**1. Introdução da Empresa e Cenário**

**Nome da Empresa:** TechMed Solutions  
**Setor:** Saúde (Tecnologia para gestão hospitalar)  
**Resumo:** A TechMed Solutions é uma empresa fictícia que desenvolve soluções tecnológicas para o setor hospitalar, incluindo softwares de gestão e sistemas de armazenamento de dados médicos. Dado o seu papel crítico em ambientes de saúde, a TechMed precisa garantir a continuidade dos serviços e a proteção dos dados, inclusive em situações de crise.

**2. Recursos Críticos Identificados**

Para manter a TechMed funcionando sem interrupções, identificamos os seguintes recursos críticos:

* **Infraestrutura de Servidores:** Essencial para armazenar os dados de pacientes e operar o sistema de gestão.
* **Sistemas de Gestão Hospitalar:** Software central que gerencia informações de pacientes, exames e processos internos dos hospitais.
* **Equipe de TI e Suporte Técnico:** Responsável por garantir a operação contínua e solucionar problemas técnicos rapidamente.
* **Rede de Internet e Conectividade:** Conexão de alta disponibilidade é fundamental, pois a empresa depende da rede para realizar operações.
* **Sistemas de Backup e Armazenamento de Dados:** Backups regulares para evitar perda de dados e garantir rápida recuperação em caso de falha.

**3. Análise de Impacto nos Negócios (BIA)**

Abaixo, os eventos disruptivos mais críticos e seus possíveis impactos nos negócios da TechMed:

1. **Falha na Infraestrutura de TI (ex.: interrupção do servidor):**
   * **Impacto:** Indisponibilidade do sistema de gestão hospitalar, afetando diretamente o atendimento de pacientes e o fluxo hospitalar.
2. **Desastres Naturais (ex.: incêndios, enchentes):**
   * **Impacto:** Possível comprometimento físico dos equipamentos e servidores, levando à perda de dados e paradas operacionais.
3. **Ataques Cibernéticos (ex.: ransomware):**
   * **Impacto:** Comprometimento de dados sensíveis e paralisação de serviços críticos, com risco de perda de reputação e possíveis implicações legais.

**4. Estratégias de Recuperação Propostas**

Para minimizar o impacto de incidentes e garantir a recuperação rápida das operações, propomos as seguintes estratégias:

* **Redundância de Sistemas:** Implementação de servidores de backup geograficamente distribuídos para garantir acesso ininterrupto aos sistemas.
* **Backup de Dados:** Realização de backups automáticos diários e semanais, com armazenamento em nuvem e em local físico, visando a proteção contra perdas de dados.
* **Plano de Comunicação de Crise:** Estabelecimento de um plano de comunicação para informar a equipe interna e externa, assegurando uma resposta coordenada.
* **Treinamento em Segurança Cibernética:** Adoção de programas de treinamento contínuo para a equipe, visando fortalecer a prevenção contra ataques cibernéticos.

**5. Plano de Ação Detalhado**

As etapas para resposta e recuperação em caso de incidente são:

* **Etapa 1:** Notificação e Ativação do Plano de Recuperação – acionamento imediato da equipe de TI (Tempo estimado: 1 hora).
* **Etapa 2:** Migração para o Servidor de Backup – transferência dos dados para a estrutura de backup (Tempo estimado: 3 horas).
* **Etapa 3:** Verificação e Validação dos Dados – checagem completa dos dados para garantir integridade e segurança (Tempo estimado: 2 horas).
* **Designação de Responsabilidades:** Identificação dos membros da equipe responsáveis por cada etapa, incluindo equipe de TI, gerentes e colaboradores chave.

**6. Sugestão de Teste do Plano**

Para testar a eficácia do BCP, propomos uma simulação de um ataque cibernético. A simulação permite avaliar o tempo de resposta da equipe, a eficácia das medidas de recuperação e a comunicação entre os membros, ajustando possíveis falhas e aperfeiçoando o plano.