

## **ATHENA COMPANY**

### **PLANO DE CONTINUIDADE DE NEGÓCIOS (BCP)**

#### **1 INTRODUÇÃO**

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

#### **2 IDENTIFICAÇÃO DOS RECURSOS CRÍTICOS**

Os recursos considerados essenciais para a manutenção das atividades da empresa são:

- 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 e técnicos);
- Garagem de armazenamento e logística;
- Servidores e banco de dados com projetos e informações de clientes;
- Sistema de comunicação interno e externo.

#### **3 ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)**

A análise de impacto nos negócios (Business Impact Analysis - BIA) contempla os seguintes cenários de risco:

- Falha de energia elétrica: paralisação total da produção;
- Desastre natural (enchentes ou incêndio): danos às instalações e aos 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 na entrega de pedidos.

## **4 ESTRATÉGIAS DE RECUPERAÇÃO**

Para mitigar os impactos e promover a rápida recuperação, foram definidas as seguintes estratégias:

- Instalação de geradores de emergência e sistemas UPS para garantir a continuidade do fornecimento elétrico;
- Backup diário dos dados em servidores na nuvem e em locais externos;
- Contratação de fornecedores alternativos para os insumos críticos;
- Treinamento cruzado de funcionários para atuação em múltiplas funções;
- Implementação de um plano de resposta a incidentes cibernéticos, incluindo firewall e antivírus avançados.

## **5 PLANO DE AÇÃO**

As ações operacionais e estratégicas para garantir a efetividade do BCP incluem:

- Definição de responsáveis por cada frente de resposta a incidentes;
- Realização de simulações trimestrais de cenários de crise (exemplo: falha total de energia);
- Estabelecimento de comunicação direta com fornecedores e transportadoras para retomada rápida das atividades;
- Manutenção de estoque de segurança de peças essenciais;
- Comunicação proativa com clientes prioritários em caso de atraso, com prazos ajustados previamente.

## **6 TESTES DO PLANO**

A validação contínua do plano será realizada por meio de:

- Simulações de falha de energia e ataques cibernéticos, programadas semestralmente;
- Avaliação dos tempos de recuperação e adequação dos procedimentos conforme os resultados;
- Envolvimento de todos os setores da empresa nas simulações;
- Elaboração de relatórios pós-teste para promover a melhoria contínua do BCP.