PLANO DE CONTINUIDADE DE NEGÓCIOS

1. Introdução da empresa e seu cenário

A empresa TechFusion, localizada em São Paulo - Brasil, oferece tecnologia de software de alta qualidade (SaaS - Software as a Service), que emprega serviços de ERP (Enterprise Resource Planning), aplicativos de CRM (Customer Relationship Management) e suporte técnico online.

O público-alvo da organização são empresas de médio a grande porte, e que necessitam de alta segurança e confiabilidade de suas informações.

2. Recursos críticos identificados

Nos últimos 6 meses, a TechFusion teve que lidar com imprevistos que proporcionaram um grande prejuízo. Os principais foram:

- Falha de servidor: um dos principais servidores começou a apresentar falhas por causa da falta de manutenção e interrompeu o acesso de clientes por no mínimo 12 horas;
- Ataque cibernético: a empresa sofreu um ataque ransomware, o que ocasionou a perda de dados confidenciais dos clientes da TechFusion, prejudicando sua imagem e reduzindo drasticamente a sua confiança, tanto no mercado consumidor, quanto no de trabalho;
- Desastres naturais: devido às fortes tempestades ocorridas em São Paulo recentemente, o escritório teve de ser fechado dia 11 de outubro, sexta-feira à noite, e permaneceu sem energia por no mínimo 4 dias seguidos;
- Dependência profissional: a organização tem poucos funcionários que compreendem a sua infraestrutura técnica, o que causa uma dependência dos mesmos. Há o risco desses funcionários serem cortados e, causando ainda mais prejuízo para a empresa.

3. Análise de impacto nos negócios (BIA)

Falha no servidor

- Impacto: interrupção de serviço para os clientes de médio e grande porte, causando perdas na confiança e financeiramente.
- Tempo de Recuperação Aceitável (RTO): até 4 horas para evitar danos significativos.
- Perda de Dados Tolerável (RPO): Nenhuma. A interrupção não pode causar perda de dados devido ao armazenamento sensível.
- Impacto Financeiro: Perda equivalente ao período de inatividade.

Ataque Cibernético

- Impacto: Comprometimento de dados confidenciais de clientes e da empresa.
- Tempo de Recuperação Aceitável (RTO): 24 horas para retomar operações.
- Perda de Dados Tolerável (RPO): Idealmente nenhuma perda, no máximo de 1 hora caso backups sejam comprometidos.
- Impacto Financeiro: Possível perda de clientes, custos de resposta ao incidente e potenciais multas.

Desastres Naturais

- Impacto: Interrupção total dos serviços e operações físicas do escritório.
- Tempo de Recuperação Aceitável (RTO): 48 horas, implementando soluções alternativas de energia ou trabalho remoto.
- Perda de Dados Tolerável (RPO): Nenhuma, pois as operações e dados devem estar protegidos independente do local.
- Impacto Financeiro: Pode haver perda de produtividade e gastos com realocação temporária ou geradores.

Dependência Profissional

- Impacto: Risco de perda de continuidade dos serviços da empresa devido à baixa flexibilidade organizacional.
- Tempo de Recuperação Aceitável (RTO): Nenhum tempo de recuperação é aceitável.
- Impacto Financeiro: A falta de profissionais capacitados aumenta os custos de operação em caso de rotatividade.

4. Estratégias de recuperação propostas

Falha no servidor

- Backups Frequentes: Realizar backups automáticos e frequentes com replicação para servidores em outras localidades pode prevenir perdas significativas.
- Manutenção Preventiva: Desenvolver um cronograma de manutenção para prevenir problemas.

Ataque Cibernético

- Treinamento de Funcionários: Treinar os funcionários em práticas de segurança na manipulação de dados, reduzindo riscos.
- Plano de Resposta a Incidentes: Desenvolver um plano de resposta para casos de ataques, incluindo backups isolados da empresa que não possam ser afetados.

Desastres Naturais

- Backup de Energia: Instalar geradores e fontes de energia que não possam ser interrompidas.
- Locais Alternativos e Trabalho Remoto: Estabelecer um protocolo que permite os funcionários trabalharem remotamente.

Dependência Profissional

- Documentação Completa e Atualizada: Implementar uma política de documentação sobre a infraestrutura técnica da empresa.
- Cross-Training: Criar programas de treinamento para que outros usuários possam assumir em caso de ausência dos profissionais principais.

5. Plano de ação detalhado

5.1. Identifique o Essencial

Objetivo: Listar as atividades que não podem parar e os recursos para mantê-las funcionando.

Como fazer: Descubra quais áreas são mais importantes e de quais recursos, fornecedores e parceiros essas áreas dependem.

5.2. Avalie os Riscos

Objetivo: Saber os riscos que podem prejudicar a empresa.

Como fazer: Liste as ameaças mais prováveis (ex.: falha de energia, problemas no prédio) e entenda como isso afetaria as funções essenciais.

5.3. Crie Planos de Recuperação

Objetivo: Planejar maneiras de retomar as atividades rapidamente.

Como fazer: Defina o que será feito para cada função essencial, incluindo tempo de recuperação, locais alternativos de trabalho e backups.

5.4. Planeje a Comunicação

Objetivo: Ter uma estratégia de comunicação em caso de crise.

Como fazer: Organize uma lista de contatos e defina como e por onde informar funcionários, clientes e fornecedores.

5.5. Prepare a Equipe para Crises

Objetivo: Formar um grupo que saiba agir em uma crise.

Como fazer: Escolha a equipe responsável e treine-a sobre o plano e suas tarefas.

5.6. Documente e Obtenha Aprovação

Objetivo: Formalizar o plano e garantir que todos estão a par.

Como fazer: Coloque o plano no papel, com todos os detalhes, e peça aprovação da diretoria.

5.7. Atualize o Plano Sempre

Objetivo: Manter o plano sempre alinhado com a realidade da empresa.

Como fazer: Revise periodicamente e ajuste o plano sempre que a empresa passar por mudanças importantes.

6. Sugestão de teste do plano

6.1. Simule uma Situação de Crise

Objetivo: Ver se o plano funciona e se a equipe está preparada.

Como fazer: crie um cenário, suponha uma crise, como uma pane geral de servidores.

Reúna a equipe de crise: chame o grupo para decidir as ações.

Execute o plano: ponha em prática as etapas previstas.

Informe a todos: teste os canais de comunicação para avisar o pessoal.

6.2. Revise os Resultados e Melhore o Plano

Objetivo: identificar o que funcionou e o que pode melhorar.

Como fazer: após o teste, converse com a equipe para ajustar pontos fracos e incluir melhorias no plano.