Sistema de Continuidade de Negócios (BCP)

1. Objetivo

Garantir que a RS - Servidores mantenha suas operações críticas (armazenamento, servidores e backup em nuvem) disponíveis em caso de incidentes como falhas técnicas, desastres naturais, ataques cibernéticos ou indisponibilidade de infraestrutura.

2. Análise de Riscos e Impacto

- **Falhas de energia elétrica** → risco de indisponibilidade total.
- **Falhas de hardware** (servidores, storage, switches).
- **Ataques cibernéticos** (ransomware, DDoS, invasões).
- **Desastres naturais** (enchentes, incêndios e etc.).
- **Erro humano** (configuração incorreta, exclusão acidental de dados).

Impacto:

- Interrupção dos serviços de cloud e backup.
- Perda de credibilidade e confiança de clientes.
- Multas e processos (LGPD e contratos de SLA).

3. Estratégias de Continuidade

1. **Redundância de Data Centers**
    - Estrutura replicada em dois locais diferentes (Indaiatuba + nuvem pública de apoio).
    - Replicação síncrona/assíncrona de dados críticos.
2. **Backup e Recuperação**
    - Backups diários automáticos em múltiplos locais.
    - Política de retenção (curto, médio e longo prazo).
    - Testes periódicos de restauração.
3. **Plano de Resposta a Incidentes**
    - Monitoramento 24/7 de infraestrutura e segurança.
    - Ações imediatas em caso de ataque (isolamento, bloqueio, rollback).
    - Comunicação rápida com clientes em caso de incidente.
4. **Gestão de Energia e Infraestrutura**
    - No-breaks (UPS) e geradores.
    - Sistema de climatização redundante.
    - Contratos com fornecedores críticos (energia, internet, hardware).

4. Plano de Comunicação

- **Interna**: equipe técnica acionada imediatamente via canais de emergência.
- **Clientes**: informados por e-mail, portal e telefone sobre a indisponibilidade e previsão de recuperação.
- **Investidores/Stakeholders**: relatório pós-incidente com medidas corretivas.

5. Procedimentos de Recuperação

1. Ativação do site secundário (failover automático/manual).
2. Recuperação de dados a partir dos backups.
3. Restauração da operação no data center principal.
4. Retorno ao estado normal com auditoria completa.

6. Treinamento e Testes

- Simulações semestrais de falha total.
- Testes de restauração de backup trimestrais.
- Treinamento contínuo da equipe em resposta a incidentes.

7. Política de Melhoria Contínua

- Revisão anual do plano.
- Inclusão de novas ameaças identificadas.
- Feedback de clientes e parceiros após incidentes reais ou simulados.