					Insira aqui a designação da entidade jurídica registada							
Número do documento: P04					Título do documento: **Política de Controlo de Acesso**							
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 5.15, 5.17, 5.18	Gestão de acessos lógicos e físicos
ISO/IEC 27002:2022	Controlos 8.2, 8.3	Acesso baseado em funções e gestão de identidades
NIST SP 800-53 Rev. 5	AC-1 a AC-20, IA-1 a IA-8	Controlos de contas e acessos, identidade e autenticação
RGPD da UE	Artigos 5(1)(f), 32(1)(b); Considerando 39	Proteção de dados e minimização
Diretiva NIS2 da UE	Artigo 21(2)(c–e)	Controlo de acesso, autenticação de utilizadores e proteção de ativos
DORA da UE	Artigos 6, 9(2)	Acesso de utilizadores a TIC e controlos robustos sobre terceiros
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Admissão, operações, monitorização e conformidade

1. Finalidade

1.1 A presente política estabelece princípios, responsabilidades e requisitos de controlo obrigatórios para a gestão do acesso a sistemas de informação, aplicações, instalações físicas e ativos de dados em toda a organização.

1.2 Assegura que o acesso é concedido com base na necessidade de negócio, na função exercida e no nível de risco, aplicando princípios como o menor privilégio, a necessidade de conhecer e a segregação de funções.

1.3 A política suporta a implementação da Cláusula 5.15 da ISO/IEC 27001:2022 e dos controlos relacionados aplicáveis ao acesso lógico e físico, à autenticação de utilizadores e à gestão do ciclo de vida dos acessos.

1.4 Esta política sustenta a proteção dos recursos digitais e físicos contra utilização não autorizada, abuso ou comprometimento.

2. Âmbito

2.1 Esta política aplica-se a todos os utilizadores, sistemas e instalações abrangidos pelo âmbito do SGSI, incluindo:

2.1.1 trabalhadores, prestadores de serviços, fornecedores e pessoal temporário

2.1.2 infraestrutura local, sistemas alojados na nuvem e ambientes híbridos

2.1.3 todos os ativos corporativos — hardware, software, dados e áreas físicas seguras

2.1.4 acesso lógico (por exemplo, sistemas, redes, aplicações, APIs) e acesso físico (por exemplo, edifícios, centros de dados)

2.2 Regula o acesso ao longo de todo o ciclo de vida da identidade e da interação com os recursos, desde a integração e o provisionamento de acessos até às alterações de funções e à cessação.

2.3 A política abrange igualmente contextos de dispositivo pessoal no trabalho (BYOD) e de acesso remoto (VPN, gestão de dispositivos móveis), garantindo que os controlos são consistentes entre localizações e modelos de propriedade dos dispositivos.

3. Objetivos

3.1 Implementar controlos de acesso seguros e baseados em funções que suportem a integridade operacional e a conformidade regulamentar.

3.2 Assegurar que os direitos de acesso são adequadamente aprovados, monitorizados e revogados em tempo útil.

3.3 Prevenir acessos não autorizados, elevação de privilégios ou a manutenção de direitos de acesso desatualizados.

3.4 Suportar princípios de confiança zero, adotando por defeito a negação de acesso, salvo quando exista aprovação e justificação explícitas.

3.5 Fornecer garantias a auditores e partes interessadas através de revisões de acesso automatizadas e baseadas em evidência, bem como da aplicação desta política.

3.6 Integrar o controlo de acesso nos processos de negócio, nos eventos do ciclo de vida de recursos humanos e nas arquiteturas técnicas.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova a Política de Controlo de Acesso e assegura orçamento e recursos humanos adequados para a sua aplicação.

4.1.2 Revê os riscos de controlo de acesso durante as revisões pela gestão do SGSI e atribui responsabilidades ao nível estratégico.

4.2 Diretor de Segurança da Informação / Gestor do SGSI

4.2.1 É responsável pelo quadro de controlo de acesso e assegura o alinhamento com a ISO/IEC 27001 e normas relacionadas.

4.2.2 Coordena a aplicação da política, os testes de controlos e o reporte de métricas de controlo de acesso.

4.2.3 Supervisiona a modelação de acessos baseada no risco e monitoriza lacunas sistémicas de controlo.

[... 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 Fatores desencadeadores de revisão e frequência

9.1.1 Esta política deve ser revista:

9.1.1.1 anualmente, ou

9.1.1.2 na sequência de uma alteração relevante na infraestrutura de TI, nos requisitos regulamentares ou no nível de risco

9.1.1.3 após incidentes que revelem fragilidades nos controlos de acesso

9.1.1.4 quando ocorram alterações significativas nas tecnologias de autenticação ou nas plataformas de identidade

9.2 Autoridade e processo de revisão

9.2.1 O Diretor de Segurança da Informação ou o responsável designado pelo SGSI deve gerir o ciclo de revisão, incorporando:

9.2.1.1 constatações da auditoria interna

9.2.1.2 resultados e métricas das revisões de acessos

9.2.1.3 atualizações legais e regulamentares

9.2.1.4 alterações das plataformas tecnológicas

9.2.2 Todas as revisões devem ser aprovadas pela Alta Direção e comunicadas a todas as partes interessadas.

9.2.3 Pode ser exigido aos utilizadores afetados que confirmem novamente a política após atualizações materiais.

9.3 Controlo de versões e documentação

9.3.1 A versão mestra deve ser armazenada no repositório documental do SGSI com os seguintes metadados:

9.3.1.1 número da versão e registo de alterações

9.3.1.2 data de entrada em vigor e data da próxima revisão

9.3.1.3 responsável e autoridade de aprovação

9.3.1.4 registos de distribuição e confirmação

9.3.2 As versões substituídas devem ser arquivadas e permanecer acessíveis por um período mínimo de 3 anos.

10. Políticas relacionadas e ligações

10.1 Esta política depende funcionalmente das seguintes políticas e deve ser interpretada em conjunto com elas:

10.1.1 P01 – Política de Segurança da Informação: define o compromisso da organização com a segurança e as expectativas de alto nível em matéria de controlo de acesso.

10.1.2 P03 – Política de Utilização Aceitável: estabelece as condições comportamentais de acesso e a responsabilização dos utilizadores pela utilização responsável dos sistemas.

10.1.3 P05 – Política de Gestão da Mudança: regula a forma como alterações a configurações de acesso, funções ou estruturas de grupos devem ser implementadas e testadas com segurança.

10.1.4 P07 – Política de Admissão e Cessação: determina o início e a revogação de direitos de acesso de acordo com eventos do ciclo de vida do utilizador.

10.1.5 P11 – Política de Gestão de Contas de Utilizador e Privilégios: operacionaliza os controlos ao nível da conta e complementa esta política com orientações técnicas para a aplicação do controlo de acesso.

10.2 Em conjunto, estas políticas proporcionam um quadro coeso e aplicável de governação de acessos em todas as unidades de negócio e tecnologias.

11. Normas e referenciais de referência

11.1 ISO/IEC 27001:2022:

11.1.1 Cláusula 5.15 – Controlo de acesso: esta política cumpre o requisito de controlar o acesso à informação e a outros ativos associados, com base em requisitos de negócio e de segurança da informação.

11.1.2 Cláusula 5.17 – Gestão de identidades e Cláusula 5.18 – Informação de autenticação: estas são operacionalizadas através do provisionamento de identidades, dos mecanismos de autenticação e das atribuições de privilégios.

11.1.3 Controlos do Anexo A 8.2 (Política de controlo de acesso) e 8.3 (Gestão de identidades): fornecem a base para os objetivos de controlo desta política, incluindo acesso baseado em funções, integração do ciclo de vida da identidade e proteção de acessos privilegiados.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Família AC (AC-1 a AC-20): esta política suporta os requisitos de controlo de acesso do NIST para sistemas físicos e lógicos, incluindo definição de política (AC-1), gestão de contas (AC-2) e segregação de funções (AC-5).

11.2.2 Família IA (IA-1 a IA-8): fornece orientação para autenticação de identidade, proteção de credenciais e MFA.

11.2.3 AU-2, AU-12: os requisitos de registo e auditoria aplicados ao abrigo desta política suportam a responsabilização dos utilizadores e a investigação de incidentes.

11.2.4 PE-2 a PE-6: tratam restrições de acesso físico, que esta política aplica parcialmente através de controlos sobre crachás e permissões de acesso às instalações.

11.3 RGPD da UE (2016/679):

11.3.1 Artigo 5(1)(f): os dados pessoais devem ser protegidos contra acessos não autorizados. Esta política assegura a aplicação técnica e processual desse princípio.

11.3.2 Artigo 32(1)(b): exige a implementação de controlos de acesso, pseudonimização e cifragem para prevenir o tratamento não autorizado de dados pessoais.

11.3.3 Considerando 39: determina a minimização do acesso a dados pessoais, aqui aplicada através do princípio do menor privilégio e de requisitos de justificação de acesso.

11.4 Diretiva NIS2 da UE (2022/2555):

11.4.1 Artigo 21(2)(c–e): esta política viabiliza medidas técnicas e organizativas de controlo de acesso, autenticação de utilizadores e proteção de ativos em entidades essenciais e importantes.

11.5 DORA da UE (2022/2554):

11.5.1 Artigo 6: exige políticas de gestão do risco de TIC que incluam explicitamente a gestão de acessos de utilizadores e os controlos do ciclo de vida da identidade. Esta política cumpre esse requisito para os setores financeiro e de serviços TIC.

11.5.2 Artigo 9(2): esta política suporta a aplicação de controlos de acesso robustos no âmbito da gestão de serviços TIC de terceiros e intragrupo.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: aplica controlos de admissão e cessação para suportar a governação de acessos.

11.6.2 BAI03 – Managed Solutions Identification and Build: integra requisitos de controlo de acesso nos processos de desenho de sistemas e de alteração.

11.6.3 DSS01 – Managed Operations e DSS05 – Managed Security Services: regulam a aplicação de restrições de acesso lógico e a monitorização de violações.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: suporta mecanismos de auditoria e garantia para validar a eficácia do controlo de acesso.