Plano de Continuidade de Negócios (BCP) - ENEL

Identificação dos Recursos Críticos

A ENEL, sendo uma empresa de energia, depende de diversos recursos essenciais para garantir a entrega eficiente e ininterrupta de seus serviços. Alguns dos recursos críticos incluem:

Infraestrutura de Distribuição: Redes de transmissão e distribuição de energia elétrica.
Sistemas de Tecnologia da Informação:
Supervisory Control and Data Acquisition (SCADA) para monitoramento remoto da rede elétrica.
• Sistemas de gestão (ERP) e sistemas de faturamento.
• Equipamentos Críticos: Subestações, geradores e transformadores.
Recursos Humanos: Técnicos e operadores de campo, equipe de TI, equipe de segurança.
Fornecedores e Parceiros: Manutenção de equipamentos, fornecedores de combustíveis e materiais.
Centro de Operações: Infraestrutura responsável pelo controle e acompanhamento das operações 24/7.

Análise de Impacto nos Negócios (BIA)

Eventos Disruptivos e Impactos no Negócio:

Falha nos Sistemas de TI
Impacto no negócio:
Interrupção do monitoramento e controle remoto da rede.

Ataque Cibernético
Impacto no negócio:
Roubo de dados, paralisação de sistemas e perda de receita.

Desastre Natural:
Impacto no negócio:
Danos à infraestrutura e atraso na retomada de operações.

Falha de Equipamentos Críticos
Impacto no negócio:
Apagões e interrupção no fornecimento de energia.

Greves ou Falta de Mão de Obra
Impacto no negócio:
Redução na capacidade operacional.

Falta de Materiais:
Impacto no negócio:
Atrasos na manutenção de equipamentos.

Estratégias de Recuperação

Redundância de Sistemas: implementar servidores e datacenters de backup em locais diferentes para garantir o funcionamento dos sistemas de TI.

Backup de Dados: realizar backups diários dos sistemas críticos e armazená-los em locais seguros.

Plano de Comunicação em Emergências: estabelecer canais alternativos de comunicação com funcionários, clientes e fornecedores.

Contratos de Contingência com Fornecedores: manter contratos com fornecedores secundários para garantir insumos e serviços essenciais.

Plano de Manutenção Preventiva: monitorar continuamente os equipamentos para antecipar ou prevenir falhas.

Treinamento e Capacitação de Equipes: preparar os colaboradores para emergências, simulando cenários críticos periodicamente.

Plano de Ação para Resposta e Recuperação

Ativação do Comitê de Crise:
Convocar a equipe de resposta para coordenar ações.

Avaliação dos Danos**:**
Avaliar a extensão do impacto e priorizar ações.

Comunicação**:**
Informar clientes e autoridades via canais de comunicação e redes sociais.

Recuperação dos Sistemas de TI**:**

Restaurar sistemas críticos.

Retomada das Operações:
Reiniciar a distribuição de energia.

Avaliação Pós-Incidente:
Revisar falhas e elaborar melhorias para que, se possível, não volte a acontecer falhas.

Teste do Plano de Continuidade

Simulação de Cenário de Crise: Realizar um exercício prático que simule uma falha nos sistemas de TI ou uma interrupção na infraestrutura de rede, envolvendo todos os departamentos relevantes.

Teste de Backup e Recuperação: Verificar a integridade dos backups e o tempo necessário para restaurar os sistemas.

Treinamento das Equipes: Simular uma emergência para que os colaboradores se familiarizem com suas responsabilidades.

Avaliação de Fornecedores: Testar a eficiência de fornecedores de contingência em cenários críticos.