TIPO : ATAQUE CIBERNÉTICO ALVO: TODOS	Folha de Reflexos **RANSOMWARE – INDISPONIBILIDADE** **MASSA DE ESTAÇÕES DE TRABALHO**	

1. Alerta

NÃO FAÇA	FAZER
NÃO APAGUE NADA : todas as informações serão utilizadas como prova para a investigação	**ALERTA O CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC) E O GERENTE DE SEGURANÇA SISTEMA DE INFORMAÇÃO**
NÃO ABRA ARQUIVOS OU DE APLICATIVOS CRIPTOGRAFADOS: a infecção deve ser interrompida	**COMPARTILHE TODAS AS INFORMAÇÕES COM O SOC** para avaliar a escala do ataque e as prioridades de resposta a emergências
	SIGA AS INSTRUÇÕES SOC

2. Ações emergenciais

1. **Isole sistemas críticos :**
   - Desconecte todas as redes
   - Desconecte o cabo de rede dos computadores
   - Desconectar conexões Wifi
2. **Desconecte todos os periféricos**
3. Avalie a extensão do comprometimento e **colete evidências**

3. Solução de continuidade

Fornecimento de um ambiente de trabalho virtualizado acessível pela Internet através de qualquer estação de trabalho por ordem de criticidade das atividades

4. Critérios para ativação do Plano de Continuidade de Negócios

É a unidade de tomada de decisão de crise que toma a decisão final da actividade, o PCA
Critério 1: 5% das estações de trabalho estão inutilizáveis
Critério 2: risco de disseminação de ransomware para outros sites/entidades/aplicativos