# Universidade São Judas Tadeu - Noturno

## Ciências da Computação

## Plano de Continuidade de Negócios (BCP)

### 1. Introdução da Empresa e Cenário

A empresa fictícia escolhida pelo grupo é a TechSolutions Solutions, uma startup da área de tecnologia da saúde. Ela desenvolve sistemas digitais para hospitais e clínicas, como prontuários eletrônicos e ferramentas para gestão médica. A sede é em Belo Horizonte, e a empresa atende instituições em vários estados do Brasil.  
  
Cenário: Recentemente, a empresa enfrentou um ataque cibernético que tirou do ar seus principais sistemas por cerca de 12 horas. Isso impactou diretamente o atendimento de hospitais parceiros.

### 2. Recursos Críticos Identificados

Os principais recursos que sustentam a operação da TechSolutions são:  
- Os servidores onde ficam hospedados os sistemas;  
- A plataforma de prontuário eletrônico usada pelos clientes;  
- A equipe de TI e suporte técnico;  
- O banco de dados com informações dos pacientes;  
- Os canais de comunicação com os clientes (chat, e-mail e telefone).

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

Entre os riscos mais relevantes que identificamos:  
- Falha nos servidores: Interrompe o acesso ao sistema, prejudicando o atendimento médico;  
- Ataque cibernético: Pode comprometer dados sensíveis e causar perda de confiança dos clientes;  
- Problemas na internet ou energia: Afetam o funcionamento da equipe e suporte;  
- Desastres naturais (enchentes, incêndios): Podem afetar o escritório ou o data center.  
  
Cada um desses eventos pode gerar prejuízos financeiros, perda de dados ou danos à imagem da empresa.

### 4. Estratégias de Recuperação Propostas

Para evitar ou amenizar esses impactos, propomos:  
- Ter servidores de backup em outra região geográfica;  
- Usar criptografia e autenticação em dois fatores para proteger os dados;  
- Fazer backup automático dos sistemas todos os dias;  
- Criar um canal de comunicação interna para emergências;  
- Treinar a equipe sobre como agir em situações críticas.

### 5. Plano de Ação Detalhado

Em caso de incidente:  
1. Identificação do problema: A equipe de TI analisa o que aconteceu e isola o sistema afetado;  
2. Comunicação: Informar imediatamente os clientes e os responsáveis internos;  
3. Ação de resposta: Restaurar o backup, aplicar correções e reforçar a segurança;  
4. Retomada: Após estabilização, monitorar o sistema por 48h;  
5. Relatório: Registrar o que ocorreu, as ações tomadas e lições aprendidas.  
  
Responsáveis:  
- Equipe de Segurança da Informação – identificar e conter o problema;  
- Suporte Técnico – restaurar os serviços;  
- Comunicação – manter clientes informados.

### 6. Sugestão de Teste do Plano

Sugerimos fazer uma simulação anual de um incidente, como uma queda de servidor, para treinar a equipe e avaliar o tempo de resposta. Também seria útil aplicar testes de backup e recuperação de dados com frequência.