Atividade 1

Plano de Continuidade de Negócios (BCP) – Startup de Tecnologia: TI Flow

Objetivo:
Desenvolver um esboço de Plano de Continuidade de Negócios para a TI Flow, uma startup de tecnologia focada em soluções de TI e infraestrutura digital para empresas. O plano identifica riscos, recursos críticos, estratégias de recuperação e ações de resposta.

1. Identificação dos Recursos Críticos:
- Servidores de hospedagem de aplicações.
- Banco de dados dos clientes.
- Sistema de monitoramento em tempo real (NOC).
- Equipe técnica especializada.
- Conexão de internet de alta disponibilidade.
- Plataforma de atendimento ao cliente (Service Desk).
- Repositório de código e pipelines de deploy.

2. Análise de Impacto nos Negócios (BIA):
Possíveis eventos disruptivos:
• Falha de servidor ou indisponibilidade da nuvem.
• Ataque cibernético (ransomware, DDoS, vazamento de dados).
• Falha de energia na matriz.
• Erro humano em deploy.
• Quebra de equipamento crítico.
Impactos:
• Interrupção dos serviços prestados a clientes.
• Perda de reputação e confiança.
• Multas por descumprimento de SLA.
• Retrabalho técnico e aumento de custos operacionais.

3. Estratégias de Recuperação:
- Implementação de redundância em nuvem (multi-região).
- Backups automáticos horários e diários.
- Failover automático para ambiente secundário.
- Política de versionamento e rollback imediato em deploy.
- Firewall avançado e monitoramento 24/7.
- Comunicação emergencial via canais alternativos (grupo de crise, e-mail externo).
- Estações de trabalho sobressalentes para equipe técnica.

4. Plano de Ação:
- Ativação do Comitê de Crise em até 10 minutos após incidente.
- Ação rápida de diagnóstico pelo analista de plantão.
- Execução do processo de failover em até 15 minutos.
- Restauração de dados a partir de backup verificado.
- Comunicação imediata aos clientes com estimativa de normalização.
- Registro detalhado em relatório pós-incidente.

5. Teste do Plano:
Para assegurar a eficácia do plano, a TI Flow realizará:
• Teste semestral de simulação de indisponibilidade.
• Teste de restauração de backup.
• Simulação de ataque cibernético com resposta da equipe.
• Avaliação de tempo real de recuperação (RTO e RPO).