Davi Deosmar Batista Oliveira Miranda – RA: 823.212.282
Silas Rodrigues Nascimento – RA: 823.273.38

Plano de Continuidade de Negócios (BCP)

Histórico de versão

Data	Versão	Descrição
18/11/2025	1	Elaboração do Plano de Continuidade de Negócios

1. Introdução da empresa e seu cenário

A empresa internacional de Cloud Computing atua globalmente fornecendo serviços de infraestrutura em nuvem, incluindo máquinas virtuais, bancos de dados, armazenamento escalável e soluções corporativas sob demanda.

A matriz está localizada em Los Angeles (EUA) e conta com filiais distribuídas estrategicamente em São Paulo, Nova York, Estocolmo, Buenos Aires e outras capitais globais. Cada filial mantém datacenters robustos que hospedam os serviços dos clientes de acordo com a região escolhida para garantir baixa latência, melhor desempenho e conformidade regulatória local.

Toda a infraestrutura é monitorada continuamente e cada filial envia métricas de utilização, capacidade, segurança e performance para a matriz, que centraliza a análise e coordena ações preventivas e corretivas.

Objetivo

O objetivo geral deste documento é propor um conjunto de planos que possibilitem a disponibilidade dos serviços essenciais envolvendo TI durante as mais diversas situações de falhas e interrupções.

Benefícios esperados

Com a implementação deste conjunto de planos espera-se obter os seguintes benefícios:

a) capacidade de identificação proativa dos impactos de uma interrupção operacional;

b)capacidade de resposta eficiente às interrupções, o que minimiza o impacto à organização;

c) capacidade de gerenciar os riscos que não podem ser segurados;

d)infraestrutura mais resiliente e segura;

e) redução do impacto nos negócios;

f) restauração de serviços, sistemas e soluções de TI de forma mais rápida;

g)redução no volume de incidentes que impactam o negócio;

h)antecipação aos problemas;

i) minimização de interrupções dos serviços e sistemas; e

j) capacidade de demonstrar uma resposta possível por meio de um processo de testes.

2. Recursos críticos

• Datacenters regionais com energia redundante, climatização e segurança física.

• Hypervisors, clusters de virtualização e sistemas de orquestração de máquinas virtuais.

• Rede global com comunicação criptografada e links redundantes.

• Firewalls, IDS/IPS, WAF e sistemas de segurança cibernética.

• Plataformas de banco de dados, armazenamento em blocos, objetos e arquivos.

• Dashboard corporativo com métricas e telemetria em tempo real.

• Equipes de engenharia, SRE, segurança e suporte técnico 24/7.

• Sistemas de automação de criação, escalabilidade e distribuição de workloads.

3. Análise de Impacto nos Negócios (BIA)

Impactos avaliados:

• Queda total de um datacenter regional:

– Impacto: Crítico

– Consequências: interrupção de serviços regionais, violação de SLA, impacto financeiro.

• Congestionamento ou falha em backbone de rede global:

– Impacto: Alto

– Consequências: lentidão, interrupções na comunicação entre regiões.

• Comprometimento de dados ou incidentes de segurança:

– Impacto: Crítico

– Consequências: inviabilização dos serviços, danos à reputação e risco legal.

• **Interrupção de sistemas de gerenciamento de instâncias:**

– Impacto: Alto

– Consequências: falha na criação e manutenção de recursos críticos.

• **Falha de equipe técnica essencial por indisponibilidade ou emergência:**

– Impacto: Médio/Alto

– Consequências: demora na resposta a incidentes.

4. Estratégias de recuperação propostas

• Redundância geográfica entre datacenters com replicação síncrona e assíncrona.

• Failover automatizado com balanceamento inteligente entre regiões próximas.

• Backups contínuos (hourly snapshots) e backups externos (off-site).

• Firewall em alta disponibilidade e múltiplos provedores de internet.

• Esteiras de CI/CD com rollback automático em caso de falha crítica.

• Monitoramento 24/7 com dashboards, alertas e inteligência de ameaças.

• Plano de recuperação de desastres (DRP) com:

– RTO: 4 horas

– RPO: 5 a 15 minutos

• Treinamento anual obrigatório para equipes de emergência.

• Execução de simulações de ataques e falhas massivas (chaos engineering).

5. Plano de ação detalhado

1. Identificação imediata do incidente via alertas e logs.

2. Classificação do nível do incidente (baixo, moderado, alto, crítico).

3. Notificação da equipe de resposta e acionamento do comitê de crise.

4. Contenção inicial: isolamento da região, bloqueio de usuários/fluxos suspeitos, ativação de redundâncias.

5. Recuperação primária: failover para ambiente secundário.

6. Restauração de sistemas e dados utilizando backups validados.

7. Verificação de integridade: auditoria pós-incidente e testes de estabilidade.

8. Retorno ao ambiente original após validação técnica.

9. Documentação completa do incidente e relatório com plano de melhoria contínua.

6. Sugestão de teste do plano

• Teste anual completo de DRP (Disaster Recovery Plan).

• Simulação de falha total de datacenter com migração de carga em tempo real.

• Testes trimestrais de restauração de backup.

• Testes mensais de failover de rede e redundância de links.

• Exercícios de resposta a incidentes de segurança.

• Avaliação das equipes com treinamento e simulações práticas.

• Auditoria anual independente sobre segurança, continuidade e disponibilidade.