Atividade 2

Plano de Continuidade de Negócios (BCP) – Empresa: TI Flow

1. Introdução da Empresa e Cenário:
A TI Flow é uma startup de tecnologia especializada em infraestrutura de TI, soluções em nuvem, automação de ambientes corporativos e suporte técnico para empresas de diversos segmentos. A empresa opera com serviços críticos como manutenção de servidores, monitoramento 24/7, atendimento técnico e gestão de ambientes cloud. Como os serviços são essenciais para o funcionamento contínuo de seus clientes, a TI Flow necessita de um plano robusto de continuidade de negócios para garantir estabilidade e recuperação rápida em caso de incidentes.

2. Recursos Críticos Identificados:
- Servidores cloud e ambiente de virtualização.
- Banco de dados interno e dos clientes.
- Plataforma de Service Desk.
- Sistema de monitoramento NOC 24/7.
- Conexões de internet redundantes.
- Equipe técnica especializada (analistas, engenheiros e suporte).
- Ferramentas de versionamento e pipelines de deploy.
- Firewall e sistemas de segurança cibernética.

3. Análise de Impacto nos Negócios (BIA):
Eventos disruptivos possíveis:
• Falha de servidores ou instabilidade em provedores de nuvem;
• Ataque cibernético (DDoS, ransomware, invasões);
• Queda de energia elétrica ou falha estrutural;
• Erro humano em deploys ou atualizações;
• Quebra de hardware crítico.

Impactos principais:
• Interrupção nos serviços prestados aos clientes;
• Prejuízo financeiro e perda de contratos por SLA quebrado;
• Danos à reputação e à confiabilidade da empresa;
• Paralisação da operação interna;
• Retrabalho técnico e aumento de custos emergenciais.

4. Estratégias de Recuperação Propostas:
- Redundância em nuvem com failover automático entre regiões.
- Backups de banco de dados realizados de forma horária e diária.
- Ambiente de disaster recovery ativo em data center secundário.
- Plano de rollback para atualizações e deploys.
- Firewalls de última geração e monitoramento contínuo de ataques.
- Comunicação emergencial padronizada com clientes e equipe.
- Uso de equipamentos reserva (notebooks, modems, roteadores).

5. Plano de Ação Detalhado:
Etapas:
1. Identificação imediata do incidente pelo NOC (máximo 5 minutos).
2. Acionamento do Comitê de Crise (até 10 minutos).
3. Diagnóstico e validação do impacto.
4. Ativação do ambiente de contingência e failover (até 15 minutos).
5. Comunicação oficial aos clientes com previsão de retorno.
6. Registro de logs, evidências e documentação do incidente.
7. Restauração total do ambiente ou serviços afetados.
8. Reunião pós-incidente para análise de melhorias.

Responsáveis:
• Líder Técnico – coordenação da recuperação;
• NOC – monitoramento e diagnóstico inicial;
• Segurança da Informação – mitigação de riscos em caso de ataque;
• Suporte e Atendimento – comunicação com clientes.

Recursos necessários:
• Acesso aos sistemas de backup;
• Conexões alternativas de internet;
• Equipamentos reserva;
• Equipes treinadas e disponíveis em regime 24/7.

6. Sugestão de Teste do Plano:
Para avaliar a eficácia do BCP, a TI Flow realizará:
• Simulações semestrais de incidentes (queda de servidor, falha de energia, ataque DDoS);
• Testes trimestrais de restauração de backup;
• Avaliação de tempo real de resposta (RTO) e perda tolerável de dados (RPO);
• Treinamento interno para todos os colaboradores;
• Relatórios de desempenho e melhorias contínuas.