PLANO DE CONTINUIDADE DE NEGÓCIOS (BCP)

TechLink Solutions LTDA

PLANO DE CONTINUIDADE DE NEGÓCIOS (BCP)

Versão: 1.2
Data: 2025-11-11

1. Introdução

A TechLink Solutions é uma startup especializada em hospedagem de sites, manutenção de servidores em nuvem e desenvolvimento de sistemas web. Atende aproximadamente 200 clientes ativos, incluindo e-commerces e sistemas críticos que demandam alta disponibilidade.

Objetivo do documento: Estabelecer procedimentos e estratégias para garantir a continuidade das operações em eventos disruptivos, minimizando impactos financeiros e preservando a reputação da empresa.

2. Recursos Críticos Identificados

Recurso / Sistema	Descrição	Importância
Servidores de hospedagem (cloud)	Armazenam sites e dados dos clientes	Crítico
Banco de dados dos clientes	Informações contratuais e operacionais	Crítico
Sistema interno de gestão (ERP)	Controle financeiro, faturamento e suporte	Alto
Conectividade de internet	Comunicação com clientes e acesso à nuvem	Crítico

Equipe de TI	Administração, monitoramento e resposta a incidentes	Alto
Backup de dados	Cópias para recuperação	Crítico
Comunicação corporativa	E-mail, telefone e canais de suporte	Médio
Fornecedores cloud	AWS / GCP - infraestrutura principal e redundância	Crítico

3. Análise de Impacto nos Negócios (BIA)

Evento Disruptivo	Impacto Potencial	RTO	RPO	Probabilidade
Falha no servidor principal	Interrupção total dos serviços hospedados	4 horas	15 minutos	Média
Ataque de ransomware	Criptografia de dados e indisponibilidade	8 horas	Dependente de backup	Média
Queda de energia prolongada	Indisponibilidade dos servidores locais	6 horas	Sem perda se backups em nuvem	Baixa
Perda de conexão com Internet	Impossibilidade de acesso remoto e suporte	2 horas	N/A	Alta
Desastre natural (incêndio/enxurrada)	Danos físicos e perda de hardware	24 horas (com DR)	Até 24h dependendo da replicação	Baixa
Falha humana (erro de configuração)	Instabilidade parcial ou perda de dados	4 horas	15 min	Média

4. Estratégias de Recuperação

- Redundância geográfica: servidores espelhados em duas regiões com balanceamento de carga e failover automático.
- Backup e retenção: backups incrementais a cada 15 minutos para bases críticas; backups completos diários; retenção mínima de 30 dias.
- Procedimentos de restauração: playbooks detalhados para restauração automática e manual; scripts versionados em repositório seguro.
- Comunicação de crise: templates padronizados, lista de contatos atualizada, portal de status público e porta-vozes designados.
- Continuidade de energia e rede: nobreaks dimensionados, gerador local e múltiplos ISPs com failover automático.
- Segurança preventiva: segmentação de rede, EDR/antivírus, políticas de gestão de patches e controle de acessos.

5. Plano de Ação Detalhado

Etapa	Ação	Responsável	Prazo de Execução	Recursos Necessários	RTO Metas	RPO Metas	Observações
1	Identificação do incidente e ativação do Comitê de Crise	Gerente de TI / Analista de Segurança	Imediato	Sistema de monitoramento e alertas (PagerDuty, Grafana)	Imediato	N/A	Notificar Níveis 1 e 2 de escalonamento
2	Avaliação do impacto e priorização dos serviços críticos	Comitê de Crise	30 min	Relatórios de monitoramento e inventário de ativos	30 min	N/A	Definir serviços com SLA mais alto
3	Acionamento de servidores de backup / failover em nuvem	Administrador de sistemas	1 h	Infraestrutura redundante e scripts de failover	1-2 h	15 min	Validar integridade dos backups

4	Comunicação aos clientes e stakeholders	Gerente de Atendimento / Comunicação	1 h	Templates de e-mail, status page (Statuspage)	1 h	N/A	Informar estimativa de tempo e passos seguintes
5	Recuperação dos serviços principais e validação	Equipe de TI	Até 4 h	Backups, scripts de restauração, runbooks	Até 4 h	15 min	Testar endpoints críticos após restauração
6	Mitigação e correção de vulnerabilidades (se aplicável)	Analista de Segurança	24 h	Ferramentas de forense, logs	24 h	N/A	Isolar sistemas comprometidos
7	Auditoria pós-incidente e relatório final	Coordenador de Segurança / Compliance	24-72 h após resolução	Logs, evidências e timeline de ações	N/A	N/A	Lições aprendidas e ações preventivas

6. Sugestão de Teste do Plano

- Tipo de teste: Simulação controlada (failover) com intervenção limitada.

- Frequência: Semestral (teste completo) e trimestral (teste parcial).

- Objetivos: Validar RTO/RPO, comunicação, execução dos playbooks e retomada dos serviços críticos.

- Métricas de sucesso: RTO ≤ metas definidas, RPO ≤ metas definidas, comunicação eficiente em ≤1 hora.

- Registro: Checklist do teste, logs de execução e relatório com ações corretivas.

Anexos e Contatos

Comitê de Crise: Gerente de TI, Coordenador de Segurança, Gerente de Atendimento, Diretor Executivo.

Contatos de emergência:

- Gerente de TI: +55 11 9XXXX-XXXX (email: ti@techlink.com.br)

- Coordenador de Segurança: +55 11 9YYYY-YYYY (email: seguranca@techlink.com.br)

- Suporte Nível 1: suporte@techlink.com.br

Bruno de Oliveira Santos - 8232235123

Guilherme Dourado Nascimento - 825116419

Felipe Pereira do Nascimento - 825126069

Kauane Sandes Brandão - 825113309

Stephanny Ramos Rodrigues -825123391

Pedro Miranda Rabelo - 825243591