# Plano de Continuidade de Negócios (BCP) - Athena Company

Este Plano de Continuidade de Negócios (BCP) foi desenvolvido para a Athena Company, uma empresa fictícia especializada na fabricação de equipamentos e máquinas hidráulicas. O objetivo é garantir a continuidade das operações em caso de eventos disruptivos, assegurando a resiliência dos processos críticos e minimizando impactos.

## 1. Identificação dos Recursos Críticos

- Máquinas industriais de usinagem e montagem  
- Sistemas de controle de produção e estoque (ERP)  
- Fornecimento de energia elétrica e hidráulica  
- Mão de obra especializada (engenheiros, técnicos)  
- Garagem de armazenamento e logística  
- Servidores e banco de dados com projetos e informações de clientes  
- Sistema de comunicação interno e externo

## 2. Análise de Impacto nos Negócios (BIA)

- Falha de energia elétrica: paralisação total da produção  
- Desastre natural (enchentes ou incêndio): danos às instalações e equipamentos  
- Ataques cibernéticos: perda de dados críticos e interrupção dos sistemas de controle  
- Ausência de funcionários-chave: comprometimento na operação de máquinas específicas  
- Falha no fornecimento de matérias-primas: atraso na produção e entrega de pedidos

## 3. Estratégias de Recuperação

- Instalação de geradores de emergência e sistemas UPS para continuidade elétrica  
- Backup diário dos dados em servidores na nuvem e locais externos  
- Contratação de fornecedores alternativos para insumos  
- Treinamento cruzado de funcionários para múltiplas funções  
- Plano de resposta a incidentes cibernéticos com firewall e antivírus avançados

## 4. Plano de Ação

- Definir responsáveis por cada frente de resposta a incidentes  
- Realizar simulações trimestrais de cenários de crise (ex: falha total de energia)  
- Estabelecer comunicação direta com fornecedores e transportadoras para retomada rápida  
- Manter estoque de segurança de peças essenciais  
- Comunicar clientes prioritários em caso de atraso, com prazos ajustados previamente

## 5. Testes do Plano

- Simulações de falha de energia e ataque cibernético programadas a cada semestre  
- Avaliação dos tempos de recuperação e ajuste dos procedimentos  
- Envolvimento de todos os setores nas simulações  
- Relatórios pós-teste para melhorias contínuas