Política de controle de acesso

Código do Documento: POL-CTL-ACS-001	Versão: 1.0
Data de Aprovação: Janeiro de 2026	Classificação de Informação: Uso Interno
Área Gestora: Segurança da Informação / TI	Aplica-se a: Todos os Colaboradores e Prestadores de Serviço

1. OBJETIVO

Esta Política estabelece as diretrizes e padrões necessários para garantir a proteção, integridade, confidencialidade e disponibilidade dos ativos de informação da organização. Seu propósito principal é assegurar que o acesso a dados, sistemas, redes e infraestruturas seja concedido estritamente a usuários e serviços devidamente autorizados, prevenindo acessos indevidos, incidentes de segurança e vazamentos de dados.

2. ALCANCE E APLICAÇÃO

As diretrizes contidas neste documento aplicam-se obrigatoriamente a:

- Todos os colaboradores diretos, estagiários, diretores e prestadores de serviços terceirizados;
- Todas as plataformas, sistemas corporativos, bancos de dados, redes e infraestruturas em nuvem ou locais (*on-premises*);
- Serviços e integrações automatizadas (*APIs*, *jobs*, contas de serviço).

3. PRINCÍPIOS FUNDAMENTAIS

O controle de acesso corporativo deve seguir rigorosamente os três princípios abaixo:

Princípio	Descrição Operacional
Menor Privilégio (Least Privilege)	Todo usuário ou serviço receberá apenas o nível mínimo de permissões indispensável para a execução regular de suas atribuições.
Necessidade de Conhecer (Need-to-Know)	A concessão de acesso a informações restritas ou sensíveis fundamenta-se na necessidade técnica ou operacional, e não no nível hierárquico do solicitante.
Segregação de Funções (Separation of Duties - SoD)	Processos críticos que envolvam riscos operacionais ou financeiros devem exigir a atuação/aprovação de pessoas distintas, evitando a concentração de privilégios.

4. DIRETRIZES DE AUTENTICAÇÃO E IDENTIDADE

4.1. Credenciais Individuais e Intransferíveis

É expressamente proibido o compartilhamento de logins, senhas, chaves de API ou quaisquer outras credenciais de acesso entre colaboradores. Toda conta deve estar associada a uma identidade individual rastreável.

4.2. Autenticação Multi-Fator (MFA)

A utilização de Autenticação Multi-Fator (MFA) é obrigatória para todos os acessos a sistemas corporativos, plataformas em nuvem, ambientes de desenvolvimento e produção, sem exceções.

4.3. Requisitos de Senhas e Chaves

- As senhas corporativas devem atender aos requisitos mínimos de complexidade e tamanho estabelecidos pela equipe de TI;
- Chaves de acesso a ambientes de produção e APIs devem ser armazenadas em cofres de senhas corporativos e rotacionadas periodicamente.

5. GESTÃO DO CICLO DE VIDA DE ACESSOS

5.1. Concessão de Acesso

A liberação de acessos depende obrigatoriamente de solicitação formal realizada via canal oficial de TI, acompanhada da justificativa operacional e da aprovação expressa da liderança imediata e do responsável pelo recurso/sistema.

5.2. Movimentação e Desligamento

- Mudança de Cargo/Função: A área de Recursos Humanos deve notificar a TI sobre transferências internas para que os acessos anteriores sejam revogados e novos perfis ajustados.
- Desligamento: Em caso de encerramento do vínculo contratual, o bloqueio das contas e revogação das permissões devem ser executados imediatamente após a notificação oficial.

6. MONITORAMENTO, RASTREABILIDADE E AUDITORIA

Todos os sistemas, bancos de dados, aplicações e ativos de rede devem gerar registros de auditoria (*logs*) contendo:

- Identificação do usuário ou serviço;
- Data e hora exata do evento (*timestamp*);
- Tipo de tentativa de acesso (sucesso ou falha);
- Ação executada ou alteração efetuada em privilégios.

7. RESPONSABILIDADES E PENALIDADES

O descumprimento das normas estabelecidas nesta Política de Controle de Acesso sujeita o infrator às sanções disciplinares previstas em contrato de trabalho e no regimento interno da empresa, além de eventuais penalidades cíveis e criminais aplicáveis nos termos da legislação vigente.

Revisão #6
Criado 2026-09-03 13:23:07 UTC por Marcio Klitzke
Atualizado: 2026-09-04 18:02:06 UTC por Marcio Klitzke