CORPORATIVO	POLÍTICAS
Plano de Continuidade do Negócio	Data: 27/08/2022
	Revisão: 20/01/23
	Número de Página: 1/2

Introdução à Continuidade do Negócio

Objetivo: O objetivo do plano de Continuidade do Negócio da DK2 é identificar as ameaças, corrigi-las para evitar um problema futuro e, saber lidar caso o problema aconteça, sendo o PCN suficiente para o funcionamento da operação.

Identificar Ameaças Potenciais: Análise de riscos periodicamente para identificar ameaças potenciais à segurança da informação, como vírus, ataques cibernéticos, falhas de hardware, entre outras.

Pontos Críticos: Identificar os sistemas e processos críticos para o negócio e como eles seriam afetados em caso de interrupção.

Plano de Contingência: Plano de contingência específico para lidar com ameaças identificadas e manter a continuidade dos negócios.

Testar e Treinar: Testamos os planos de contingência e treinamos os funcionários garantindo que eles estejam preparados para lidar com uma interrupção.

Atualize Regularmente: nosso plano de continuidade do negócio é atualizado regularmente para refletir mudanças no ambiente de negócios ou na tecnologia.

Equipe de Resposta a Incidentes: é importante ter uma equipe dedicada a monitorar os incidentes e responder rapidamente.

CORPORATIVO	POLÍTICAS
Plano de Continuidade do Negócio	Data: 27/08/2022
	Revisão: 20/01/23
	Número de Página: 2/2

Backup: Todos os colaboradores devem fazer um backup em um HD externo e entregar para a diretoria guardar em um local fora da base para garantia.

Monitoramento Constante: Monitorar continuamente o ambiente para detectar incidentes em tempo hábil.

Plano de Comunicação: Defina um plano de comunicação para manter os funcionários, parceiros e clientes informados em caso de interrupção.

Plano de Continuidade do Negócio

1 – Entrar em contato com a equipe de TI para diagnosticarem o ocorrido
2 – Solicitar o Backup da nuvem para a equipe de TI (Caso tenha atingido os arquivos)
3 – Solicitar ao Analista a planilha do Operacional para a Operação continuar em andamento
4 – Desligar todos os aparelhos da rede para que não sejam afetados de qualquer maneira
5 – Verificar com todos os departamentos se algo foi perdido e solicitar o Backup a equipe de TI
6 – Após o diagnóstico da equipe de TI fazer as trocas se necessário de firewall, antivírus ou Sistema.