

BCP Enel

1. Identificação dos Recursos Críticos

Infraestrutura Energética

Centrais Elétricas: Usinas de geração de energia (hidrelétricas, termelétricas, parques eólicos e solares).

Rede de Distribuição: Sistemas de transmissão e distribuição de energia elétrica.

2. Tecnologia da Informação

Monitoramento e controle em tempo real das operações.

Gerenciamento de Ativos: Softwares para gestão e manutenção de ativos de infraestrutura.

3. Gestão Financeira

Sistemas integrados para gerenciar finanças, contabilidade e orçamento.

Faturamento e Cobrança: Sistemas para gestão de contas e cobrança de clientes.

4. Atendimento ao Cliente

Ferramentas para gerenciar o relacionamento com os clientes.

Plataformas de Atendimento: Sistemas de suporte ao cliente, incluindo bots e atendimento telefônico.

5. Gestão de Operações

Planejamento e Controle de Produção: Ferramentas para otimização da geração de energia.

Gestão de Projetos: Softwares para acompanhar projetos de expansão e modernização.

6. Análise de Dados e Inteligência

Sistemas para análise de dados operacionais e previsão de demanda.

Modelagem e Simulação: Ferramentas para simulação de cenários e otimização de recursos.

7. Segurança e Compliance

Gestão de Segurança da Informação: Sistemas de proteção de dados e cibersegurança.

Compliance Regulatório: Ferramentas para garantir conformidade com normas e regulamentações do setor.

8. Sustentabilidade e Inovação

Gestão de Sustentabilidade: Sistemas para monitorar e relatar indicadores de sustentabilidade.

Inovação e Pesquisa: Plataformas para pesquisa em novas tecnologias de geração e eficiência energética.

9. Comunicação Interna

Plataformas de Colaboração: Ferramentas como Microsoft Teams ou outras para comunicação entre equipes.

Gestão de Conhecimento: Sistemas para documentação e compartilhamento de melhores práticas.

2. Análise de impacto nos negócios

1º Exemplo: Tempestade; Incidente com prioridade crítica, pelo motivo de que afeta além de casas e apartamentos também prejudica hospitais, bancos, o bem-estar e segurança. Além disso, situações assim podem gerar riscos adicionais, como incêndios ou falta de aquecimento em ambientes frios.

2º Exemplo: Falha nas Contas da Enel; é um erro no sistema de faturamento da Enel, que pode resultar em cobranças incorretas para os clientes. Isso pode incluir cobranças duplicadas, valores excessivos ou a não geração de faturas, causando a falta de confiança e além de ser algo que mexa com dinheiro.

3º Exemplo: Atrasos na entrega de materiais: Se a empresa enfrentar dificuldades para obter materiais essenciais, como transformadores, cabos ou equipamentos de proteção, isso pode atrasar tanto projetos de manutenção quanto expansões planejadas. incidente moderado

3. Estratégias de Recuperação

Planos de Recuperação de Desastres : Ter um plano de recuperação detalhado e atualizado para cada tipo de falha ou desastre, com procedimentos claros sobre as etapas a serem seguidas em caso de falha total ou parcial nos sistemas. Inclui também a alocação de equipes e recursos em períodos críticos, como picos de consumo.

Backups e Redundância de Sistemas: Implementar backups regulares de dados essenciais e redundância nos sistemas críticos. Com isso, em caso de falha em um sistema, outro pode assumir sua função automaticamente, o que é particularmente importante em sistemas SCADA (Supervisory Control and Data Acquisition), que monitoram e controlam a distribuição de energia.

Automação e Monitoramento em Tempo Real: Sistemas de monitoramento e automação podem detectar falhas ou interrupções rapidamente. Na Enel, sistemas de monitoramento são cruciais para prever falhas e realizar manutenções preventivas.

4.Plano de Ação

1. Identificação da Falha

Monitoramento Contínuo: Os sistemas de monitoramento em tempo real devem identificar e registrar a falha imediatamente, fornecendo informações sobre a localização e a extensão do problema.

Classificação da Falha: Classificar a falha (leve, moderada, crítica) para determinar o nível de resposta necessário.

2. Notificação e Mobilização das Equipes

Alerta de Equipes de Resposta a Incidentes: Enviar notificações automáticas para as equipes de TI, engenharia elétrica, segurança e demais envolvidos.

Ativação do Centro de Operações: Em falhas críticas, um centro de operações de crise pode ser ativado para coordenar as ações e a comunicação.

Notificação aos Clientes e Partes Interessadas: Informar os clientes e outras partes afetadas sobre a falha e fornecer uma previsão preliminar de resolução.

3. Isolamento e Contenção da Falha

Isolamento da Área Atingida: Utilizar dispositivos de isolamento para desconectar a área afetada e evitar que o problema se propague.

Desvio de Fluxo de Energia: Redirecionar o fornecimento para outras rotas, se possível, para reduzir o impacto sobre o fornecimento de energia em outras áreas.

5. Teste do Plano

Simulação de Cenário de Crise: -Realizar exercícios práticos com cenários hipotéticos, como falha de sistemas ou ataque cibernético.

-Avaliar a capacidade de resposta das equipes, a eficácia da comunicação e a execução das estratégias de recuperação.

-Coletar feedback para melhorias e ajustes no plano. Então quando acontecer algo, analisar onde faltou ação e soluções para estar mais preparado se acontecer algo novamente.