui a designação da entidade jurídica registada | | | | | | | |
| Número do documento:<br>P07S | | | | | Título do documento:<br>**Política de Admissão e Cessação** | | | | | | | |
| 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 aplicáveis

| Norma/Regulamento | Cláusula/Artigo | Comentário |
|---|---|---|
| ISO/IEC 27001:2022 | Cláusulas 6.2, 7 | Requisitos de segurança de recursos humanos e sensibilização |
| ISO/IEC 27002:2022 | Controlos 6.2, 6.5 | Práticas de segurança para admissão e cessação |
| NIST SP 800-53 Rev.5 | PS-4, AC-2, PL-4 | Cessação de pessoal; ciclo de vida das contas; planeamento |
| Diretiva NIS2 da UE | Artigo 21(2)(h) | Segurança de recursos humanos e ciclo de vida dos acessos |
| DORA da UE | Artigo 12 | Controlos de acesso e revogação para sistemas TIC |
| COBIT 2019 | APO07, DSS01 | Segurança do pessoal, controlos de acesso lógico e físico |
| RGPD da UE | Artigo 32 | Segurança dos dados pessoais durante o vínculo laboral |

**1. Objetivo**

1.1 A presente política define o processo de admissão de novos trabalhadores ou prestadores de serviços e de remoção segura de acessos quando uma pessoa deixa a organização ou muda de função.

1.2 Assegura que os acessos são provisionados com base no princípio do menor privilégio, que todos os ativos são devidamente registados e que ações críticas, como a desativação de sistemas e a recuperação de dados, são concluídas atempadamente.

1.3 Esta política apoia a conformidade, a integridade operacional e a proteção de dados através de atividades estruturadas e auditáveis de admissão e cessação.

**2. Âmbito**

**2.1 Esta política aplica-se a:**

2.1.1 Todos os trabalhadores permanentes e temporários

2.1.2 Contratados, consultores e estagiários

2.1.3 Prestadores de serviços externos com acesso físico ou aos sistemas

**2.2 Abrange:**

2.2.1 Admissão: criação de contas de utilizador, concessão de acessos e entrega de equipamentos

2.2.2 Cessação: remoção de acessos, recuperação de ativos da empresa e encerramento seguro de identidades digitais

2.2.3 Alterações internas de função que exijam reconfiguração de acessos ou reafetação de ativos

2.3 Aplica-se a todos os dispositivos, plataformas e localizações utilizados no exercício de funções profissionais.

**3. Objetivos**

3.1 Assegurar que os novos colaboradores recebem acessos e recursos com base em funções e responsabilidades validadas.

3.2 Confirmar que os utilizadores em saída são totalmente removidos dos sistemas e das instalações até ao final do seu último dia de trabalho.

3.3 Prevenir a existência de contas sem proprietário identificado e de ativos não devolvidos, que constituem um risco de segurança.

3.4 Manter registos documentados das ações de admissão, transferências internas e cessação.

3.5 Promover a responsabilização através de listas de verificação e da coordenação entre áreas.

## 4. Papéis e responsabilidades

### 4.1 Diretor-Geral (GM)

4.1.1 Aprova acessos para funções com privilégios elevados e supervisiona o programa de admissão e cessação.

4.1.2 Assegura que as exceções são justificadas e que são adotadas ações corretivas quando os processos não são seguidos.

### 4.2 Responsável de escritório / Recursos Humanos

4.2.1 Inicia a admissão de novos colaboradores e notifica a TI sobre saídas.

4.2.2 Assegura a conclusão da documentação legal necessária (por exemplo, Acordo de Confidencialidade (NDA)) e das confirmações das políticas de segurança.

4.2.3 Mantém as listas de verificação de admissão e de cessação e monitoriza o cumprimento da política.

[ ... 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 Esta política deve ser revista pelo menos uma vez por ano pelo Diretor-Geral (GM) e pelos responsáveis de Recursos Humanos e TI.

### 9.2 Desencadeadores de revisão antecipada

#### 9.2.1 Devem ser efetuadas atualizações se:

9.2.1.1 Forem introduzidos novos sistemas de Recursos Humanos ou TI

9.2.1.2 Houver alteração do prestador externo de serviços de TI ou do serviço gerido de Recursos Humanos

9.2.1.3 As auditorias de segurança revelarem lacunas no processo

9.2.1.4 As obrigações regulamentares se alterarem (por exemplo, atualizações ao RGPD da UE)

9.2.1.5 Ocorrer uma falha crítica de cessação ou uma violação

### 9.3 Controlo de versões e aprovação

#### 9.3.1 Cada versão desta política deve incluir:

9.3.1.1 Número da versão e data

9.3.1.2 Resumo das alterações

9.3.1.3 Aprovação pelo Diretor-Geral (GM)

9.3.1.4 Versões anteriores arquivadas e retidas durante, pelo menos, três anos

### 9.4 Comunicação e confirmação

9.4.1 Todo o pessoal responsável por admissão ou cessação deve ser notificado de quaisquer atualizações desta política. São obrigatórias sessões anuais de sensibilização ou formação de reciclagem.

## 10. Políticas relacionadas e articulações

**10.1 Esta política apoia e é apoiada pelas seguintes:**

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: Assegura a responsabilização nos processos de acesso e admissão

10.1.2 P4S – Política de Controlo de Acesso: Estabelece a aplicação técnica do provisionamento e da desativação de acessos com base em funções

10.1.3 P6S – Política de Gestão de Riscos: Avalia os riscos decorrentes de falhas nos controlos de admissão e cessação

10.1.4 P8S – Política de Sensibilização e Formação em Segurança da Informação: Impõe requisitos de integração do pessoal durante a admissão

10.1.5 P30S – Política de Resposta a Incidentes: Trata a falha no desprovisionamento de acessos ou o furto de ativos como incidentes de segurança

## 11. Normas e referenciais aplicáveis

**11.1 ISO/IEC 27001**

11.1.1 Cláusula 6.2 – Estabelece requisitos de segurança de recursos humanos

11.1.2 Cláusula 7.2 – Impõe formação de sensibilização para novos colaboradores

**11.2 ISO/IEC 27002**

11.2.1 Controlos 6.2 e 6.5 – Detalham práticas de segurança para admissão e cessação da relação laboral

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

11.3.1 PS-4 – Procedimentos de cessação de pessoal, incluindo desativação de acessos

11.3.2 AC-2 – Assegura a gestão do ciclo de vida das contas de utilizador

11.3.3 PL-4 – Exige planeamento para transições de pessoal

**11.4 RGPD da UE**

11.4.1 Artigo 32 – Assegura segurança adequada durante e após o vínculo laboral, em particular no acesso a dados pessoais

**11.5 Diretiva NIS2 da UE**

11.5.1 Artigo 21(2)(h) – Exige segurança de recursos humanos e controlos do ciclo de vida dos acessos

**11.6 DORA da UE**

11.6.1 Artigo 12 – Exige que as entidades financeiras reguladas controlem o acesso do pessoal aos sistemas TIC, incluindo procedimentos de revogação

**11.7 COBIT 2019**

11.7.1 APO07 Gerir recursos humanos – Estabelece requisitos de segurança para o ciclo de vida do pessoal

11.7.2 DSS01 – Abrange o controlo do acesso lógico e físico durante transições laborais