

4.3 Procedimento de Backup e Restore

1. Objetivo

Descrever as etapas para realização de backups e restaurações de dados e sistemas críticos, garantindo a disponibilidade e integridade das informações conforme requisitos do CIS Control v8 IG1.

2. Escopo

Aplica-se a todos os servidores, bancos de dados, aplicações e arquivos críticos definidos no inventário de ativos, incluindo ambientes de produção e sistemas de suporte.

3. Responsabilidades

- **Equipe de TI / Administradores de Sistemas:** Executar backups, armazenar mídias e realizar restores quando solicitado.
- **Gestor de Segurança da Informação:** Monitorar conformidade, revisar relatórios e aprovar cronogramas de testes.
- **RH / Gestores de Área:** Comunicar necessidades de restauração de dados de colaboradores.

4. Definições

- **Backup:** Cópia de segurança de dados e configurações.
- **Restore:** Processo de restauração de dados a partir das mídias de backup.
- **Mídia de Backup:** Dispositivo ou local de armazenamento (local, off-site, nuvem).
- **Retenção:** Período mínimo de armazenamento de backups (ex.: 30 dias).

5. Frequência e Retenção

- **Backup Full:** Semanal, às 02:00 de domingo.
- **Backup Incremental:** Diário, às 02:00 de segunda a sábado.
- **Retenção:** Backups diários mantidos por 30 dias; backups semanais por 90 dias.
- **Armazenamento Off-site:** Mídias replicadas para repositório externo semanalmente.

6. Procedimento de Backup

1. **Preparação:** Verificar espaço em disco e integridade do sistema.
2. **Execução:** Iniciar ferramenta de backup (nome e versão), selecionando o job correspondente.
3. **Verificação:** Conferir logs de conclusão; validar hashes dos arquivos.
4. **Armazenamento:** Copiar cópia compactada para repositório off-site e registrar no log central.
- **Passo a passo operacional de backup automático:** documentar o fluxo completo da rotina agendada (ferramenta, comandos, scripts e parâmetros).

7. Procedimento de Restore. Procedimento de Restore

1. **Solicitação:** Abrir chamado no sistema de Service Desk com detalhes do dado/sistema.
2. **Seleção da Mídia:** Identificar backup full ou incremental adequado.
3. **Execução:** Restaurar dados seguindo passos da ferramenta de backup.
4. **Validação:** Confirmar consistência dos dados restaurados e funcionamento da aplicação.

8. Testes e Auditoria

- **Testes de Restore:** Realizar simulações mensais e trimestrais (quarterly) de restauração, documentando e registrando resultados conforme requisitos do CIS Controls v8 (C11).
- **Auditoria:** Revisar logs de backup mensalmente para garantir sucesso das execuções.

9. Registros e Relatórios. Registros e Relatórios

- Manter registros de todos os backups e restores em planilha ou sistema de logs.
- Gerar relatório de conformidade mensal para o Gestor de Segurança.

10. Revisão do Procedimento

Revisar e atualizar este documento anualmente ou sempre que houver alteração relevante nos sistemas ou ferramentas utilizadas.