Plano de Continuidade de Negócios – BCP

Empresa Fictícia: SmartHealth Systems

Introdução da Empresa e Cenário

A **SmartHealth Systems** é uma empresa de tecnologia médica especializada em sistemas hospitalares, prontuários eletrônicos e monitoramento de pacientes em tempo real através de dispositivos IoT.
A operação da empresa depende fortemente de seus servidores, da integridade dos dados dos pacientes e da comunicação contínua com hospitais parceiros.
A empresa possui:

- 80 funcionários;
- Um datacenter próprio e servidores em nuvem híbrida;
- Sistemas críticos operando 24h por dia;
- Contratos com hospitais que exigem alta disponibilidade e confiabilidade.

Uma interrupção pode causar falhas em atendimentos médicos, perdas financeiras e risco direto a vidas humanas.

Recursos Críticos Identificados

Recursos Humanos

- Equipe de TI (infraestrutura, segurança, banco de dados)
- Equipe de suporte técnico 24h
- Gestores de crises

Tecnologia da Informação

- Servidores de aplicação e banco de dados
- Sistema de prontuário eletrônico
- Plataforma IoT de monitoramento
- Backup diário em nuvem
- Firewall e serviços de segurança

Infraestrutura

- Datacenter local (energia, climatização)
- Links redundantes de internet
- No-break e gerador

Documentos e Registros

- Contratos com hospitais
- Documentos legais e licenças
- Políticas internas e manuais operacionais

Dependências Externas

- Fornecedores de internet
- Parceiros de nuvem (AWS/Azure)
- Fornecedores de dispositivos IoT
- Empresa de segurança física

Análise de Impacto nos Negócios (BIA)

Ameaças Identificadas

Ameaça	Probabilidade	Impacto	Consequência
Falha de energia no datacenter	Média	Alto	Paralisação total dos sistemas
Ataque cibernético (ransomware)	Alto	Muito Alto	Perda de dados, paralisação e multa
Falha nos dispositivos IoT	Média	Alto	Dados incorretos de pacientes
Indisponibilidade do link de internet	Alta	Alto	Hospitais sem acesso ao sistema
Incêndio / desastre físico	Baixa	Muito Alto	Perda total da infraestrutura
Erro humano	Média	Médio	Queda parcial de serviços ou dados

Impactos

- Interrupção dos atendimentos hospitalares
- Perda de reputação
- Multas contratuais e legais
- Risco à segurança dos pacientes
- Custos com recuperação e restauração

Tempos Máximos Permitidos de Interrupção

- Sistema de prontuário eletrônico: **1h**
- Plataforma IoT: **30 minutos**
- Banco de dados principal: **2h**
- Sistema administrativo interno: **24h**

Estratégias de Recuperação

1. Redundância e Infraestrutura

- Servidores espelhados em nuvem (cloud failover)
- Backups horários para dados críticos
- Replicação em tempo real do banco de dados
- Links de internet redundantes (dupla operadora)
- Gerador + no-break com autonomia de 8h

2. Segurança da Informação

- Firewall de última geração com IDS/IPS
- Antivírus corporativo com análise comportamental
- Criptografia de ponta a ponta (TLS 1.3)
- Autenticação multifator (MFA)
- Política rígida de controle de acesso (RBAC)

3. Continuidade Operacional

- Estação de trabalho emergencial para suporte 24h
- Datacenter secundário pronto para ativação
- Scripts automatizados de restauração

4. Comunicação de Crise

- Canal de comunicação interno via WhatsApp Business e Slack
- Contatos emergenciais de todos os colaboradores

- Comunicação direta com hospitais parceiros

5. Processos de Recuperação

- Restauração de backups (hot-site)
- Ativação do servidor em nuvem em caso de falha total
- Reconfiguração rápida de dispositivos IoT

Plano de Ação Detalhado

Etapa 1 – Detecção do Incidente

Responsável: Analista de TI + SOC
Ações:

- Identificar a natureza da falha (TI, cibernética, infraestrutura etc.)
- Registrar no relatório de incidente
- Acionar o gestor responsável

Etapa 2 – Ativação do BCP

Responsável: Gerente de Continuidade
Ações:

- Avaliar se o incidente atende aos critérios de ativação
- Comunicar equipes e parceiros
- Iniciar plano de comunicação

Etapa 3 – Resposta Imediata

Ações:

- Contenção da ameaça (isolar sistemas, bloquear rede, desligar componentes)
- Migrar serviços críticos para a nuvem (failover)
- Acionar redundâncias (links, energia)

Etapa 4 – Recuperação

Ações:

- Restaurar sistemas a partir do backup mais recente
- Testar integridade dos dados restaurados
- Validar funcionamento com hospitais parceiros

Etapa 5 – Retomada

Ações:

- Voltar para operação normal
- Registrar todos os passos
- Realizar reunião de pós-incidente
- Atualizar o BCP conforme melhorias identificadas

Sugestão de Teste do Plano

Para garantir a eficácia do BCP, recomenda-se:
Teste Proposto: Simulação de Ataque Cibernético (Ransomware)
Etapas:

1. Simular indisponibilidade total do servidor local.
2. Forçar equipes a ativarem o plano de contingência.
3. Executar failover para a nuvem.
4. Medir tempo até os sistemas ficarem online.

5. Testar acesso dos hospitais parceiros.
6. Registrar falhas, atrasos ou gargalos.
7. Realizar reunião de lições aprendidas.

Frequência: Semestral.