RANSOMWARE: CÓMO RESPONDER

1. **SEGUIR EL PLAN DE RESPUESTA A INCIDENTES**
   Definir las funciones y capacitar a los contactos que participarán en la respuesta.
   Documentar las acciones tomadas y la información recopilada.

2. **CONTENER EL ATAQUE**
   Proteger los sistemas que no hayan sido comprometidos. Aislar los sistemas afectados.
   Conservar las pruebas.

3. **IDENTIFICAR EL *RANSOMWARE***
   Determinar qué *ransomware* se usó en el ataque y comprender su comportamiento.

4. **ANALIZAR LA INFORMACIÓN RECOPILADA**
   Comparar los *logs* y las pruebas con la información sobre el *ransomware*.
   Determinar la causa raíz y el alcance del ataque.

5. **ELIMINAR EL *RANSOMWARE***
   Eliminar el *malware* y los rastros dejados por el atacante. Volver a instalar y actualizar los sistemas comprometidos. Corregir las fallas explotadas por el ataque.

6. **CAMBIAR LAS CONTRASEÑAS Y REVISAR LOS ACCESOS**
   Cambiar las contraseñas de todas las cuentas. Habilitar la autenticación multifactor.
   Eliminar las cuentas y los privilegios agregados por el atacante.

7. **RESTAURAR LOS DATOS Y LA CONECTIVIDAD**
   Recuperar los datos de copias de seguridad confiables o, de ser necesario, verificar si hay descifradores para el *malware*. Volver a conectar los equipos a la red.

8. **MEJORAR EL ENTORNO CON LAS LECCIONES APRENDIDAS**
   Analizar y documentar el incidente. Reforzar el monitoreo y las medidas de seguridad. Actualizar el plan de respuesta a incidentes.

https://cert.br/docs/ransomware/es/responder/

cert.br

CERT.br (**https://cert.br/**) es un Grupo de Respuesta a Incidentes de Seguridad (CSIRT) con jurisdicción nacional y de último recurso, mantenido por NIC.br. Además de la gestión de incidentes, también trabaja en la sensibilización en temas de seguridad, conciencia situacional y transferencia de conocimiento, siempre respaldado por una fuerte integración con las comunidades de los CSIRT nacionales e internacionales.

nic.br

El Núcleo de Información y Coordinación del Punto BR - NIC.br (**https://nic.br/**) es una entidad civil de derecho privado y sin fines de lucro, encargada de la operación del dominio .br, así como de la asignación de números IP y del registro de Sistemas Autónomos en Brasil. Lleva adelante acciones y proyectos que benefician la infraestructura de Internet en Brasil.

lacnic

El Registro de Direcciones de Internet para América Latina y Caribe es una organización no gubernamental internacional, establecida en Uruguay en el año 2002. Su función es asignar y administrar los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región. Promueve y defiende los intereses de la comunidad regional y colabora en generar las condiciones para que Internet sea un instrumento efectivo de inclusión social y desarrollo económico de América Latina y el Caribe.
El LACNIC CSIRT es el equipo de respuesta a incidentes que apoya a todas las organizaciones miembros de LACNIC en la gestión de seguridad informática.

https://cert.br/docs/ransomware/es/

Septiembre / 2025

RANSOMWARE: CÓMO PROTEGERNOS

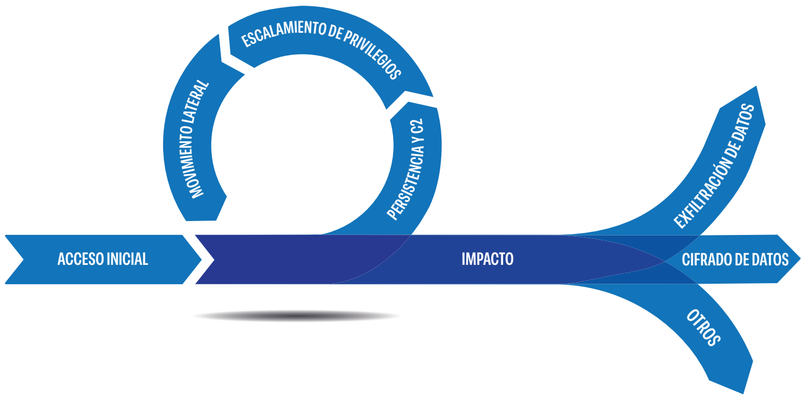
Descubra cómo funcionan los ataques, cómo proteger su red y prepararla para detectarlos, y cómo responder en caso de convertirse en víctima.

https://cert.br/docs/ransomware/es/

Apoyo de difusión:
lacnic csirt

Producción:
cert.br

RANSOMWARE: CÓMO SE PRODUCE



ACCESO INICIAL
El atacante invade la red de la empresa usando credenciales comprometidas, vulnerabilidades de *software*, ingeniería social o *malware*.

PERSISTENCIA Y C2
El atacante establece un acceso persistente y mecanismos de comunicación entre el sistema comprometido y la infraestructura de Comando y Control (C2).

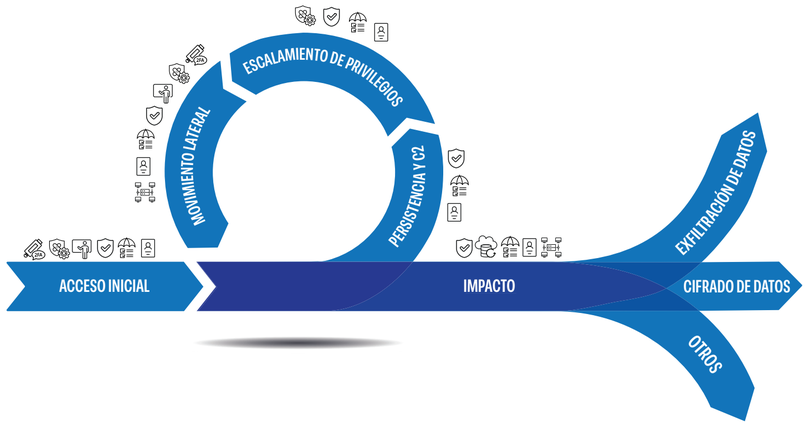
ESCALAMIENTO DE PRIVILEGIOS
El atacante obtiene permisos elevados que le permitan realizar tareas de administrador, acceder a datos confidenciales y moverse lateralmente dentro de la red.

MOVIMIENTO LATERAL
El atacante se mueve por la red, obtiene acceso a sistemas y datos críticos, y propaga el *ransomware* (*malware*) por el entorno para realizar el cifrado durante la fase de impacto.

IMPACTO
El atacante genera el máximo impacto posible para presionar a la empresa a pagar el rescate. Las técnicas más habituales son el cifrado y la exfiltración de datos.

https://cert.br/docs/ransomware/es/entender/

RANSOMWARE: CÓMO PROTEGERNOS



USAR AUTENTICACIÓN MULTIFACTOR (MFA)
Exigir autenticación multifactor para acceder a la red de forma remota, servicios web, servicios en la nube y usuarios con privilegios de administrador.

CONCIENTIZAR A LOS EMPLEADOS
Capacitar a los empleados y a terceros para que reconozcan e informen potenciales problemas de seguridad.

HACER COPIAS DE SEGURIDAD Y PROTEGERLAS
Hacer copias de seguridad periódicas. Mantener al menos una copia fuera de línea. Protegerlas contra accesos no autorizados y verificar periódicamente que los datos estén intactos y que la restauración funcione correctamente.

GESTIONAR IDENTIDADES Y ACCESOS
Otorgar a las cuentas solo los accesos esenciales y únicamente por el tiempo necesario.

GESTIONAR LAS VULNERABILIDADES
Gestionar las vulnerabilidades aplicando una estrategia de priorización basada en riesgos.

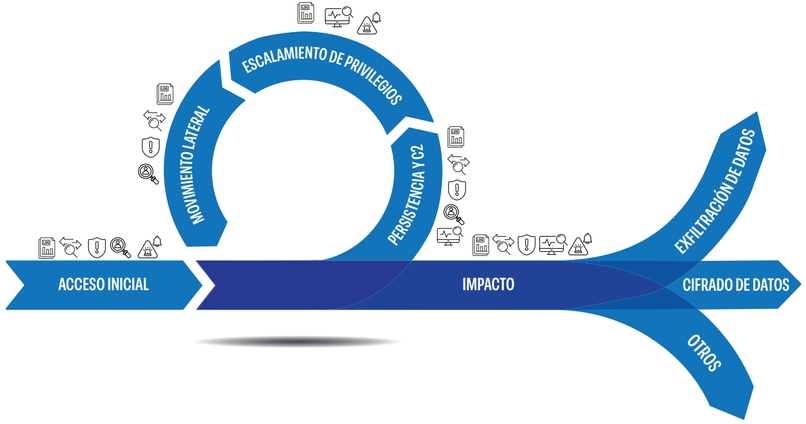
USAR HERRAMIENTAS DE PROTECCIÓN
Implementar herramientas de protección y monitoreo de la red.

REDUCIR LA SUPERFICIE DE ATAQUE
Desactivar los servicios que no se utilicen y no exponer los demás innecesariamente.

SEGMENTAR LA RED
Dividir la red en segmentos más pequeños e independientes.

https://cert.br/docs/ransomware/es/proteger/

RANSOMWARE: CÓMO DETECTARLO



HABILITAR Y ANALIZAR LOS *LOGS*
Habilitar y analizar los *logs* generados por los distintos equipos y sistemas. En dispositivos de red y *firewalls*, habilitar también los *netflows*.

OBSERVAR LAS ALERTAS DE LAS HERRAMIENTAS DE PROTECCIÓN
Observar las alertas de las herramientas de protección para detectar actividades sospechosas y, de ser posible, bloquearlas.

MONITOREAR EL USO DE LOS SISTEMAS
Monitorear el uso de los sistemas para detectar cambios en las configuraciones, transferencia y cifrado de datos, e instalación de *malware* y herramientas de acceso remoto.

MONITOREAR EL TRÁFICO DE RED
Monitorear el tráfico que entra y sale de la red, así como el tráfico interno entre las redes de la propia empresa.

MONITOREAR LAS CUENTAS DE USUARIOS Y ADMINISTRADORES
Monitorear la creación y los accesos indebidos a las cuentas de usuarios y administradores.

ESTABLECER UN CANAL PARA RECIBIR NOTIFICACIONES DE SEGURIDAD
Tener y divulgar un contacto para recibir notificaciones de seguridad, tanto de personas externas como de personas internas a la empresa.

https://cert.br/docs/ransomware/es/detectar/