Política de Backup e Restore

Julho 2025

HOSPITAL SÃO MARCOS

Sumário

HOSPITAL SÃO MARCOS

1. Introdução

O presente documento estabelece a Política de Backup e Restore de arquivos digitais armazenados no parque tecnológico do Hospital São Marcos, fornecendo uma base sólida para manter a integridade, disponibilidade e, quando necessário, a confidencialidade dos dados. Considerando que falhas de software, hardware ou erros humanos podem acarretar perdas de dados, prejuízos financeiros, sanções legais e impactos operacionais à organização, torna-se essencial a adoção de práticas robustas de backup e recuperação.

2. Objetivo

O objetivo desta política é estabelecer diretrizes e procedimentos para a realização de backups eficazes dos dados críticos do Hospital São Marcos, definindo a periodicidade, a forma de armazenamento e os métodos de recuperação, com foco na continuidade dos serviços em caso de falhas, exclusões acidentais, incidentes de segurança ou desastres.

3. Escopo

Esta política se aplica a todos os dados sob responsabilidade do Hospital São Marcos. Consideram-se dados críticos os bancos de dados, arquivos organizacionais e compartilhados, bem como quaisquer informações essenciais ao funcionamento da organização.

4. Definições

- **Backup:** Processo de cópia e armazenamento de dados para garantir sua recuperação em caso de perda ou corrupção.
- **Restore (Recuperação):** Processo de restauração dos dados a partir de backups previamente realizados.
- **Backup Full:** Cópia completa de todos os dados selecionados.
- **Backup Incremental:** Cópia apenas dos dados alterados desde o último backup (full ou incremental).
- **Mídia de Backup:** Dispositivo físico ou digital utilizado para armazenar os backups (ex: fitas magnéticas, nuvem, discos externos).
- **Dados Críticos:** Informações essenciais para a operação da organização, cuja perda pode causar impacto significativo.

5. Responsabilidades

- A equipe de TI do Hospital São Marcos é responsável por implementar, gerenciar e monitorar os procedimentos de backup e restauração, garantindo sua execução de forma segura, confiável e em conformidade com os padrões definidos nesta política, as políticas de segurança da informação e os requisitos regulatórios aplicáveis. Também é responsabilidade da equipe realizar testes periódicos de recuperação, manter a documentação atualizada e adotar melhorias contínuas nos processos.

- Os proprietários de dados e os administradores de sistemas são responsáveis por identificar os dados e sistemas que devem ser incluídos nos procedimentos de backup.

Quadro 1. Definição das responsabilidades:

Nome	Função
Eudoxio Medeiros	Gerente de TI
Vinicius Pádua	Analista de Sistemas – Responsável principal dos Backups

6. Diretrizes

Os backups devem ser executados conforme a periodicidade e a criticidade dos dados de cada sistema identificado.

6.1 Programação de Backups

Banco de dados do sistema São Marcos:

- O backup do banco de dados é realizado diariamente em disco.
- Utilizando a ferramenta BackupExec, o backup em disco deve ser transferido para fita.
- **Backup Incremental:** realizar a cada 6 (seis) horas para capturar as alterações desde o último backup completo ou incremental.
- **Backup Full:** realizar uma vez por dia, fora do horário de pico.
- **Backup de Log:** realizar a cada 1 (uma) hora para garantir recuperação detalhada, incluindo transações recentes.

6.1.1 File Server:

Com a ferramenta BackupExec, o backup do File Server deve seguir as periodicidades abaixo:

- **Backup Full:** mensal, incluindo todas as pastas e arquivos.
- **Backup Incremental:** quintas e domingos, com cópia apenas de arquivos modificados ou adicionados desde o último backup.

Para imagens (documentos digitalizados):

- **Backup Full:** em data diferente do backup do File Server, como medida de segurança adicional.
- **Backup Incremental:** terças e sábados, com cópia apenas das imagens alteradas ou novas.

6.2 Armazenamento de Dados de Backup

- Os backups dos dados críticos serão armazenados em fitas locais e/ou soluções digitais com capacidade compatível.
- As mídias devem ser armazenadas em ambientes protegidos, com controle de temperatura, umidade, proteção contra incêndios, acessos não autorizados e outros riscos físicos.
- O acesso às mídias será restrito à equipe de TI, conforme Quadro 1. Todos os acessos e manuseios devem ser registrados e auditáveis.
- Cópia externa: recomenda-se manter ao menos uma cópia dos backups críticos em local geograficamente distinto (nuvem segura, cofre digital ou site de contingência), para garantir continuidade em caso de desastre físico local.
- Criptografia: todos os backups que contenham dados sensíveis, pessoais ou confidenciais devem ser armazenados com criptografia robusta (ex: AES-256), tanto em trânsito quanto em repouso.

6.3 Retenção de Dados de Backup

- Os dados de backup serão retidos por um período mínimo de 6 (seis) meses, conforme necessidades do negócio e exigências legais ou regulatórias.

- Após esse prazo, as mídias poderão ser reutilizadas, desde que os dados anteriores sejam eliminados de forma segura, utilizando técnicas apropriadas de sobrescrita ou destruição física.

- Caso haja obrigação legal ou necessidade de investigação, o período de retenção poderá ser estendido, mediante avaliação da área jurídica.

6.4 Testes de Recuperação

- A equipe de TI deverá realizar testes periódicos de recuperação dos dados dos sistemas e arquivos críticos, utilizando a ferramenta BackupExec.

- Os testes devem incluir diferentes cenários de falha, como:

  - Corrupção de dados;
  - Falha de hardware;
  - Exclusões acidentais;
  - Incidentes de segurança e desastres simulados.

- Os testes devem ser documentados, com registro de data, escopo, tempo de recuperação e observações sobre o sucesso ou falhas ocorridas.

- Os testes devem ser realizados trimestralmente, ou sempre que houver mudanças significativas na infraestrutura de backup.

6.5 Procedimentos de Recuperação

Em caso de perda de dados, corrupção ou falhas de sistemas:

- A equipe de TI deve ser imediatamente notificada.

- Os procedimentos de recuperação devem ser executados conforme os passos abaixo:

  1. Avaliação do incidente e determinação da causa, se possível;

  2. Notificação às partes interessadas sobre o início do processo de recuperação;

  3. Identificação do backup mais recente e íntegro;

4. Execução da restauração dos dados utilizando o backup identificado;
5. Verificação da integridade e consistência dos dados restaurados;
6. Realização de testes para garantir o funcionamento normal dos sistemas antes da liberação ao uso;
7. Documentação completa do processo e análise de causa raiz para prevenir recorrências.

Incidentes que envolvam dados pessoais devem seguir o fluxo de resposta a incidentes da organização e podem exigir, conforme a gravidade e o risco identificado, a notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, conforme previsto na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018).

7. Revisão e Melhoria Contínua

Esta política deve ser revisada anualmente ou sempre que houver mudanças significativas no ambiente de TI, alterações legais ou regulamentares, ou ainda em decorrência da identificação de falhas nos processos. Auditorias internas devem ser conduzidas periodicamente para verificar a conformidade com esta política, identificar riscos e promover a melhoria contínua dos controles estabelecidos.

8. Histórico de Revisão

Data da Alteração	Responsável	Atualização
21/06/2023	Rute Lane	Criação da Política
02/07/2025	Nathali Macedo	Revisão da Política