NETWORK SECURITY ALLIANCE

Crisis de ransomware

PLAN DE RESPUESTA A INCIDENTES

*Basado en el *Checklist de seguridad para tu empresa* del **Instituto De Ciberseguridad (ICS) CSIRT, Ransomware: Prevención y respuesta a la extorsión digital.**

CONTENIDO

INTRODUCCIÓN

PREVENCIÓN

CONTENCIÓN

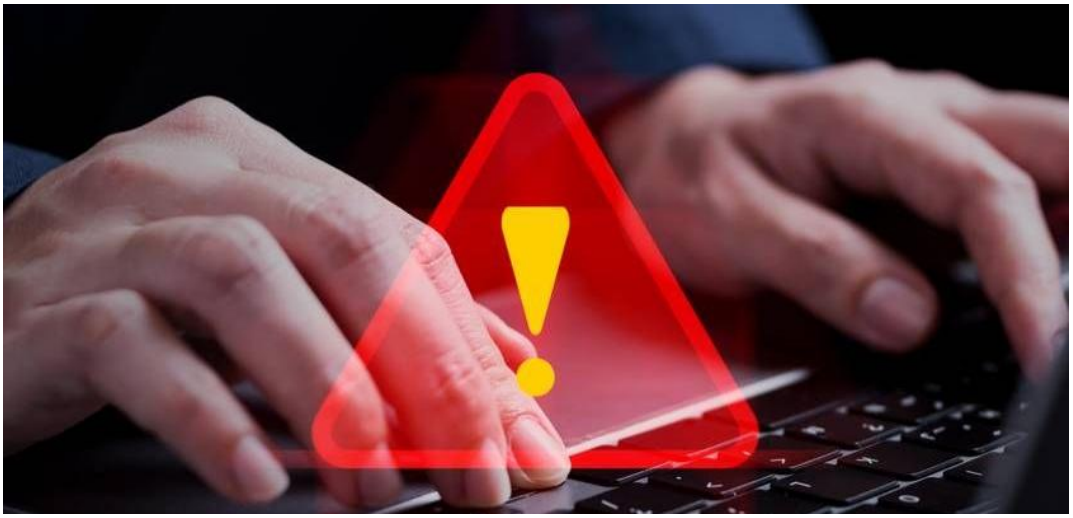
ERRADICACIÓN

RECUPERACIÓN

INTRODUCCIÓN

El ransomware está dirigido a usuarios domésticos, empresas y redes gubernamentales y puede provocar la pérdida temporal o permanente de información confidencial o de propiedad exclusiva, la interrupción de las operaciones regulares, las pérdidas financieras incurridas para restaurar los sistemas y archivos, y el daño potencial a la reputación de una organización. Nuestro Checklist de seguridad le permitirá tener una guía paso a paso para poder actuar ante posibles incidentes informáticos que sucedan en su organización, aunque este documento esté enfocado hacia la posible materialización de una infección de ransomware, es completamente funcional en caso de cualquier otro tipo de incidente que tenga la posibilidad de poner en riesgo la operación de su empresa al momento de afectar la disponibilidad de los recursos de la misma, sin importar si el in ves por desastres naturales, aplicaciones maliciosas, desgaste normal o mecánico u ocasionado por acciones humanas. Dentro de este Checklist usted encontrará una guía práctica para prevenir, contener, reaccionar y recuperar su organización de incidentes informáticos.

PREVENCIÓN



Objetivo

Implementar la triada preventiva (Usuarios, tecnología y políticas) cuya única finalidad es minimizar el área de impacto para reducir la posibilidad de sufrir un incidente con Ransomware hasta en un 90%. La prevención es tu mejor arma.

Procesos

Asegúrate de cumplir con las políticas de seguridad que se te han entregado, o con las que ya cuentas en tu organización, lo importante es darle seguimiento, no es lo mismo que digamos que contamos con políticas a que realmente las llevemos a cabo, esto va a ser una gran diferencia en la prevención de incidentes.

- Inventariado de activos: El inventario de tus equipos o activos informáticos y de información es importante, ya que nos permitirá el saber ¿a qué? ¿quién? ¿por qué? y ¿cómo? Tiene acceso a nuestros activos.

- Relación con proveedores: Controlar la relación con proveedores te ayudará a mantener nuestra información segura a través de acuerdos y contratos correspondientes.
- Copias de seguridad: Las copias de seguridad van a ser tu columna vertebral de seguridad en materia de prevención. Ver anexo Política Backup y Regla 3R.
- Culturización de usuarios: los usuarios forman parte de la estrategia de seguridad informática en la organización, es necesario no sólo educarlos en temas de seguridad, sino generar un ambiente de cultura organizacional en el que la seguridad esté incluida. Ver anexo Culturización.

Tecnología

- Anti-Malware: las soluciones antimalware son vitales para que podamos controlar nuestra organización en ambientes potencialmente hostiles. Léase el anexo Soluciones antimalware.
- Respaldos: Las soluciones de respaldos son de vital importancia a la hora de llevar a cabo nuestra política de copias de seguridad. Ver anexo Política Backup.
- Configuraciones: Las configuraciones por defecto pueden ser catastróficas al momento de no atenderse. Ver anexo Carpeta Hardening.
- Deshabilitar SMB1 Bloquear scripts Powershell Ej. (powershell Set-ExecutionPolicy -ExecutionPolicy Restricted)
- Bloquear Macros de documentos
- Deshabilitar, cambiar Puerto o uso de VPN para uso de servicio RDP
- Aplicación de mínimo privilegio
- Aplicación de 2FA
- Segmentación de redes
- Gestión de vulnerabilidades

Personas

- Culturización: La culturización lleva a los usuarios a no sólo conocer de posibles amenazas, sino a nosotros como personal de IT a detectar comportamientos maliciosos y poder atacarlos, convirtiendo a los usuarios en nuestra primera línea de defensa.

CONTENCIÓN

Si algo ha salido mal o no planeado, esta guía de contención de incidentes te dará la oportunidad de identificar qué es lo que tienes que hacer. Mantener la calma: Es momento de pensar con cabeza fría y nervios de acero, caso contrario sólo vamos a equivocarnos en algún proceso u omitir alguno

Paso 1: Aislar la infección

Es necesario cortar toda comunicación de nuestro paciente cero con el resto de nuestra red empresarial, por ello desconecta:

- Redes inalámbricas (Bluethoot, NFC)
- Red ethernet

Paso 2: Asegura tus respaldos

Aísla de la red los dispositivos o medios donde se encuentran tus copias de seguridad, esto por lo menos hasta que tengamos garantizado que la infección ha sido controlada.

Paso 3: Comunicar el incidente

En base a los planes de contingencia realizados, es necesario poner en práctica el plan de comunicación de incidentes, para que el resto de la organización realice sus procesos necesarios de contención.

Paso 4 (opcional): No reiniciar

Si apagamos o reiniciamos el equipo, el ransomware puede interrumpir su proceso de cifrado, dañando así tus archivos de por vida, o eliminando algunos.

- Mantenlo en modo de ahorro de energía
- Mantenlo aislado de la red

Paso 5: Copia de seguridad

Crea una copia de seguridad o imagen del equipo infectado, la mayoría de las veces los ransomware mantienen sus xploits en los equipos que le permitirán eliminar o sobrescribir los archivos cifrados después de cumplirse el tiempo del rescate.

Paso 6: Cuarentena

Si tu solución antimalware detectó el ransomware y lo puso en cuarentena, no lo elimines, con ello se puede encontrar la llave de eliminación de cifrado

Paso 7: Determinar el alcance de infección

Basado en nuestro inventario de activos es necesario realizar los siguientes pasos:

- Identificar las unidades de red asignadas al equipo infectado.
- Identificar carpetas compartidas en el equipo infectado con otros equipos.
- Identificar dispositivos de almacenamiento (o de cualquier tipo) en red.
- Identifica dispositivos extraíbles, usb, discos duros, etc. Conectados al equipo.
- Identifica los servicios de almacenamiento en la nube (Dropbox, One drive, Google drive) con carpetas mapeadas en el equipo infectado.

Paso 8: Identificar cepa del ransomware

Basado en las herramientas de identificación de ransomware como lo es EMSISOFT o NO MORE RANSOMWARE.

ERRADICACIÓN

Paso 1: Eliminar el malware

Para realizar la eliminación del malware es necesario haber realizado por lo menos la copia de seguridad con el equipo infectado, esto ayudará a tener la posibilidad de recuperar nuestra información en un futuro, y aplicar cualquiera herramienta de emergencia.

- Uso Kit de emergencia EMSISOFT

RECUPERACIÓN

Si algo ha salido mal o no planeado, esta guía de contención de incidentes te dará la oportunidad de identificar qué es lo que tienes que hacer. Mantener la calma: Es momento de pensar con cabeza fría y nervios de acero, caso contrario sólo vamos a equivocarnos en algún proceso u omitir alguno.

Opción 1: Copias de seguridad:

Restaurar copias de seguridad: para restablecer tus copias de seguridad de forma correcta debes realizar lo siguiente:

- Localizar copias de seguridad

1. Hay que asegurar que están todos nuestros archivos
2. Verificar la integridad de las copias de seguridad

- Eliminar el ransomware de los sistemas infectados

- Restablecer tus operaciones con tus procesos previos.

Opción 2: Eliminar cifrado

- Conocer el Ransomware: Determine la cepa y la versión del ransomware si es posible.
- Localizar un des-encriptador: puede que no haya uno para las nuevas cepas de ransomware.
- Reconectar: Adjunte cualquier medio de almacenamiento que contenga archivos cifrados (discos duros, memorias USB, etc.).
- Descifrar archivos.

Opción 3: Clientes y proveedores

- Localizar la última copia de seguridad: es necesario localizar por lo menos la última copia de seguridad que se tenga, ya sea de hace unos meses o hace unos años.
- Solicitar información: Solicitar a nuestros clientes y proveedores que nos envíen información previamente compartida con ellos.

Opción 4: Laboratorio de recuperación

- Copia de seguridad: Realizar una copia de seguridad del disco(s) duro(s) o dispositivo(s) afectado(s).
- Enviar activos: Realizar el envío de los activos para su análisis.
- Recuperar información: Solicitar de forma minuciosa qué información es la que se busca.

*Instituto de Ciberseguridad CSIRT Ransomware: Prevención y respuesta a la extorsión digital

Contáctanos

---

https://www.networksecurityalliance.com

https://www.networksecurityalliance.com

comercial@networksecurityalliance.com

CHECKLIST A EFECTUAR

PASO 1. Aislar la infección

Es necesario cortar toda comunicación de nuestro paciente cero con el resto de nuestra red empresarial, por ello desconecta:

- ☐ Corta red: Ethernet, Wi-Fi, Bluetooth/NFC y datos móviles/SIM.
- ☐ Pausa sincronizadores: OneDrive/Drive/Dropbox.
- ☐ Retira USB/docks/medios externos.
- ☐ Aísla con EDR/NAC (isolate host).
- ☐ Etiqueta: "Aislado – No usar / No reiniciar".

Tip rápido: Modo avión + quitar SIM + desenchufar cable/red + retirar docks/USB cubre la mayoría de vectores. Si quieres, te lo convierto en tarjetita checklist para tu playbook.

PASO 2: Asegura tus respaldos

Aísla de la red los dispositivos o medios donde se encuentran tus copias de seguridad, esto por lo menos hasta que tengamos garantizado que la infección ha sido controlada

- ☐ Desconecta NAS/appliances/medios de backup de la red.
- ☐ Configura solo lectura e inmutabilidad/WORM.
- ☐ Pausa replicaciones/sincronizaciones.
- ☐ Separa medios offline/offsite.
- ☐ Rota credenciales y limita accesos (MFA).

PASO 3: Comunicar el incidente

- ☐ Nombra Comandante del Incidente y dueño de comunicaciones.
- ☐ Abre War Room y canal único (#INC-{id}).
- ☐ Agenda updates periódicos (p. ej., cada 60 min).
- ☐ Notifica TI/SOC/Dir/Legal/PR según RACI.
- ☐ Registra todo y custodia evidencias.

Correo ejemplo para equipos de TI

Para: *TI Infraestructura; SOC; Seguridad; Service Desk*
CC: *Dirección de Tecnología; Legal/Compliance*
Hora/Fecha: *{HH:MM} (Hora CDMX), {DD/MM/AAAA}*

Asunto: *[REPORTE DE INCIDENTE – RANSOMWARE]*

Detección confirmada en {HOSTNAME} (INC-{AAAAMMDD}-{###})

Hola equipo de TI,

Les escribo para **reportar un problema** que acabamos de detectar.

Qué vimos (en palabras simples):
Aparecieron **mensajes extraños** pidiendo pago y varios **archivos cambiaron de nombre** y **ya no abren** en la computadora de **{NOMBRE}** del área **{ÁREA}**.

Cuándo pasó:
Hoy **{DD/MM/AAAA}** a las **{HH:MM} (hora CDMX)**.

Dónde está la persona:
{Oficina/Sitio/Trabajo remoto} – ubicación: **{lugar/piso/sucursal}**.

Equipo / Persona afectada:
Computadora de **{NOMBRE}** (usuario: **{correo o usuario}**).

Qué hicimos de inmediato (sin cosas técnicas):

- **Quitamos el internet** (Wi-Fi y cable) de esa computadora.

- **Dejamos de usarla**.
- **Tomamos fotos** de lo que sale en pantalla y las **adjuntamos**.

Qué podría estar afectado (lo que notamos):
Carpetas **{mencionar si son de trabajo compartidas o locales}** y archivos de **{tipo de archivos, p. ej., Word/Excel/Imágenes}**. No sabemos el alcance total.

Contacto para cualquier duda:
{Nombre y teléfono de quien reporta} / {Nombre de la persona afectada y teléfono}.

Adjunto: **capturas de pantalla** con lo que vemos.

Este mensaje es **solo para informar** del incidente. Quedamos pendientes de sus indicaciones.

Gracias,
{Nombre de quien envía}
{Puesto – Administración/Comercial/Mkt}
Network Security Alliance (NSA)

PASO 4. No reiniciar

Paso 5: Copia de seguridad

Crea una copia de seguridad o imagen del equipo infectado, la mayoría de las veces los ransomware mantienen sus xploits en los equipos que le permitirán eliminar o sobrescribir los archivos cifrados después de cumplirse el tiempo del rescate.

Preparación

☐ Medio externo limpio y offline con espacio suficiente (≥ 2× tamaño del disco origen).
☐ Bloqueador de escritura (si aplica) y equipo de adquisición confiable.
☐ Herramientas de imagen/hashing (para SHA-256/MD5) y reloj sincronizado.

Antes de la imagen (evidencia volátil, si TI lo permite y el cifrado no está activo)

☐ Captura de memoria (RAM) y lista de procesos/conexiones.
☐ Exporta logs clave (EDR, sistema, seguridad, VPN) del último día.
☐ Copia la nota de rescate y nombres/extensiones de archivos cifrados.

Imagen del sistema (bit a bit)

☐ No montes discos en lectura/escritura; desactiva auto-mount.
☐ Realiza imagen completa del/los discos (incluye espacio no asignado y sectores de arranque).
☐ Calcula y registra hashes (SHA-256/MD5) de la imagen al terminar.
☐ Verifica la imagen (comparación de hash / verificación de herramienta).

Copias selectivas adicionales (si procede)

☐ Perfiles de usuario (Documentos/Escritorio/Descargas).
☐ Carpetas de trabajo locales y archivos PST/OST (correo local).
☐ Programación de tareas, servicios, claves de inicio (arranque/Run).
☐ Sombras de volumen (estado), prefetch y archivos temporales.
☐ Discos/USB conectados y VMs/containers asociados (discos virtuales y snapshot de memoria si es posible).

Entornos virtuales y nube

☐ En VMs: crea snapshot de disco y memoria desde el hipervisor.
☐ En nube: snapshot inmutable de volúmenes (S3/Azure/GCP con retención/WORM).

Custodia y almacenamiento

☐ Etiqueta medios con ID de incidente, fecha y operador.
☐ Almacena offline (caja fuerte/almacén seguro) y, si es posible, en repositorio WORM/inmutable.
☐ Documenta cadena de custodia (quién, cuándo, cómo, dónde).

PASO 6. Cuarentena

Si tu solución antimalware detectó el ransomware y lo puso en cuarentena, no lo elimines, con ello se puede encontrar la llave de eliminación de cifrado

☐ Verifica archivo en Cuarentena (AV/EDR).
☐ No eliminar / no restaurar; extiende retención.
☐ Extrae muestra segura (ZIP con contraseña) y registra hashes.
☐ Mantén host aislado; no subas la muestra públicamente.

PASO 7. Determinar el alcance de infección

Mapear todos los lugares a los que el "paciente cero" pudo impactar para dimensionar el daño y priorizar contención.

☐ Identificar las unidades de red asignadas al equipo infectado.
☐ Lista de mapeos SMB/NFS/iSCSI (letras de unidad, rutas \\servidor\share o nfs://...).
☐ Registra: nombre del share, servidor, permisos del usuario, última hora de modificación observada.
☐ Identificar carpetas compartidas en el equipo infectado con otros equipos.
☐ Enumera shares locales y quién tiene acceso (lectura/escritura).
☐ Registra: ruta, permisos, equipos/usuarios que las usan y cambios recientes (archivos cifrados/notas).
☐ Identificar dispositivos de almacenamiento (o de cualquier tipo) en red.
☐ NAS/SAN, servidores de archivos, appliances de backup, cabinas iSCSI, montajes NFS/SMB.
☐ Registra: IP/hostname, rutas montadas, si hubo accesos o cambios en las últimas 24–48 h.
☐ Identificar dispositivos extraíbles conectados al equipo.
☐ USB, discos externos, SD/microSD, teléfonos (MTP), docking stations con almacenamiento.

☐ Registra: etiqueta/serie, contenido crítico, hora de conexión/desconexión (si se conoce).
☐ Identificar servicios de almacenamiento en la nube con carpetas mapeadas.
☐ Dropbox, OneDrive, Google Drive, iCloud, Box, etc. (carpetas sincronizadas locales).
☐ Registra: cuentas conectadas, rutas sincronizadas, estado de sync y archivos cambiados recientemente.

Verificación rápida de impacto (en cada ítem anterior)

☐ Muestreo de archivos: verifica si hay cifrado/notas en cada ubicación detectada.
☐ Tiempos: anota cuándo empezaron los cambios por carpeta/share (línea de tiempo).
☐ Permisos: valida si el usuario afectado tenía escritura (riesgo alto) o solo lectura.
☐ Listado final: arma una matriz con: recurso → impacto (sí/no) → evidencia → prioridad.

PASO 8. Identificar cepa del ransomware

Determinar la familia/variante del ransomware para saber si existe decryptor confiable y orientar la respuesta.

☐ Lista unidades de red mapeadas y shares locales.
☐ Identifica NAS/SAN y otros dispositivos en red.
☐ Registra USB/medios conectados.
☐ Revisa carpetas en la nube (OneDrive/Drive/Dropbox).
☐ Verifica impacto (archivos cifrados/notas) por recurso.

Resultado esperado

Ficha de identificación por incidente con: cepa/variante, evidencias cargadas, tools usadas, si existe decryptor (sí/no/en evaluación) y enlaces oficiales.

QUE NO HACER

- No **reconectar** ni **usar** el equipo afectado.
- No **borrar** evidencias ni **formatear** antes de la imagen.
- No **restaurar** backups hasta confirmar **contención**.
- No **desactivar** AV/EDR ni **levantar** cuarentenas.
- No usar **herramientas/decryptors no verificados** ni subir muestras públicamente.
- No **pagar/negociar** sin Legal/CSIRT.
- No **cambiar contraseñas** desde el equipo comprometido.
- No romper **cadena de custodia**.