UNIVERSIDADE SÃO JUDAS TADEU

Carlos Eduardo 825154398

Eduardo Oliveira 825137370

Felipe Cadena 825144852

Guilherme Garcia 824222500

Gustavo Cavalcante 82512399

Hugo Diniz 82515555

Bruno Henrique 825142649

Plano de Continuidade de Negócios (BCP) – GreenTech Solutions

Contexto:

A GreenTech Solutions é uma startup de tecnologia que desenvolve softwares e plataformas de monitoramento ambiental, focados em redução de carbono, otimização de consumo de energia e gestão de resíduos para empresas e cidades.

1. Identificação dos Recursos Críticos

Recursos/Sistemas	Função Principal
Servidores de Aplicação e Banco de Dados	Hospedam os softwares de monitoramento ambiental.
Plataforma Web e Aplicativos Móveis	Interface dos clientes com os produtos e serviços.
Equipe de Desenvolvimento e Suporte Técnico	Correções de bugs, atualizações e suporte a clientes.
Sistemas de Backup em Nuvem	Armazenamento seguro dos dados de clientes e operação.
Sistema de Comunicação Interna (e-mails, chats)	Coordenação interna rápida e eficiente.
Fornecedores de Internet e Energia	Serviços essenciais para operação contínua.

2. Análise de Impacto nos Negócios (BIA)

Evento Disruptivo / Ameaça	Descrição	Impacto Potencial	Nível de Impacto
Ransomware	Malware que sequestra dados e exige pagamento para desbloqueio.	Paralisação total, perda de dados, dano à imagem.	**Alto**
Phishing direcionado (spear phishing)	Ataque por e-mail para roubo de	Vazamento de dados, acesso	**Alto**

	credenciais de acesso.	indevido aos sistemas.	
Falha no servidor principal	Queda dos servidores que hospedam a plataforma.	Interrupção total dos serviços para os clientes.	**Alto**
Ataque DDoS (Negação de Serviço Distribuído)	Enchente de tráfego malicioso para tirar sistemas do ar.	Indisponibilidade da plataforma por horas ou dias.	**Alto**
Falha no fornecimento de energia	Interrupção de energia na sede física.	Paralisação local, possíveis atrasos no suporte.	**Médio**
Desastre natural (enchente/incêndio)	Danos físicos à sede, perda de equipamentos.	Interrupção crítica das operações.	**Alto**
Exposição acidental de dados	Vazamento por falha de configuração em nuvem ou repositórios.	Comprometimento de dados sensíveis, LGPD.	**Alto**
Equipe crítica indisponível	Doença, greve ou alta rotatividade de funcionários-chave.	Atrasos em suporte e manutenção.	**Médio**

3. Estratégias de Recuperação:

Backup de Dados:

- Backup automático diário em múltiplos provedores de nuvem (AWS, Azure).
- Políticas de recuperação rápida de dados (RTO - Recovery Time Objective - de 4 horas).

Plano de Comunicação de Emergência:

- Grupo de WhatsApp de crise para comunicação rápida entre diretoria e equipes chave.
- Comunicado automático para clientes via e-mail e redes sociais em caso de indisponibilidade.

Contrato com Fornecedores Alternativos:

- Internet: contrato ativo com dois provedores.

Energia:

- gerador de emergência e baterias UPS (Uninterruptible Power Supply).

Segurança Cibernética:

- Firewall avançado, antivírus atualizado, treinamentos frequentes de conscientização de segurança.

4. Plano de Ação

Fase 1: Identificação e Comunicação

- Detectar a falha/situação anormal.
- Acionar o Comitê de Continuidade de Negócios.
- Comunicar colaboradores e principais clientes.

Fase 2: Resposta Imediata

- Migrar operação para servidores de backup.
- Restaurar dados a partir do último backup (se necessário).
- Estabelecer atendimento de emergência ao cliente.

Fase 3: Recuperação Completa

- Analisar a causa raiz do problema.
- Corrigir falhas de infraestrutura ou segurança.
- Atualizar o BCP baseado nas lições aprendidas.

Designação de Responsabilidades:

Responsável	Atribuições
CTO	Coordenação técnica da recuperação de sistemas.
Gerente de Suporte	Comunicação com clientes e usuários afetados.
RH	Gerenciamento de equipe e realocação de pessoal.
CEO	Comunicação oficial com mídia e stakeholders.

Prazos:

- RTO (Recovery Time Objective): 4 horas para serviços essenciais.
- RPO (Recovery Point Objective): 1 hora (dados perdidos no máximo de 1 hora antes da falha).

5. Teste do Plano

Simulação de Cenário de Crise:

- Periodicidade: Teste a cada 6 meses.

Tipo de Teste:

- Simulação completa de queda dos servidores primários.
- Teste de recuperação de backup (restore de uma base de dados crítica).

- Simulação de phishing para avaliar resposta de segurança cibernética.

Relatório Pós-Teste:

- Avaliar tempo de resposta real x esperado.

- Identificar melhorias no processo.

- Atualizar o BCP conforme necessário.