PLANO DE AUDITORIA DE ACESSOS DE TI
NITERÓI PREV

OBJETIVOS

Verificar se os controles de acesso lógico e físico aos sistemas de informação estão adequados, eficazes e em conformidade com as melhores práticas e a regulamentação aplicável, mitigando riscos de acessos não autorizados, perda de integridade, disponibilidade ou confidencialidade das informações.

NORMATIVOS E REFERÊNCIAS

- **Manual de Segurança da Informação do Governo Federal**
- Resolução nº 03/NITPREV/2026 – Institui a **Política de Segurança da Informação da Niterói Prev**
- **Instrução Normativa nº 1/2018 (DISI/ME)** sobre auditoria de registros (log) e controles de acesso.
- **LGPD** (Lei Geral de Proteção de Dados – Lei nº 13.709/2018)
- **Normas de Auditoria Interna – IIA**, COSO, COBIT 2019
- Regulamentações específicas da **Secretaria de Previdência** sobre controles e integridade de RPPS e Pró-Gestão

ESCOPO DE AUDITORIA

Sistemas auditados:

- Sistemas geridos internamente:

  ✓ Infraestrutura de TI (Active Directory, servidores de aplicação e banco de dados)

  ✓ Controles de rede e acessos remotos

- Sistemas geridos externamente (*):
  ✓ Microsoft 365 (OneDrive, Outlook)
  ✓ Processo Eletrônico e-Ciga
  ✓ ERP e-Cidade
  ✓ Servidores de aplicação (File Server)

(*) Para sistemas geridos externamente, o escopo restringe-se à conformidade das solicitações de acesso e cancelamento via sistema e-Niterói, devendo-se considerar a necessidade de tempo hábil para a solicitação de relatório de auditoria junto aos administradores desses sistemas.

Controles auditados:

- Gestão de Identidades e Acessos (IAM)
- Políticas de senha e MFA
- Privilégios e segregação de funções
- Logs de acesso e registro de eventos
- Monitoramento e respostas a incidentes

METODOLOGIA

A metodologia proposta prevê várias etapas:

1. Planejamento e levantamento documental
2. Mapeamento de controles de acesso
3. Testes de conformidade e efetividade
4. Análise de logs e detecção de incidentes
5. Teste de controle técnicos
6. Entrevistas com responsáveis
7. Emissão de relatório de auditoria

1) Planejamento e levantamento documental

- Levantamento das políticas e normas internas de TI.
- Identificação de papéis/classe de usuários por sistema.

- Priorização de áreas críticas (ex.: gestores de benefícios, contabilidade, atendimento, etc).

2) Mapeamento de Controles de Acesso

Verificar se existem controles definidos e documentados para:

✓ Criação, alteração e exclusão de contas
✓ Perfis de acesso por função
✓ Revisões periódicas de acessos
✓ Padronizações de senhas e complexidade
✓ Autenticação multifator (MFA)

Evidências a coletar:

- Políticas de TI
- Logs do Active Directory e sistemas
- Relatórios de provisionamento/deprovisionamento

3) Testes de Conformidade e Efetividade

a) Microsoft 365 (OneDrive e Outlook)

Auditar:

- Logs de acesso e eventos de falhas (Azure AD)
- Aplicação de MFA
- Compartilhamento externo em OneDrive, especialmente de dados sensíveis
- Políticas DLP (Prevent Data Loss)
- Configurações de retenção e backup
- Acessos de dispositivos desconhecidos

b) Processo Eletrônico e-Ciga

Auditar:

- Registros de acesso por usuário
- Perfis que alteram/assinam processos
- Auditoria de trilhas de auditorias nos processos

c) ERP e-Cidade

Auditar:

- Perfis de usuários e acesso por módulo
- Privilégios sensíveis (ex.: inclusão/alteração/exclusão de dados financeiros)
- Segregação de Funções
- Logs de transações críticas (suficiência, tempo de retenção)

d) Conformidade com LGPD

- Não conformidade na retenção e proteção de registros
- Dado pessoal exposto ou vulnerável em acessos

4) Análise de Logs e Detecção de Incidentes

Verificar rotinas de geração, armazenamento e análise de logs:

- Active Directory
- ERP
- Ferramentas O365
- Servidores e Firewall

Critérios:

- Logs são armazenados por período definido?
- Há alertas automáticos para eventos críticos?
- Há evidências de análises periódicas?

5) Teste de Controles Técnicos

Exemplos:

✓ Senhas padrão alteradas?
✓ Contas de serviço com senha “never expire”?
✓ Contas inativas > 30/60 dias?
✓ Acesso remoto autorizado com MFA?
✓ Contas com privilégio de administrador são auditadas e justificadas?

6) Entrevistas com responsáveis

As entrevistas envolvem profissionais tanto da Niterói Prev como da Prefeitura de Niterói, uma vez que os sistemas são comuns a todas as entidades do Poder Executivo.

- Gestores de TI
- Administradores de sistemas
- Responsáveis pelos processos (e-Ciga, e-Cidade)
- Usuários chave

Objetivo: entender procedimentos reais e eventuais pontos de risco não formalizados.

7) Relatório de Auditoria

Deve conter:

📌 Sumário executivo
📌 Achados classificados por risco

- 📌 Evidências das não conformidades
- 📌 Recomendação de ações corretivas
- 📌 Plano de ação com responsáveis e prazos

INDICADORES DE AUDITORIA

Indicador	Meta
% de contas com MFA habilitado	≥ 95%
% de contas inativas removidas	≥ 90%
% de acessos com log suficiente	100%
% de revisões de acesso concluídas dentro do prazo	≥ 90%

CHECKLIST

Item	Conforme (Sim/Não)	Observações
Existe política formal de controle de acessos aprovada?		
Há processo formal de criação e exclusão de usuários?		
Contas inativas são revisadas periodicamente?		
MFA está habilitado para usuários e administradores?		

Perfis de acesso estão compatíveis com as funções exercidas?		
Existe segregação de funções implementada no ERP?		
Logs de acesso são armazenados por período mínimo definido?		
Há monitoramento ativo de eventos críticos?		
Contas privilegiadas são revisadas periodicamente?		
Compartilhamentos externos no OneDrive são controlados?		
Existe plano de resposta a incidentes de segurança?		
Backups dos logs e sistemas são realizados regularmente?		

PERIODICIDADE

A auditoria será realizada no final do primeiro e terceiro trimestres de cada ano.

8) Responsabilidade e Governança

- Comitê de Segurança da Informação: Fica estabelecido que o Comitê de Segurança da Informação da Niterói Prev é o órgão responsável pela supervisão e governança deste Plano de Auditoria.

- Atribuições do Comitê: Compete ao Comitê a aprovação formal do cronograma de auditorias, o provimento de recursos necessários para sua execução e a análise deliberativa dos relatórios de auditoria e planos de ação.
- Monitoramento: O Comitê deve revisar os Indicadores de Auditoria semestralmente para assegurar a efetividade dos controles de acesso e o cumprimento das metas estabelecidas.