Plano de Continuidade de Negócios (BCP) – TechData Solutions

1. Introdução da Empresa e Cenário

Nome da empresa: TechData Solutions

Setor: Tecnologia – Serviços de Análise de Dados e BI

Descrição: A TechData Solutions é uma startup que oferece soluções de análise de dados, dashboards e pipelines de integração para empresas de médio porte. Atua 100% online, utilizando infraestrutura em nuvem e fornecendo suporte remoto.

Cenário Operacional:

- 20 funcionários
- Operações críticas totalmente dependentes de TI
- Uso de servidores em nuvem (AWS/Azure)
- Atendimento ao cliente via e-mail, chat e plataforma própria
- Equipe distribuída (home office)

Contexto de Continuidade: A operação deve permanecer ativa mesmo diante de eventos disruptivos como falhas de servidores, perda de dados, ataques cibernéticos e interrupções de energia.

2. Identificação dos Recursos Críticos

Categoria	Recursos Criticos	Função
Infraestrutura de TI	Servidores em Nuvem	Hospedam a plataforma de dados e dashboards dos clientes
Sistemas Essenciais	Banco de Dados Principal	Armazena dados dos clientes e históricos de interação
Sistemas Essenciais	Sistema de Autenticação	Controle de acesso e segurança

Sistemas Essenciais	Ferramentas de Pipeline (ETL)	Integração e processamento de dados
Pessoas	Analistas de Dados	Atendem clientes e gerenciam pipelines
Pessoas	Equipe de Suporte	Resolve incidentes e opera o sistema
Comunicação	E-mail corporativo	Contato com clientes e parceiros
Comunicação	Plataforma de suporte	Abertura e acompanhamento de chamados
Documentação	Procedimentos internos	Manuais e protocolos
Segurança	Backups automáticos	Garantia de recuperação de dados

3. Análise de Impacto nos Negócios (BIA)

Eventos Disruptivos Analisados:

- Falha de servidor em nuvem
- Ataque de ransomware
- Queda de energia na sede administrativa
- Indisponibilidade do provedor de internet
- Perda ou corrupção de banco de dados
- Falha humana (exclusão acidental de dados)

Evento	Probabilidade	Impacto	Consequências	RTO	RPO
Falha de servidor	Média	Alto	Plataforma fora do ar	2h	15 min
Ransomware	Baixa	Muito Alto	Perda total ou sequestro de	4h	1h

			dados		
Queda de energia	Média	Médio	Equipe fica inoperante	1h	0
Falha de internet	Alta	Alto	Suporte indisponível	1–2h	0
Perda do banco	Baixa	Muito Alto	Clientes perdem dados	4h	15 min
Falha humana	Média	Alto	Dados excluídos incorretamente	2h	15 min

RTO = Tempo para recuperação | RPO = Perda máxima tolerável de dados

4. Estratégias de Recuperação Propostas

4.1 Redundância e Infraestrutura

- Servidores replicados em duas regiões de nuvem
- Load Balancer para redirecionamento automático
- Banco de dados em cluster, com réplicas síncronas

4.2 Backup e Restauração

- Backups automáticos a cada 15 minutos
- Armazenamento em nuvem isolada (bucket com versionamento)
- Teste de restauração mensal

4.3 Segurança Cibernética

- Firewall e WAF configurados
- Autenticação multifator (MFA) para colaboradores
- Monitoramento 24/7 de atividades suspeitas
- Plano de resposta a incidentes: isolar máquina, analisar logs, restaurar backups

4.4 Plano de Comunicação

- Enviar alerta interno via WhatsApp corporativo e e-mail
- Avisar clientes com comunicado automático na plataforma
- Designar porta-voz oficial para comunicação externa

4.5 Continuidade Operacional

- Equipe pode operar remotamente 100%
- Caso a internet caia, há modem 4G de contingência
- Protocolos documentados no repositório interno

5. Plano de Ação Detalhado

5.1 Papéis e Responsabilidades

Função	Responsável	Atividade
Líder de Continuidade	CTO	Coordenar ações durante incidentes
Equipe de TI	DevOps e Analistas	Ativar redundância, restaurar sistemas
Segurança da Informação	Especialista em Cyber	Investigar incidentes de segurança
Comunicação	Coordenador de CX	Comunicar clientes e status
Diretoria	CEO	Aprovar decisões críticas

5.2 Ações em Caso de Falhas (Exemplo: Falha de Servidor)

1. Detectar falha via monitoramento automático
2. Acionar equipe de TI imediatamente
3. Redirecionar tráfego para servidor secundário
4. Verificar integridade dos dados
5. Validar funcionamento completo do sistema
6. Comunicar clientes sobre normalização
7. Registrar o incidente em relatório pós-mortem

5.3 Ações em Caso de Ataque Cibernético

- Isolar máquinas afetadas
- Bloquear credenciais comprometidas
- Restaurar backup seguro
- Analisar logs e pontos de entrada
- Notificar clientes (se necessário)

- Ajustar controles de segurança
- Documentar lições aprendidas

5.4 Ações em Caso de Queda de Energia/Internet

- Acionar rede 4G de contingência
- Direcionar equipe ao modo remoto
- Reduzir operações não essenciais
- Manter comunicação com clientes

6. Sugestão de Teste do Plano

Simulação prática – "Dia do Incidente"

Cenário sugerido: Falha total do servidor principal

Etapas do exercício (1h):

- Desativação simulada do servidor
- Ativação de backup
- Verificação da comunicação interna
- Notificação simulada aos clientes
- Restauração dos dados
- Elaboração de relatório pós-teste

Objetivos do teste:

- Avaliar resposta da equipe
- Medir RTO e RPO reais
- Identificar falhas no plano
- Ajustar documentação