1. Objetivo

Garantir a remoção rápida e completa de privilégios de acesso de colaboradores, prestadores ou contas obsoletas, minimizando riscos de uso indevido conforme CIS Controls v8 IG1 (C6).

2. Escopo

Aplica-se a todos os tipos de acessos: sistemas, redes, aplicações, bases de dados e contas administrativas ou de serviço, em ambientes on-premises e em nuvem.

3. Responsabilidades

- **Equipe de TI / Administradores de Sistemas**: Executar revogação, registrar ações e validar conclusão.
- **Gestor de Segurança da Informação**: Monitorar SLAs de revogação (até 24 horas após solicitação) e revisar relatórios periódicos.
- **RH**: Informar imediatamente desligamentos ou mudanças de função via sistema de RH.
- **Gestores de Área**: Solicitar revogação de acessos em mudanças de função ou término de contrato.

4. Definições

- **Revogação de Acesso**: Desativação ou remoção de contas e privilégios de usuário.
- **SLA de Revogação**: Prazo máximo de 24 horas após comunicação.
- **Logs de Revogação**: Registros que comprovam data, hora, responsável e escopo da ação.

5. Pré Requisitos

- Inventário de ativos e mapeamento de contas (registrado em planilha ou sistema).
- Acesso administrativo às plataformas alvo.
- Acordos de comunicação definidos (canal e responsáveis).

6. Procedimento Operacional

• Processo ágil para remoção de acessos de colaboradores desligados ou mudança de função, com prazos claros (CIS C6)

1. **Recepção da Solicitação**: RH ou gestor abre chamado no sistema de Service Desk com: nome do usuário, funções atuais e tipo de acesso.
2. **Validação**: Administrador confere inventário e identifica todos os sistemas e aplicações onde o usuário possui acesso.
3. **Desativação de Conta**:
    - Desabilitar login no Active Directory / IAM principal.
    - Remover do(s) grupo(s) de segurança ou perfil(s) de função.

4. **Remoção de Acessos Específicos**:
    - Revogar chaves de API, tokens ou certificados associados.
    - Remover permissões em bancos de dados e aplicações sob demanda.
5. **Desinstalação / Retirada de Dispositivos**:
    - Coletar equipamentos (notebook, token, cartão de acesso) entregues pelo colaborador.
6. **Confirmação e Notificação**:
    - Registrar data/hora e responsável no log centralizado.
    - Informar RH e gestor de área sobre conclusão.

7. Verificação e Auditoria. Verificação e Auditoria

- **Verificação Pós-Ação**: Administrador revisita contas 24 a 48 horas depois para garantir que não há acessos remanescentes.
- **Auditoria Mensal**: Comparar lista de colaboradores ativos versus contas ativas, reportar discrepâncias ao Gestor de Segurança.

8. Registros e Relatórios

- Manter log de todas as revogações em planilha ou sistema de ticketing, incluindo:
    - Nome do usuário
    - Sistemas afetados
    - Data e hora da ação
    - Responsável técnico
- Gerar relatório trimestral de conformidade para revisão pela Alta Direção.

9. Revisão do Procedimento

Este documento deverá ser revisado anual ou sempre que houver mudanças nos sistemas ou no processo de RH.