					Insira aqui a designação da entidade jurídica registada							
Número do documento: P11					Título do documento: **Política de Gestão de Contas de Utilizador e Privilégios**							
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	Cláusula 6.1.3, Cláusula 8	-
ISO/IEC 27002:2022	Controlos 5.15-5	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
RGPD da UE	Artigos 5(1)(f), 32; Considerando 39	-
Diretiva NIS2 da UE	Artigos 21(2)(a, d), 21(3)	-
DORA da UE	Artigos 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Finalidade

1 Esta política estabelece controlos obrigatórios para a gestão de contas de utilizador e privilégios em todos os sistemas e serviços de informação. Garante que o acesso aos recursos da organização é concedido com base numa identidade validada, na necessidade associada à função e nos princípios do menor privilégio e da segregação de funções.

1.1 Sustenta o compromisso da organização com a segurança da informação através da implementação de processos estruturados e auditáveis para o provisionamento de acessos, atribuição de privilégios, monitorização da utilização e revogação de acessos.

1.2 Esta política é essencial para reduzir o risco de acessos não autorizados, uso indevido de privilégios, ameaças internas e incumprimento dos quadros legais e regulamentares aplicáveis.

2. Âmbito

2.1 Esta política aplica-se a todos os trabalhadores, prestadores de serviços, prestadores terceiros, consultores e outros indivíduos a quem seja concedido acesso aos recursos de TI, aplicações ou dados da organização.

2.2 Rege todos os sistemas e ambientes em que sejam utilizados mecanismos de autenticação de utilizadores e de controlo de acesso, incluindo, entre outros:

2.2.1 Aplicações empresariais e bases de dados

2.2.2 Plataformas na nuvem e ambientes SaaS

2.2.3 Sistemas operativos e consolas de administração

2.2.4 Ferramentas de acesso remoto e VPN

2.2.5 Sistemas de gestão de identidades e acessos

2.3 A política abrange tanto contas de utilizador padrão como contas privilegiadas, incluindo controlos sobre:

2.3.1 Criação, alteração e desativação de contas

2.3.2 Elevação e delegação de privilégios

2.3.3 Controlo e monitorização de sessões

2.3.4 Métodos de autenticação e gestão de credenciais

3. Objetivos

3.1 Assegurar que todas as contas de utilizador sejam identificáveis de forma única, devidamente autorizadas e atribuídas apenas após validação formal da necessidade.

3.2 Implementar os princípios do menor privilégio e prevenir acessos desnecessários ou excessivos, impondo controlos rigorosos sobre a atribuição e utilização de contas privilegiadas.

3.3 Exigir atualizações atempadas ao estado das contas com base em alterações laborais ou de função, incluindo a desativação imediata após cessação.

3.4 Permitir a deteção e remediação proativas de contas inativas, indevidamente utilizadas ou não autorizadas através de registo, revisões e automatização.

3.5 Manter o alinhamento com a ISO/IEC 27001:2022 e normas associadas, bem como cumprir as obrigações decorrentes de quadros legais e regulamentares relevantes, como o RGPD da UE, a Diretiva NIS2 da UE, a DORA da UE e o COBIT 2019.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável por esta política e assegura a sua aplicação em toda a organização.

4.1.2 Revê e aprova quaisquer exceções formais ou casos de acesso de emergência.

4.1.3 Reporta os resultados de auditoria relacionados com contas e escalona os riscos para a gestão de topo.

4.2 Gestor de controlo de acessos / administrador de TI

4.2.1 Mantém e opera os controlos técnicos para a gestão do ciclo de vida das contas de utilizador.

4.2.2 Executa ações de provisionamento e desprovisionamento de acessos e de gestão de privilégios mediante pedido aprovado.

4.2.3 Mantém um registo fidedigno de todas as contas de utilizador, do respetivo estado e nível de privilégio.

4.2.4 Apoia auditorias e revisões de conformidade com registos e relatórios de atividade.

[... 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 sempre que ocorram alterações significativas a:

9.1.1 Estrutura organizacional ou processos de negócio

9.1.2 Sistemas de TI, plataformas de identidade ou métodos de acesso

9.1.3 Requisitos regulamentares ou contratuais relacionados com a gestão de identidades e acessos

9.2 O Diretor de Segurança da Informação (CISO), em conjunto com o Gestor de controlo de acessos, é responsável por iniciar o processo de revisão e coordenar o feedback das partes interessadas.

9.3 As revisões intercalares podem ser desencadeadas por:

9.3.1 Incidentes de segurança relacionados com uso indevido de contas

9.3.2 Resultados de auditoria que evidenciem deficiências na gestão do ciclo de vida das contas

9.3.3 Implementação de novas ferramentas de gestão de identidades ou gestão de acessos privilegiados (PAM)

9.4 As atualizações desta política devem:

9.4.1 Estar sujeitas a controlo de versões e ser registadas na biblioteca documental do SGSI

9.4.2 Ser comunicadas a todas as partes interessadas relevantes, incluindo responsáveis de departamento, operações de TI e RH

9.4.3 Ser suportadas por materiais de formação e guias procedimentais atualizados

9.5 Todas as alterações devem ser aprovadas pela gestão de topo ou pelo Comité de Direção de Segurança da Informação e registadas para efeitos de auditoria.

10. Políticas relacionadas e interdependências

10.1 Esta política está operacionalmente ligada e é suportada pelas seguintes políticas relacionadas no âmbito do SGSI:

10.1.1 P4 Política de Controlo de Acesso: estabelece os princípios e mecanismos gerais de controlo de acesso, incluindo controlos baseados em regras e controlo de acesso baseado em funções (RBAC).

10.1.2 P7 Política de Admissão e Cessação: define os passos procedimentais para iniciar e terminar o acesso de utilizadores em alinhamento com as ações de RH.

10.1.3 P8 Política de Sensibilização e Formação em Segurança da Informação: reforça as responsabilidades dos utilizadores relativamente à segurança das contas e à salvaguarda de credenciais.

10.1.4 P13 Política de Classificação e Rotulagem de Dados: orienta os níveis de acesso com base na classificação de dados, assegurando que os limites de privilégios estão alinhados com os níveis de sensibilidade.

10.1.5 P22 Política de Registo e Monitorização: assegura que os rastos de auditoria são recolhidos para todas as atividades relacionadas com contas e revistos para detetar anomalias ou utilização não autorizada.

10.1.6 P30 Política de Resposta a Incidentes: rege o escalonamento, a contenção e as ações pós-incidente em casos de uso indevido de privilégios ou atividade não autorizada em contas.

10.2 Cada uma destas políticas funciona de forma complementar para aplicar um quadro coerente de gestão de identidades e acessos baseado no risco em toda a organização.

11. Normas e quadros de referência

11.1 Esta política está alinhada com normas de cibersegurança e quadros regulamentares globalmente reconhecidos que exigem a gestão segura de identidades, acessos e privilégios como componente essencial da segurança da informação da organização.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 6.1.3 - exige que as organizações determinem, avaliem e tratem os riscos de segurança da informação, tornando a gestão de acessos e privilégios um controlo formal baseado no risco, integrado no processo de planeamento do SGSI.

11.2.2 Cláusula 8.1 - Planeamento e controlo operacional: reforça a implementação de salvaguardas técnicas e procedimentais que regem o acesso de utilizadores e o acesso privilegiado.

11.3 ISO/IEC 27002:2022 - Controlos 5.15 a 5:

11.3.1 Controlo 5.15 - gestão de acessos de utilizadores: suporta processos formais para provisionamento de acessos, autorização de acesso e revisão periódica de direitos de acesso.

11.3.2 Controlo 5.16 - gestão de identidades: estabelece a unicidade da identidade, os controlos do ciclo de vida e a aplicação de autenticação segura.

11.3.3 Controlo 5.17 - assegura que a atribuição e a utilização de direitos de acesso privilegiado são estritamente controladas, rastreáveis e alinhadas com o princípio do menor privilégio ao longo do ciclo de vida da conta de utilizador.

11.3.4 Controlo 5.18 - direitos de acesso privilegiado: plenamente tratado através da atribuição de privilégios baseada em funções, auditoria e requisitos de aprovação para acesso elevado.

11.4 Estes controlos orientam a implementação estruturada do registo e cancelamento de contas, segregação de privilégios e utilização de informação de autenticação. A política aplica a governação do ciclo de vida da identidade, o acesso just-in-time e a monitorização de sessões elevadas para prevenir a utilização não autorizada dos sistemas.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Política de controlo de acesso) e AC-2 (Gestão de contas): mapeados através de requisitos da política para aprovações de acesso, mapeamento de funções e auditoria de contas de utilizador.

11.5.2 AC-5 (Segregação de funções) e AC-6 (Menor privilégio): cumpridos através de restrição de privilégios, alinhamento com funções profissionais e dupla aprovação para tarefas de alto risco.

11.5.3 IA-2 a IA-5 (Identificação e autenticação): aplicados através de mecanismos fortes de autenticação, regras do ciclo de vida das credenciais e requisitos de MFA.

11.5.4 AU-2, AU-12 (Registo e análise de auditoria): tratados através de gravação de sessões e monitorização de atividade privilegiada em ambientes sensíveis.

11.6 RGPD da UE (2016/679):

11.6.1 Artigo 32 - Segurança do tratamento: exige controlos de acesso e mecanismos de verificação de identidade para proteger dados pessoais. É cumprido através da obrigatoriedade de aprovações de contas, revisões de privilégios e salvaguardas fortes de autenticação.

11.6.2 Artigo 5(1)(f) - Integridade e confidencialidade: assegura que os dados pessoais são acedidos apenas por utilizadores autorizados com funções legítimas, reforçado pela aplicação da gestão de contas.

11.6.3 Considerando 39: exige limitação clara de acesso e responsabilização — esta política suporta a rastreabilidade integral das identidades de utilizador e das atribuições de privilégios.

11.7 Diretiva NIS2 da UE (2022/2555):

11.7.1 Artigo 21(2)(a, d): exige que as entidades apliquem políticas de gestão de acessos e tratamento seguro de credenciais e sessões privilegiadas, suportado pelos controlos desta política de provisionamento, monitorização e exceções.

11.7.2 Artigo 21(3): promove disciplina de acesso e forte garantia de identidade em setores críticos, assegurada pelo uso de identificadores únicos, RBAC e acesso elevado com restrição temporal.

11.8 DORA da UE (2022/2554):

11.8.1 Artigo 5 - Governação e controlo das TIC: impõe processos formalizados para gestão de utilizadores de TIC, cobertos através de provisionamento documentado, desativação e tratamento de exceções.

11.8.2 Artigo 9 - Gestão do risco das TIC: orienta as organizações a proteger sistemas através de restrições de acesso e monitorização, tratadas por MFA, registo de acessos privilegiados e revisões centralizadas.

11.9 COBIT 2019:

11.9.1 DSS01 - Operações geridas: promove a aplicação de controlos operacionais normalizados, incluindo gestão do ciclo de vida das contas de utilizador e documentação de acessos.

11.9.2 DSS05 - Gerir Serviços de Segurança: reflete a administração segura dos privilégios de utilizadores e de sistemas, apoiando a mitigação de riscos através do menor privilégio e da validação do rasto de auditoria.

11.9.3 APO13 - Segurança gerida: exige governação de acessos sobre ativos digitais, cumprida através de práticas formalizadas de autorização de contas e funções com requisitos de revisão periódica.