Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	03/11/2025	Ageu	Criação da Norma	Larissa
2	16/11/2025	Samuel	Detalhamento de procedimentos	Larissa

Sumário

1. Objetivo

Esta Norma tem como objetivo definir as diretrizes, responsabilidades e procedimentos para a execução de backups e a determinação de prazos para a retenção e o descarte seguro dos dados corporativos do Hospital LISA. O cumprimento desta norma busca assegurar a capacidade de recuperação de informações críticas em caso de incidentes, falhas ou desastres, além de garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), especialmente no tratamento de Dados Pessoais Sensíveis de pacientes.

2. Escopo

Esta norma é aplicável a todos os dados e informações de propriedade do Hospital LISA ou sob sua custódia, em todos os formatos (digitais ou físicos), como por exemplo:

a. Bancos de dados de sistemas de gestão hospitalar (prontuários eletrônicos, agendamentos, faturamento);
b. Servidores de arquivos, aplicações e e-mail;
c. Resultados de exames, laudos e imagens médicas;
d. Configurações de ativos de rede e sistemas.

3. Responsabilidades

a. Área de Tecnologia da Informação (TI):
  i. Elaborar, documentar (o "Plano de Backup"), implementar e gerenciar as rotinas de backup (diárias, semanais, mensais) conforme o definido nesta norma. Este plano deve ser formalmente aprovado pelo Gestor de TI e validado pela Diretoria Executiva.
  ii. Monitorar a execução dos backups, garantindo sua conclusão com sucesso;

iii. Garantir a segurança das mídias de backup, incluindo o armazenamento em local externo (off-site) e o uso de criptografia;
iv. Realizar e documentar testes periódicos de restauração para comprovar a integridade dos dados;
v. Executar o descarte seguro dos dados após o término do período de retenção, conforme autorização.

b. Proprietários da Informação (Gestores de Áreas):
i. Definir, em conjunto com a área de TI e o Encarregado de Dados, os prazos de retenção das informações de sua área, respeitando os requisitos legais, regulatórios e contratuais;
ii. Solicitar formalmente à TI a restauração de dados quando necessário;
iii. Autorizar o descarte de informações que chegaram ao fim de seu ciclo de vida.

c. Todos os Profissionais do Hospital LISA:
i. Assegurar que todos os dados corporativos críticos sejam armazenados nos servidores de rede oficiais (e não em estações de trabalho locais ou dispositivos pessoais), assegurando sua inclusão nas rotinas de backup.

4. Diretrizes de Backup

4.1. Frequência e Tipos de Backup

As rotinas de backup devem seguir uma estratégia que reduza ao mínimo a perda de dados.

a. **Backups Diários:** Devem ser realizados backups de todos os dados críticos e transacionais, como bancos de dados de prontuários eletrônicos.

b. **Backups Semanais:** Devem ser realizadas cópias de segurança completas de todos os servidores e sistemas críticos.
c. **Backups Mensais e Anuais:** Cópias completas devem ser geradas para arquivamento de longo prazo.

4.2. Armazenamento, Mídia e Criptografia

a. **Regra 3-2-1:** A estratégia de backup deve contemplar, no mínimo, 3 (três) cópias dos dados, em 2 (duas) mídias diferentes, e 1 (uma) cópia precisa estar em local externo (off-site). Para o Hospital LISA, este local será um ambiente em nuvem (pública ou privada) que atenda aos seguintes requisitos mínimos de segurança:
    i. O provedor deve possuir contrato que assegure a conformidade com a LGPD.
    ii. O provedor deve possuir certificações de segurança auditáveis, como ISO 27001 e, preferencialmente, conformidade com a HIPAA (padrão de segurança para saúde).
b. **Segurança da Mídia:** O acesso às mídias de backup (fitas, discos ou nuvem) deve ser restrito e controlado pela Área de TI.
c. **Criptografia:** Todas as cópias de backup que contenham Dados Pessoais Sensíveis (dados de pacientes ou colaboradores) devem ser obrigatoriamente criptografadas.

4.3. Testes de Restauração

A efetividade dos backups deve ser comprovada por meio de testes de restauração.

a. **Frequência:** Os testes devem ser realizados em intervalos regulares (no mínimo, semestralmente) e sempre que houver mudanças significativas na infraestrutura.
b. **Documentação:** Todos os testes de restauração devem ser documentados com o detalhamento dos dados restaurados e o tempo de recuperação e os resultados obtidos.

4.4. Monitoramento e Tratamento de Falhas

a. Todas as rotinas de backup, sejam elas bem-sucedidas ou falhas, devem gerar logs automatizados e centralizados, que serão retidos por no mínimo 30 dias.
b. A Área de TI deve analisar ativamente os logs de falhas de backup diariamente.
c. Qualquer falha em um backup de dados críticos (ex: prontuários) deve ser tratada como um incidente de prioridade alta, e a rotina deve ser re-executada manualmente no menor tempo possível.

4.5. Indicadores de Desempenho (KPIs)

Para garantir a eficácia desta norma e facilitar auditorias, a Área de TI manterá os seguintes indicadores de desempenho (KPIs):

a. **Taxa de Sucesso de Backup:** Meta de > 99% dos jobs de backup concluídos com sucesso mensalmente.
b. **Taxa de Sucesso de Restore:** Meta de 100% de sucesso nos testes de restauração (restore) semestrais.
c. **Tempo Objetivo de Recuperação (RTO):** O tempo máximo aceitável para restauração será definido no Plano de Continuidade de Negócios (PCN).

5. Diretrizes de Retenção e Descarte

5.1. Prazos de Retenção

a. **Princípio da Necessidade (LGPD):** Os dados pessoais serão mantidos armazenados apenas pelo período necessário para cumprir as finalidades para as quais foram coletados.
b. **Obrigações Legais:** Os prazos de retenção devem seguir estritamente os requisitos legais e regulatórios do setor de saúde (ex:

normas do Conselho Federal de Medicina, Ministério da Saúde) e outras legislações (tributária, trabalhista).

c. **Tabela de Temporalidade:** O Hospital LISA manterá uma Tabela de Temporalidade que especifica os prazos exatos para cada tipo de dado. A título de exemplo, seguem as diretrizes gerais:
   i. **Prontuários de Pacientes:** Mínimo de 20 (vinte) anos após o último registro
   ii. **Exames (Laudos e Imagens):** Mínimo de 20 (vinte) anos (integrados ao prontuário)
   iii. **Dados Financeiros (Faturamento):** Mínimo de 5 (cinco) anos (Legislação Tributária)
   iv. **Logs de Acesso a Aplicações:** Mínimo de 6 (seis) meses (Marco Civil/LGPD)
   v. **Dados de Colaboradores (RH):** Período definido por legislação trabalhista]

5.2. Descarte Seguro

a. Expirado o período de retenção definido, ou mediante solicitação de eliminação de dados por um titular (conforme Art. 18 da LGPD) os dados devem ser descartados mediante uma solicitação formal de descarte.
b. O descarte deve ser feito por métodos que assegurem a eliminação permanente e irreversível dos dados, impedindo sua recuperação.
c. Rastreabilidade e Evidência de Descarte:
   i. A solicitação de descarte do Proprietário da Informação deve ser formalizada via sistema de chamados (ticket) ou formulário eletrônico com assinatura, servindo como autorização formal.
   ii. A Área de TI deve, após a eliminação segura, anexar ao ticket as evidências do descarte (ex: logs de exclusão do sistema, relatório de wipe da mídia).

iii. Este registro completo (autorização + evidência) deve ser arquivado por, no mínimo, 5 (cinco) anos para fins de auditoria.

6. Disposições Gerais

6.1. Penalidades

O descumprimento desta Norma ou de qualquer dos demais padrões institucionais de Segurança de Informação poderá ser passível de penalidades, tanto na esfera administrativa (advertências, punições administrativas, afastamento) quanto na esfera legal (reparação dos danos), de acordo com a gravidade do ato.

6.2. Revisão da Norma

Este documento será revisado e poderá ser alterado em caso de mudanças de processo, tecnologia, diretrizes institucionais ou da legislação vigente. A revisão deve ocorrer com frequência mínima anual.