Respuesta a ransomware

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Responsables de TI y gerencia de organizaciones de cualquier tamaño.

Qué hacer cuando un atacante cifra archivos o sistemas y exige un pago. El objetivo es detener la propagación, conservar la evidencia y recuperar la operación desde respaldos confiables.

Señales de que está ocurriendo

- Archivos que no abren y cambiaron de extensión.
- Nota de rescate en el escritorio o en las carpetas afectadas.
- Respaldos, copias de sombra o antivirus desactivados sin explicación.
- Uso alto de disco y CPU en varios equipos al mismo tiempo.
- Cuentas de administrador nuevas o inicios de sesión a horas inusuales.

Qué tan grave es

Crítica	Servidores, respaldos o varios sitios afectados; servicio al público detenido.
Alta	Varios equipos de un área cifrados; la operación continúa de forma parcial.
Media	Un solo equipo afectado y aislado, sin señales de propagación.

Primera hora

- [ ] **1.** Desconecta de la red los equipos afectados: cable y Wi-Fi. No los apagues.
- [ ] **2.** Desconecta los respaldos de la red de inmediato, incluidos los discos externos y la nube sincronizada.
- [ ] **3.** Deshabilita las cuentas que el atacante pudo usar, empezando por las de administrador.
- [ ] **4.** Avisa a gerencia y designa a una sola persona que coordine la respuesta.
- [ ] **5.** Toma fotos de la nota de rescate y anota hora, equipo y usuario de cada hallazgo.
- [ ] **6.** No contactes al atacante ni pagues antes de recibir asesoría técnica y legal.

Preparación (antes del incidente)

- Mantén respaldos con la regla 3-2-1: tres copias, dos medios, una fuera de línea.
- Prueba la restauración al menos cada trimestre; un respaldo que no se ha restaurado no cuenta.
- Activa verificación en dos pasos en accesos remotos, correo y cuentas de administrador.
- No expongas RDP ni paneles de administración a internet; usa VPN.
- Ten impresa la lista de contactos de emergencia: TI, proveedor, legal, aseguradora.

Detección y análisis

- Identifica la familia de ransomware por la nota y la extensión de los archivos.
- Determina el alcance: qué equipos, qué servidores, qué recursos compartidos.
- Busca el punto de entrada: correo, RDP expuesto, VPN sin parches o credenciales robadas.
- Revisa si hubo robo de datos antes del cifrado (tráfico saliente grande, herramientas de compresión).

Contención

- Segmenta la red para aislar las áreas afectadas de las sanas.
- Bloquea en el firewall las direcciones y dominios de comando y control identificados.
- Cambia las contraseñas de todas las cuentas con privilegios desde un equipo limpio.
- Suspende las tareas programadas y los accesos remotos hasta entender el alcance.

Erradicación

- Reinstala desde cero los equipos comprometidos; no confíes en una limpieza parcial.
- Corrige la vulnerabilidad o el acceso que usó el atacante antes de reconectar nada.
- Elimina cuentas, tareas y herramientas que haya dejado el atacante.
- Busca los indicadores del ataque en el resto de la red.

Recuperación

- Verifica que el respaldo sea anterior a la intrusión y esté libre de malware.
- Restaura primero los sistemas críticos para la operación, en una red aislada.
- Reconecta por etapas y vigila de cerca durante al menos dos semanas.
- Consulta nomoreransom.org por si existe un descifrador gratuito para esa familia.

Lecciones aprendidas

- Reúne al equipo en los 15 días siguientes y documenta la línea de tiempo.
- Registra qué funcionó, qué falló y qué controles habrían evitado el incidente.
- Actualiza este playbook y asigna responsables y fechas a cada mejora.

Evidencia que debes conservar

- Nota de rescate y una muestra de archivo cifrado.
- Registros de firewall, VPN, controlador de dominio y antivirus.
- Imagen de memoria y de disco de al menos un equipo afectado, si hay capacidad.
- Línea de tiempo con fecha, hora, acción y persona responsable.

Qué no hacer

- Apagar los equipos: se pierde la evidencia en memoria.
- Pagar el rescate sin asesoría: no garantiza la recuperación y puede tener implicaciones legales.
- Restaurar respaldos sobre equipos que no se han reinstalado.
- Conectar respaldos a la red antes de contener el ataque.

A quién avisar

- Gerencia y asesoría legal, desde la primera hora.
- Personal: qué pasó, qué no deben hacer y a quién reportar.
- Clientes y personas afectadas, si hubo exposición de sus datos.
- Ministerio Público, mediante denuncia con la evidencia reunida.
- Regulador de tu sector, si aplica (por ejemplo la SIB para entidades supervisadas).
- cert.gt, para orientación y para alertar a otras organizaciones.

Cuándo dar por cerrado el incidente

- Los sistemas críticos operan con normalidad y sin indicadores del ataque.
- El punto de entrada está identificado y corregido.
- Todas las credenciales con privilegios fueron cambiadas.
- El informe del incidente está entregado a gerencia.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Guía general de buenas prácticas; no sustituye asesoría legal ni técnica especializada para tu caso. No es un documento de una entidad gubernamental. Puedes copiarla y adaptarla citando la fuente (CC BY 4.0).