Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	09/11/2025	Igo	Criação da Política	Samuel

Sumário

1. Objetivo

O objetivo central deste Plano de Continuidade de Negócios (PCN) e Recuperação de Desastres (DRP) é detalhar como o Hospital LISA irá agir em incidentes críticos. Ele fornece as diretrizes e os procedimentos para garantir a continuidade das operações essenciais, colocando em primeiro lugar a segurança do paciente e a proteção dos Dados Pessoais Sensíveis. Nosso propósito é minimizar o impacto de qualquer desastre, assegurando que os processos e sistemas críticos sejam retomados rapidamente e dentro dos prazos aceitáveis.

2. Escopo

Este plano aplica-se a todos os processos, sistemas de informação, dados e infraestruturas (físicas e lógicas) que suportam as operações críticas do Hospital LISA, definidos na Política de Gestão de Acessos (PGA) e na Política de Classificação da Informação (PCI).

Abrange cenários de desastre que incluem, mas não se limitam a:

a. Falhas de infraestrutura (energia, rede, servidores);
b. Ataques cibernéticos (Ransomware, negação de serviço);
c. Desastres naturais ou incidentes físicos (incêndio, inundação);
d. Indisponibilidade de pessoal-chave ou pandemias.

3. Glossário

Para padronizar e facilitar o entendimento dos termos utilizados neste documento, abaixo estão os conceitos relacionados:

Análise de Impacto no Negócio (BIA): Processo que identifica os processos de negócio críticos e os recursos necessários para sua operação, bem como o impacto de uma interrupção.

Plano de Continuidade de Negócios (PCN): Estratégia focada na continuidade dos processos de negócio (incluindo procedimentos manuais) durante uma crise.

Plano de Recuperação de Desastres (DRP): Subconjunto do PCN, focado especificamente na recuperação da infraestrutura e sistemas de Tecnologia da Informação (TI).

Objetivo de Tempo de Recuperação (RTO): O tempo máximo aceitável que um processo ou sistema pode ficar indisponível após um desastre.

Objetivo de Ponto de Recuperação (RPO): A quantidade máxima aceitável de perda de dados medida em tempo (ex: "dados das últimas 4 horas").

Incidente Crítico: Um evento que excede a capacidade de resposta a incidentes padrão e requer a ativação deste plano.

4. Análise de Impacto no Negócio (BIA)

A priorização da recuperação baseia-se na criticidade do processo para a vida do paciente e para a operação do hospital, conforme a classificação de dados "CONFIDENCIAL" e as áreas seguras "críticas".

4.1. Processos Críticos

Os processos são classificados em níveis de prioridade para recuperação:

a. **Prioridade 0 (Crítico - RTO < 1 hora):**
   i. Sistemas de suporte à vida (ex: monitores em CTI e Centro Cirúrgico).
   ii. Sistemas de admissão de emergência (Pronto-Socorro).
   iii. Acesso imediato a Prontuários Eletrônicos para pacientes em atendimento.
   iv. Sistemas da Farmácia Hospitalar (para dispensação de emergência).
b. **Prioridade 1 (Alta - RTO < 4 horas):**

i. Sistemas de Prontuário Eletrônico - funcionalidade completa.
ii. Sistemas de Laudos e Imagens Médicas.
iii. Sistemas de agendamento cirúrgico.
iv. Infraestrutura de rede e servidores principais.

c. **Prioridade 2 (Média - RTO < 24 horas):**
   i. Sistemas de Faturamento e Contas.
   ii. Sistemas de agendamento de consultas.
   iii. Servidores de arquivos e e-mail corporativo.
d. **Prioridade 3 (Baixa - RTO < 72 horas):**
   i. Sistemas de Recursos Humanos (RH).
   ii. Sistemas administrativos não assistenciais.

4.2. Aceitação de Riscos Residuais

A aceitação de riscos residuais poderá ocorrer quando a recuperação dentro do RTO não for possível ou viável. Toda exceção deve ser formalizada com justificativa, impacto e período de validade, e aprovada conforme a autoridade definida no item 4.3.

4.3. Autoridade de Aprovação

a. **Prioridade 0 e 1:** Somente a Diretoria Executiva, após parecer técnico da Área de TI e Segurança da Informação.
b. **Prioridade 2:** Aprovação da Diretoria Administrativa, com análise técnica da Área de TI.
c. **Prioridade 3:** A aceitação poderá ser aprovada pela Gestão de TI, com ciência da Diretoria Administrativa, dada a menor criticidade e tolerância ampliada à indisponibilidade.

Prioridade	RTO (Tempo de Recuperação)	RPO (Perda de Dados)
Prioridade 0	< 1 Hora	< 15 Minutos (Replicado)
Prioridade 1	< 4 Horas	< 24 Horas (Backup Diário)
Prioridade 2	< 24 Horas	< 24 Horas (Backup Diário)
Prioridade 3	< 72 Horas	< 48 Horas

5. Estratégias de Continuidade e Recuperação

5.1. Continuidade de Processos

Caso os sistemas de TI (Prioridade 0 e 1) fiquem indisponíveis, os seguintes procedimentos manuais de contingência devem ser adotados pelos Gestores da Informação:

a. **Prontuários e Atendimento:** Utilização de formulários de contingência (papel) pré-impressos e armazenados nas áreas de atendimento (Enfermarias, CTI, Pronto-Socorro). Os registros deverão ser inseridos no sistema assim que este for restabelecido.
b. **Dispensação de Medicamentos:** A Farmácia Hospitalar utilizará controles manuais (livro de atas ou formulários) para registro de entrada e saída de medicamentos, com base em prescrições físicas assinadas.
c. **Laudos e Exames:** Os equipamentos de diagnóstico (ex: Tomografia, Raio-X) que funcionam de forma independente do sistema central devem salvar os exames localmente. Os laudos serão emitidos em formulários de contingência.

d. **Infraestrutura Física:** Em caso de falha no Data Center principal, os serviços essenciais serão migrados para o local de recuperação.

5.2. Recuperação de Desastres de TI (DRP)

A recuperação da infraestrutura de TI seguirá a estratégia definida na Norma D.NBRD.TI.01:

a. **Declaração de Desastre:** A Área de Segurança da Informação, após aprovação da Diretoria Executiva, declara o desastre de TI.
b. **Ativação do Ambiente de DR:** A recuperação dos sistemas será priorizada no "ambiente em nuvem seguro" (local externo), conforme a estratégia 3-2-1 de backup.
c. **Restauração:** A Área de TI iniciará a restauração dos sistemas a partir das cópias de backup (diárias, semanais), seguindo a ordem de prioridade definida na BIA.
d. **Segurança:** Todas as cópias de backup de dados sensíveis de pacientes são criptografadas, garantindo a confidencialidade durante a restauração.
e. **Validação:** A Área de TI e os Gestores da Informação (Proprietários) validarão a integridade dos dados e o funcionamento dos sistemas restaurados antes de liberar o acesso aos usuários.

6. Ativação do Plano e Gerenciamento de Crise

A eficácia do plano depende de uma estrutura de resposta clara, sabendo quando ativar o plano e quem é responsável por cada ação.

6.1. Critérios de Ativação

Este plano deve ser ativado pela Diretoria Executiva ou pela Área de Segurança da Informação quando um incidente crítico:

a. Ameaçar a segurança ou a vida de pacientes e colaboradores;
b. Causar a indisponibilidade dos processos de Prioridade 0 ou 1 por um tempo superior a 30 minutos;
c. Resultar na perda ou inacessibilidade do Data Center principal ou da Sala de Arquivos Médicos.

6.2. Estrutura de Resposta (Equipes)

Uma vez que o plano é ativado, a seguinte estrutura de comando e controle é estabelecida:

a. **Comitê de Gerenciamento de Crise:**
    i. **Líder:** Membro da Diretoria Executiva.
    ii. **Membros:** Líderes da Área de Segurança da Informação, TI, Encarregado de Dados (DPO), RH e Gestores das áreas de negócio afetadas.
    iii. **Responsabilidade:** Tomada de decisão estratégica, alocação de recursos e comunicação externa.
b. **Equipe de Recuperação de TI (DRP):**
    i. **Líder:** Gestor da Área de TI / Segurança da Informação.
    ii. **Responsabilidade:** Executar os procedimentos técnicos de restauração (Seção 5.2), gerenciar o ambiente de DR e restaurar a conectividade.
c. **Equipes de Continuidade Operacional:**
    i. **Líder:** Gestores de cada área de negócio (ex: Diretor Clínico, Gerente de Enfermagem).
    ii. **Responsabilidade:** Implementar os procedimentos manuais de contingência (Seção 5.1), gerenciar a equipe da área e garantir o atendimento mínimo ao paciente.

6.3. Comunicação de Crise

A gestão da informação durante a crise é fundamental para manter a ordem e a confiança. A comunicação será segmentada da seguinte forma:

a. **Comunicação Interna:** A Área de Recursos Humanos será responsável por manter os colaboradores informados sobre o status da crise, locais seguros e instruções de trabalho.
b. **Comunicação Externa (Pacientes e Imprensa):** O Comitê de Gerenciamento de Crise definirá a comunicação oficial, visando a transparência e a calma.
c. **Comunicação Regulatória:** Em caso de incidente de segurança que afete Dados Pessoais Sensíveis, o Encarregado (DPO), em conjunto com a área de Segurança da Informação, avaliará a necessidade e realizará a comunicação à Autoridade Nacional de Proteção de Dados.

7. Testes e Manutenção do Plano

Para garantir a eficácia deste plano, conforme exigido pela PSI e pela NBRD, serão realizados:

a. **Testes de Recuperação de Desastres (DRP):** A Área de TI deve realizar testes de restauração de dados com frequência mínima semestral, para validar os backups e o tempo de recuperação (RTO). Todos os testes devem ser documentados.
b. **Testes de Continuidade de Negócios:** O Comitê de Gerenciamento de Crise deve coordenar, no mínimo anualmente, um exercício simulado ("Tabletop" ou "Walk-through") envolvendo os Gestores de Área para validar os procedimentos manuais.
c. **Revisão do Plano:** Este documento deve ser revisado anualmente ou sempre que ocorrerem mudanças significativas na infraestrutura, processos ou após um incidente real.

8. Disposições Gerais

O não cumprimento das diretrizes estabelecidas neste Plano por parte dos colaboradores, especialmente das Equipes de Resposta designadas, será considerado uma falha grave de segurança.

Após a devida apuração, o descumprimento estará sujeito às penalidades administrativas e legais cabíveis, conforme a gravidade do ato e o impacto gerado à segurança dos pacientes ou à integridade dos dados do Hospital LISA.

Este plano considera as diretrizes das normas ISO 22301:2019 e ISO/IEC 27031:2011 como referência técnica para estruturação das estratégias de continuidade e recuperação.