Política de Revisão e Auditoria Periódica de Usuários

Política de Revisão e Auditoria Periódica de Usuários

1. Objetivo

Estabelecer diretrizes, metodologia e responsabilidades para a revisão e auditoria periódica de acessos de usuários aos sistemas sob responsabilidade do time de Operações de Sistemas, visando garantir a segurança da informação, conformidade e o princípio do menor privilégio.

2. Escopo

Esta política aplica-se aos seguintes sistemas:

- ADM Crefaz
- ADM-CP
- Cobrança
- Webscm
- Datacob
- Crefazon

- LIS CrefazMais

Inclui todos os usuários internos, prestadores de serviços e contas de serviço com acesso a estes sistemas.

A base utilizada para essa revisão será a do RH para internos e a fornecida pelos gestores do contratos referente a prestadores de serviços.

3. Periodicidade

A auditoria deverá ser realizada a cada 3 (três) meses, com registro formal dos resultados.

4. Responsabilidades

4.1 Time de Operações de Sistemas

- Consolidar listas de usuários por sistema
- Conduzir o processo de auditoria
- Documentar evidências
- Acompanhar e garantir a execução das correções

4.2 Gestores dos Sistemas

- Validar os acessos sob sua responsabilidade
- Aprovar ou revogar permissões
- Justificar exceções

4.3 Segurança da Informação (quando aplicável)

- Apoiar na definição de critérios
- Auditar o processo
- Avaliar riscos identificados

5. Metodologia da Auditoria

A auditoria deverá seguir as seguintes etapas:

5.1 Levantamento de Acessos

- Extração da lista completa de usuários por sistema
- Identificação de perfis, papéis e níveis de acesso
- Identificação de contas inativas e contas técnicas

5.2 Classificação de Usuários

- Usuários ativos
- Usuários inativos
- Usuários com privilégios elevados
- Contas genéricas/compartilhadas

5.3 Validação com Gestores

- Envio da lista consolidada para os responsáveis por área
- Validação formal (e-mail, sistema ou ferramenta controlada)
- Registro de aprovação, ajustes ou revogações

5.4 Análise de Conformidade

- Verificação de aderência ao princípio do menor privilégio
- Identificação de acessos incompatíveis com a função
- Verificação de segregação de funções (SoD)

5.5 Correções e Ajustes

- Revogação de acessos indevidos
- Ajuste de perfis de acesso
- Remoção de contas inativas

5.6 Documentação e Evidências

- Registro da auditoria realizada
- Evidência de aprovações
- Lista de inconsistências encontradas
- Registro das ações corretivas

5.7 Relatório Final

- Sumário executivo
- Principais achados
- Riscos identificados
- Plano de ação

6. Metodologia por Sistema

6.1 ADM Crefaz

- Extração via base de usuários do sistema
- Validação por perfil funcional
- Atenção para perfis administrativos e acessos financeiros

6.2 ADM-CP

- Extração feita via tela do sistema
- Revisar acessos de acordo com usuários da base do RH e apontar modal de usuários terceiros, sistemáticos e administradores para análise.

6.3 Cobrança (RBM)

- Extração feita via banco.
- Revisar acessos de acordo com usuários da base do RH e apontar modal de usuários terceiros, sistemáticos e administradores para análise.

6.4 Datacob

- Extração feita via tela do sistema
- Revisar acessos de acordo com usuários da base do RH e apontar modal de usuários terceiros, sistemáticos e administradores para análise.

6.5 Crefazon

- Extração feita via banco de dados, com filtros específicos.
- Revisar acessos de acordo com usuários da base do RH e apontar modal de usuários terceiros e sistemáticos para análise.

6.6 LIS CrefazMais

- Extração feita via tela
- Revisar acessos de acordo com usuários da base do RH e apontar modal de usuários terceiros, sistemáticos e administradores para análise.

7. Pontos de Atenção

- Existência de usuários inativos ainda habilitados
- Contas com privilégios excessivos
- Contas genéricas sem responsável definido
- Falta de segregação de funções críticas
- Usuários com múltiplos perfis conflitantes
- Falta de evidência de aprovação de acesso privilegiado.
- Acessos não utilizados por longos períodos

8. Indicadores de Controle

- Quantidade de acessos revogados
- Quantidade de inconsistências identificadas
- Tempo médio de correção

9. Conformidade

Esta política está alinhada com boas práticas de segurança da informação, incluindo:

- Princípio do menor privilégio
- Segregação de funções (SoD)
- Gestão de Identidades e Acessos (IAM)

10. Disposições Finais

- Esta política deve ser revisada anualmente ou conforme necessidade

---

Revision #3
Created 6 May 2026 14:19:49 by Rodrigo
Updated 6 May 2026 21:01:49 by Rodrigo