**Aula prática** - 22/10

Luan Bernardo Alves - **824134204**
Artur Rosa Correia - **824135943**

Elaboração de um Plano de Continuidade de Negócios – BCP: **ENEL**

**PRIMEIRA SITUAÇÃO CRÍTICA**

**1. Recurso Crítico:** Rede de Distribuição

**2. Análise de Impacto nos Negócios:** Falhas na rede podem causar interrupções no fornecimento de energia para grandes áreas, resultando em perdas financeiras, danos à reputação e insatisfação dos clientes.

**3. Estratégias de Recuperação:**

- Manutenção preventiva, com inspeções regulares e troca de equipamentos obsoletos.
- Criação de circuitos alternativos para garantir o fornecimento de energia em caso de falhas.
- Implementação de sistemas em tempo real para o monitoramento da rede, como sensores ou cameras.

**4. Plano de Ação:**

- Isolar o trecho afetado;
- Mobilizar as equipes de campo;
- Realizar os reparos e reenergizar a rede.
- Responsabilidades: Equipes de manutenção, engenheiros, centro de operações.
- Estabelecer metas  de prazo possivéis e claras para a restauração do serviço de acordo com a complexidade da falha.

**5. Teste de plano**:

Simulação de Desastres Naturais: Simular eventos como tempestades, enchentes ou más condições climáticas. Conseguindo assim avaliar a resposta da equipe em relação à velocidade, localização, reparo de danos na rede, comunicação com os clientes e funcionamento do plano de emergência.

**SEGUNDA SITUAÇÃO CRÍTICA**

**1. Recurso Crítico:** Plataforma de E-commerce

**2. Análise de Impacto nos Negócios:** Uma falha na plataforma pode interromper as vendas online, impactando diretamente a receita da empresa. Além disso, pode causar perda de dados de clientes e produtos, afetando a reputação da empresa e a relação com os clientes.

**3. Estratégias de Recuperação**:

- Realizar backups diários da plataforma e dos dados, armazenando-os em local seguro e acessível.

- Ter um ambiente de testes idêntico ao ambiente de produção para realizar testes e atualizações sem interromper as operações.

- Migrar parte da infraestrutura para a nuvem para garantir alta disponibilidade e escalabilidade.

**4. Plano de Ação:**

- Detectar a falha e isolar o problema.
- Ativar plano de recuperação de desastres.
- Restaurar o sistema a partir do último backup.
- Notificar os clientes sobre a interrupção e o tempo estimado para a resolução.
- Responsabilidades: Equipe de TI, gerente de e-commerce.

**5. Teste do Plano**:

- Simular uma falha na plataforma em um ambiente de testes, cronometrando o tempo de recuperação, a comunicação e coordenação dos funcionários, e as ocilações no sistema e no plano.

**TERCEIRA SITUAÇÃO CRÍTICA**

**1. Recurso Crítico:** Segurança Física das Instalações

**2. Análise de Impacto nos Negócios:** Intrusões, vandalismo, roubos e sabotagem podem causar danos às instalações, interrupção dos serviços, perda de equipamentos e materiais, além de colocar em risco a vida dos funcionários.

**3. Estratégias de Recuperação:**

- Implementar um sistema de vigilância por câmeras, alarmes e rondas de segurança.

- Controlar o acesso às instalações através de catracas, biometria e identificação por rádio frequência.

**4. Plano de Ação:**

- Evacuar a área, acionar os serviços de emergência, isolar a área afetada, realizar os reparos e retomar as atividades.

- Responsabilidades: Equipe de segurança e manutenção.

- Estabelecer um tempo máximo para controlar a situação e iniciar os reparos.

**5. Teste do Plano**:

- Realizar simulações com os seguranças em casos de invasões e assaltos, analisar a comunicação entre eles e a busca de ajuda exterior.

- Realizar simulações e exercícios de evacuação para garantir que todos os funcionários saibam como agir em caso de emergência.