Plano de Continuidade de Negócios (BCP)

Empresa Fictícia: TechData Solutions

---

1. Introdução da Empresa e Cenário

A **TechData Solutions** é uma empresa fictícia do setor de tecnologia especializada em serviços de gestão de dados, hospedagem em nuvem e processamento seguro de informações para pequenas e médias empresas. Seu modelo de negócio depende fortemente da disponibilidade contínua de servidores, segurança das informações e operação ininterrupta do suporte técnico.

A empresa opera com: - Um data center próprio; - Uma equipe de TI de plantão; - Serviços 24/7 para clientes corporativos; - Plataformas SaaS para gestão de dados.

Dada a criticidade dos serviços prestados, a TechData Solutions precisa de um **Plano de Continuidade de Negócios (BCP)** para garantir resiliência e confiabilidade em cenários de falhas ou desastres.

---

2. Identificação dos Recursos Críticos

Os principais recursos essenciais para o funcionamento da empresa são:

Infraestrutura tecnológica

- Servidores físicos e virtuais
- Banco de dados corporativo
- Rede interna e roteadores
- Sistemas de backup e armazenamento
- Plataforma de atendimento ao cliente

Recursos humanos

- Equipe de TI (infraestrutura, redes, suporte e segurança)
- Gerentes de projeto e analistas de sistemas

Processos críticos

- Monitoramento de servidores 24h
- Suporte técnico aos clientes
- Gestão e processamento dos dados armazenados

Informações sensíveis

- Bases de dados dos clientes
- Documentos operacionais internos
- Credenciais administrativas

---

3. Análise de Impacto nos Negócios (BIA)

A seguir, possíveis eventos disruptivos e seus impactos:

1. Falha de TI (queda de servidor)

- Impacto: indisponibilidade total dos serviços, perda de contratos, danos à reputação.
- Tempo máximo tolerável de inatividade (MTD): 2 horas.

2. Ataque Cibernético (ransomware)

- Impacto: perda de dados, vazamento de informações, paralisação completa.
- Consequências: multas, processos legais e quebra de confiança.

3. Desastre Natural (enchente no data center)

- Impacto: perda física de equipamentos e paralisação prolongada.
- Consequências: necessidade de ativar ambiente secundário.

4. Falha de Energia em larga escala

- Impacto: interrompe sistemas críticos e comunicação.
- Consequências: serviços inoperantes até restauração.

5. Indisponibilidade de funcionários essenciais

- Impacto: atrasos em reparos, queda na qualidade de suporte.
- Consequências: aumento do tempo de resposta e risco de perda de clientes.

---

4. Estratégias de Recuperação Propostas

Para minimizar os impactos identificados, as seguintes estratégias serão adotadas:

Redundância e continuidade tecnológica

- Ambiente de backup em nuvem (data center secundário);
- Redundância de servidores em cluster;
- Sistema automático de failover;
- UPS e geradores para manutenção de energia.

Segurança da informação

- Criptografia de dados em repouso e em trânsito;
- Sistema avançado de detecção de intrusão (IDS/IPS);
- Políticas rígidas de senhas e autenticação multifator;
- Atualizações e patches aplicados mensalmente.

Backup e recuperação de dados

- Backups diários automáticos em múltiplos locais;
- Testes quinzenais de restauração;

• Versionamento de arquivos para prevenção contra ransomware.

Comunicação em caso de emergência

• Grupo de WhatsApp corporativo de contingência;
• E-mails automáticos para clientes alertando sobre incidentes;
• Canal emergencial de suporte via telefone.

Gestão de recursos humanos

• Treinamento anual em resposta a incidentes;
• Escalonamento de responsabilidades;
• Formação de uma equipe de crise.

---

5. Plano de Ação Detalhado

Etapas de resposta e recuperação

1. **Detecção do incidente**
2. Monitoramento identifica falha ou ataque.
3. Notificação imediata ao gestor de TI.
4. **Avaliação inicial**
5. Verificar extensão do dano.
6. Classificar nível da crise.
7. **Acionamento do plano**
8. Equipe de crise assume controle.
9. Ferramentas de contingência são ativadas.
10. **Recuperação técnica**
11. Ativação do servidor secundário.
12. Restauração de backups.
13. Reconfiguração de sistemas.
14. **Comunicação**
15. Informar clientes sobre a situação.
16. Atualizar status a cada 30 minutos durante a crise.
17. **Retorno à normalidade**
18. Teste de estabilidade.

19. Retorno ao ambiente primário quando seguro.

20. **Relatório pós-incidente**

21. Documentar causa raiz.
22. Revisar eficácia do plano.

---

6. Sugestão de Teste do Plano

Para garantir que o BCP é eficaz, será realizado:

Simulado anual de crise:

- Simulação de ataque cibernético ou queda de servidor;
- Medição do tempo real de recuperação;
- Avaliação da comunicação interna e externa;
- Registro de falhas e pontos de melhoria.

Essa prática ajuda a empresa a verificar se os colaboradores conhecem seus papéis e se as estratégias funcionam na prática.

Este documento apresenta o esboço completo do Plano de Continuidade de Negócios (BCP) da empresa fictícia TechData Solutions.