TIPO: CIBERATAQUE OBJETIVO: TODOS	Ficha Reflejos **RANSOMWARE – INDISPONIBILIDAD MASIVA DE PUESTOS DE TRABAJO**	

1. Alerta

NO HACER	HACER
NO ELIMINAR NADA: cualquier información se utilizará como prueba para la investigación	**ALERTAR AL SECURITY OPERATIONS CENTER (SOC) Y AL RESPONSABLE DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**
NO ABRIR ARCHIVOS NI APLICACIONES CIFRADOS: la infección debe detenerse	**COMPARTIR CUALQUIER INFORMACIÓN CON EL SOC** para evaluar la magnitud del ataque y las prioridades de intervención de emergencia
	SEGUIR LAS INSTRUCCIONES DEL SOC

2. Acciones de emergencia

1. **Aislar los sistemas críticos**:
   - Desconectar todas las redes
   - Desconectar el cable de red de los ordenadores
   - Desconectar las conexiones Wi-Fi
2. **Desconectar todos los periféricos**
3. Evaluar la magnitud del compromiso y **recabar las pruebas**

3. Solución de continuidad

Provisión de un entorno de trabajo virtualizado accesible desde Internet a través de cualquier puesto de trabajo por orden de criticidad de las actividades

4. Criterios de activación del Plan de Continuidad del Negocio

La unidad de gestión de crisis es la que toma la decisión final sobre la actividad, el PCA
Criterio 1: el 5 % de los puestos de trabajo no se pueden utilizar
Criterio 2: riesgo de propagación del ransomware a otros sitios/entidades/aplicaciones