2.1 Política de Controle de Acesso

1. Objetivo

Estabelecer diretrizes para provisionamento, modificação, revisão e revogação de acessos a sistemas, aplicações e redes, garantindo o princípio do menor privilégio, autenticação forte e conformidade com o CIS Controls v8 IG1 (C5/C6).

2. Escopo

Aplica-se a todos os tipos de contas (usuário, serviço e administrativa) em todos os ativos de informação da organização, incluindo ambientes on-premises e em nuvem.

3. Responsabilidades

- **Alta Direção**: Aprovar e apoiar esta política, assegurando recursos.
- **CISO / Gestor de Segurança da Informação**: Definir padrões de acesso, revisar relatórios e aprovar exceções.
- **Equipe de TI / Administradores de Sistemas**: Configurar contas, aplicar controles de acesso, implementar MFA, executar revisão periódica e registrar evidências.
- **RH**: Fornecer dados de ingresso, desligamento e movimentações de pessoal.
- **Gestores de Área**: Solicitar e validar acessos adequados às funções de seus subordinados.
- **Todos os Colaboradores**: Usar apenas contas individuais, manter credenciais seguras e cumprir controles definidos nesta política.

4. Definições

- **Provisionamento de Acesso**: Criação ou modificação de privilégios de contas.
- **Desprovisionamento**: Revogação ou remoção de contas e privilégios.
- **Least Privilege (Menor Privilégio)**: Permissões estritamente necessárias para a função.
- **MFA (Autenticação Multifator)**: Validação por dois ou mais fatores.
- **RBAC (Role-Based Access Control)**: Controle de acesso baseado em perfis.

5. Referências e Pré-requisitos

- Inventário de ativos e perfis de acesso.
- Sistema de IAM ou Active Directory.
- Procedimentos de Onboarding (4.1) e Offboarding (4.2).
- Ferramenta de MFA integrada aos sistemas críticos.

6. Diretrizes

- **Processo de provisionamento e revisão periódica de contas** (CIS C6)
- **Requisitos de MFA para contas privilegiadas** (CIS C5)

- **Princípio do Menor Privilégio** (CIS C6)
- **Regras de complexidade (ex.: mínimo 12 caracteres) e expiração** (CIS C5)
- **Uso de gerenciador de senhas para contas privilegiadas** (CIS C5)
- **Provisionamento Ágil**: Fluxo documentado para criar contas e atribuir privilégios a novos colaboradores ou funções novas, com SLA de 24h (CIS C6).
- **Princípio do Menor Privilégio**: Conceder somente permissões estritamente necessárias (CIS C6).
- **Autenticação Forte**: Exigir MFA em todas as contas privilegiadas e acessos remotos (CIS C5).
- **Revisão Periódica**: Revisar contas e privilégios a cada 90 dias, revogando acessos obsoletos (CIS C5/C6).
- **Aprovação de Acessos**: Todas as solicitações devem ter aprovação do gestor de área e do CISO.
- **Contas Genéricas**: Evitar ou restringir contas compartilhadas; documentar exceções e auditar uso.

7. Verificação e Auditoria

- **Auditoria Trimestral**: Comparar contas ativas vs. colaboradores ativos.
- **Monitoramento de Logs**: Centralizar e analisar logs de acesso, alertando atividades suspeitas.
- **Relatórios Mensais**: Indicadores de solicitações, aprovações e revogações de acesso.

8. Registros e Relatórios

- Registrar todas as operações de acesso em sistema de ticketing:
    - Tipo de operação (provisionamento, modificação, revogação)
    - Usuário-alvo
    - Data, hora e responsável técnico
    - Aprovações obtidas
- Armazenar evidências de MFA e relatórios de revisão de contas.

9. Revisão da Política

Revisar anualmente ou sempre que houver mudanças significativas em sistemas, estrutura ou requisitos regulatórios para garantir efetividade contínua.