MS-ISAC®
Multi-State Information Sharing & Analysis Center®

# Guía de #StopRansomware

Publicación: octubre de 2023

## Registro de cambios

| Versión | Fecha | Descripción de la revisión o del cambio | Sección o página afectada |
|---|---|---|---|
| 1.0 | Septiembre de 2020 | Versión inicial | |
| 2.0 | Mayo de 2023 | Página 3: Consulte “Novedades”. | Actualizaciones en todo el documento. |
| 3.0 | Octubre de 2023 | • Se agregó una viñeta en la sección del vector de acceso inicial para abordar las vulnerabilidades conectadas a Internet.<br>• Se actualizó la orientación sobre cómo reforzar el bloque de mensajes del servidor (SMB, por sus siglas en inglés).<br>• Se agregó información sobre los agentes de amenazas que se hacen pasar por empleados.<br>• Se agregó orientación sobre cómo reforzar los navegadores web.<br>• Se agregó una viñeta sobre las cantidades anormales de datos salientes a través de cualquier puerto.<br>• Se agregó la sección “Agradecimientos”. | • Vector de acceso inicial: vulnerabilidades conectadas a Internet y medidas de mitigación, página 7.<br>• Parte 1: Prácticas recomendadas de preparación, prevención y mitigación de ransomware y extorsión de datos, páginas 8 y 9.<br>• Vector de acceso inicial: formas avanzadas de ingeniería social, página 14.<br>• Prácticas recomendadas generales y orientación para el refuerzo, página 20.<br>• Parte 2: Lista de cotejo para respuestas a ransomware y extorsión de datos, página 24.<br>• Agradecimientos, página 30. |

## INTRODUCCIÓN

El ransomware es una forma de malware diseñada para cifrar archivos en un dispositivo, de manera que estos y los sistemas que dependen de ellos se vuelven inutilizables. Luego, los delincuentes exigen el pago de un rescate a cambio del descifrado. Con el tiempo, los agentes maliciosos han ajustado sus tácticas de ransomware para que sean más destructivas e impactantes, y también han exfiltrado datos de las víctimas, así como las han presionado para que paguen amenazándolas con publicar los datos robados. La aplicación de ambas tácticas se conoce como "doble extorsión". En algunos casos, los agentes maliciosos pueden exfiltrar datos y amenazar con publicarlos como única forma de extorsión sin emplear ransomware.

El ransomware y los incidentes de filtración de datos asociados pueden afectar gravemente los procesos comerciales e impedir que las organizaciones accedan a los datos necesarios para operar y brindar servicios fundamentales para la misión. Los impactos económicos y reputacionales del ransomware y de la extorsión de datos han demostrado ser desafiantes y costosos para organizaciones de todos los tamaños durante la interrupción inicial y, en ocasiones, la recuperación prolongada.

Esta guía es una actualización de la "Guía conjunta sobre ransomware" de la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) y el Centro de Análisis e Intercambio de Información de Varios Estados (MS-ISAC, por sus siglas en inglés), que se publicó en septiembre de 2020 (consulte "Novedades") y se desarrolló a través del JRTF. Esta guía incluye dos recursos principales:

- Parte 1: Prácticas recomendadas de prevención de ransomware y extorsión de datos
- Parte 2: Lista de cotejo para respuestas a ransomware y extorsión de datos

**Esta guía se desarrolló mediante el Grupo de Trabajo Conjunto contra el Ransomware (JRTF, por sus siglas en inglés) de EE. UU.**

El JRTF, presidido en conjunto por la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés) y la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés), es un esfuerzo colaborativo e interinstitucional para combatir la creciente amenaza de los ataques de ransomware. El JRTF se inició en respuesta a una serie de ataques de ransomware de alto perfil contra agencias gubernamentales y de infraestructura fundamental de EE. UU. El JRTF hace lo siguiente:

1. Coordina y agiliza la respuesta del Gobierno de EE. UU. a los ataques de ransomware y facilita el intercambio de información y la colaboración entre agencias gubernamentales y socios del sector privado.
2. Garantiza la coordinación operativa de ciertas actividades, como desarrollar y compartir las prácticas recomendadas para prevenir ataques de ransomware y responder a estos, realizar investigaciones y operaciones conjuntas contra agentes de amenazas de ransomware, y brindar orientación y recursos a las organizaciones que han sido víctimas de ransomware.
3. Representa un importante avance para permitir la unidad de iniciativas entre todos los esfuerzos del Gobierno de EE. UU. para abordar la creciente amenaza de los ataques de ransomware.

Para obtener más información sobre el JRTF, consulte cisa.gov/joint- ransomware-task-force.

La parte 1 proporciona orientación para que todas las organizaciones reduzcan el impacto y la probabilidad de incidentes de ransomware y extorsión de datos, incluidas las prácticas recomendadas para prepararse para estos incidentes, prevenirlos y mitigarlos. Las prácticas recomendadas de prevención se agrupan en vectores de acceso inicial comunes. La parte 2 incluye una lista de cotejo de las prácticas recomendadas para responder a estos incidentes.

Estas prácticas recomendadas y recomendaciones de prevención de ransomware y extorsión de datos, así como de respuesta a estos, se basan en la información operativa de la CISA, el MS-ISAC, la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) y la Oficina Federal de Investigaciones (FBI), en lo sucesivo denominadas "las organizaciones autoras". El público de esta guía incluye a los profesionales informáticos (IT,

por sus siglas en inglés), así como a otras personas que forman parte de una organización involucradas en el desarrollo de políticas y procedimientos de respuesta a incidentes cibernéticos o en la coordinación de la respuesta a incidentes cibernéticos.

Las organizaciones autoras recomiendan que las organizaciones tomen las siguientes medidas iniciales para preparar a sus instalaciones, miembros del personal y clientes, y protegerlos de las amenazas a la seguridad física y cibernética, así como de otros peligros:

- Unirse a un centro de análisis e intercambio de información (ISAC, por sus siglas en inglés) sectorial, cuando sea elegible, como los siguientes:
    - MS-ISAC para entidades gubernamentales estatales, locales, tribales y territoriales (SLTT, por sus siglas en inglés) de EE. UU.: learn.cisecurity.org/ms-isac-registration. La afiliación al MS-ISAC está disponible para representantes de los 50 estados, el Distrito de Columbia, los territorios de EE. UU., los Gobiernos locales y tribales, las entidades educativas públicas del jardín de infantes al 12.º grado (K-12, por sus siglas en inglés), las instituciones públicas de educación superior, las autoridades y cualquier otra entidad pública no federal en los Estados Unidos.
    - Centro de Análisis e Intercambio de Información sobre Infraestructuras Electorales (EI-ISAC, por sus siglas en inglés) para organizaciones electorales de EE. UU.: learn.cisecurity.org/ei-isac-registration. Consulte el Consejo Nacional de ISAC (National Council of ISACs) para obtener más información.
- Comunicarse con la CISA enviando un correo electrónico a CISA.JCDC@cisa.dhs.gov para colaborar en el intercambio de información, las prácticas recomendadas, las evaluaciones, los ejercicios y más.
- Comunicarse con la oficina local de la FBI para obtener una lista de puntos de contacto (POC, por sus siglas en inglés) en caso de un incidente cibernético.

La interacción con las organizaciones pares y la CISA permite que su organización reciba información fundamental y oportuna, y acceda a servicios para administrar el ransomware y otras amenazas cibernéticas.

## Novedades

Desde la publicación inicial de la ”Guía sobre ransomware” en septiembre de 2020, los agentes de ransomware han acelerado sus tácticas y técnicas.

Para mantener la relevancia, agregar perspectiva y maximizar la efectividad de esta guía, se han realizado los siguientes cambios:

- Se incorporó el esfuerzo #StopRansomware en el título.
- Se agregaron recomendaciones para prevenir los vectores comunes de infección inicial, incluidas las credenciales puestas en riesgo y las formas avanzadas de ingeniería social.
- Se actualizaron las recomendaciones para abordar las copias de seguridad en la nube y la arquitectura de confianza cero (ZTA, por sus siglas en inglés).
- Se amplió la lista de cotejo para respuestas a ransomware con consejos de búsqueda de amenazas para detectarlas y analizarlas.
- Se adaptaron las recomendaciones de acuerdo con los Objetivos de Desempeño de Ciberseguridad (Cybersecurity Performance Goals, CPG) Intersectoriales de la CISA.

> #StopRansomware es el esfuerzo de la CISA y la FBI para publicar avisos dirigidos a los defensores de redes que detallen información de defensa de redes relacionada con las diversas variantes de ransomware y los agentes de amenazas. Visite stopransomware.gov para obtener más información y leer los avisos conjuntos.

# Parte 1: Prácticas recomendadas de preparación, prevención y mitigación de ransomware y extorsión de datos

Estas prácticas recomendadas se alinean con los CPG que desarrolló la CISA y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés). Los CPG proporcionan un conjunto mínimo de prácticas y protecciones que la CISA y el NIST recomiendan que todas las organizaciones implementen. La CISA y el NIST basaron los CPG en marcos y orientación de ciberseguridad establecidos para brindar protección contra las amenazas, las tácticas, las técnicas y los procedimientos más comunes e impactantes. Para obtener más información sobre los CPG y las protecciones de referencia recomendadas, consulte los Objetivos de Desempeño de Ciberseguridad (CPG) Intersectoriales de la CISA.

## Preparación para incidentes de ransomware y extorsión de datos

Consulte las prácticas recomendadas y las referencias que se indican en esta sección para ayudar a administrar los riesgos que plantea el ransomware e impulsar una respuesta coordinada y eficiente para su organización en caso de un incidente. Aplique estas prácticas en la mayor medida posible según la disponibilidad de recursos organizacionales.

- **Mantenga copias de seguridad cifradas y sin conexión de los datos fundamentales**, y pruebe periódicamente la disponibilidad e integridad de las copias de seguridad en un escenario de recuperación ante desastres [CPG 2.R]. Pruebe los procedimientos de respaldo periódicamente. Es importante que las copias de seguridad sean sin conexión, ya que la mayoría de los agentes de ransomware intentan encontrar y, posteriormente, eliminar o cifrar las copias de seguridad accesibles para hacer que la restauración sea imposible, a menos que se pague el rescate. Con frecuencia, los agentes de ransomware buscan y recopilan credenciales almacenadas en el entorno atacado, y utilizan esas credenciales para intentar acceder a las soluciones de respaldo. También utilizan las vulnerabilidades públicamente disponibles para atacar las soluciones de respaldo sin correcciones.

  > Las copias de seguridad automatizadas en la nube pueden no ser suficientes porque, si un atacante cifra los archivos locales, estos archivos se sincronizarán con la nube y posiblemente sobrescribirán los datos no afectados.

  - Mantenga y actualice periódicamente “imágenes doradas” de los sistemas fundamentales. Esto incluye mantener “plantillas” de imágenes que tengan un sistema operativo (OS, por sus siglas en inglés) preconfigurado y aplicaciones de software asociadas que se puedan implementar rápidamente para reconstruir un sistema, como una máquina virtual o un servidor [CPG 2.O].
    - Utilice la infraestructura como código (IaC, por sus siglas en inglés) para implementar y actualizar recursos de la nube, y mantenga las copias de seguridad de los archivos de plantillas sin conexión para volver a implementar los recursos rápidamente. Se deben controlar las versiones del código de IaC y se deben realizar auditorías de los cambios en las plantillas.
    - Almacene el código fuente o los ejecutables aplicables con copias de seguridad sin conexión (así como los acuerdos de licencia y de depósito en garantía). La reconstrucción a partir de imágenes del sistema es más eficiente, pero algunas imágenes no se instalarán correctamente en hardware o plataformas diferentes; en estos casos, es útil tener acceso independiente al software.
  - Conserve el hardware de respaldo para reconstruir los sistemas si no es preferible reconstruir el sistema principal.
    - Considere reemplazar el hardware obsoleto que inhibe la restauración con hardware actualizado, ya que el hardware más antiguo puede presentar obstáculos de instalación

o compatibilidad al realizar la reconstrucción a partir de imágenes.

- Considere utilizar una solución de múltiples nubes para evitar depender de un proveedor para las copias de seguridad de nube a nube, en caso de que todas las cuentas del mismo proveedor se vean afectadas.
    - Algunos proveedores de nube ofrecen soluciones de almacenamiento inmutable que pueden proteger los datos almacenados sin la necesidad de un entorno separado. Utilice el almacenamiento inmutable con precaución, ya que no cumple los criterios de conformidad de determinadas normativas, y una configuración incorrecta puede suponer un costo significativo.

- **Cree, mantenga e implemente periódicamente un plan de respuesta a incidentes (IRP, por sus siglas en inglés) cibernéticos básico y un plan de comunicaciones asociado que incluya procedimientos de respuesta y notificación** para incidentes de ransomware y filtración o extorsión de datos [CPG 2.S]. Garantice la disponibilidad de una copia impresa del plan y de una versión sin conexión.
    - Proporcione notificaciones de filtración de datos a terceros y entidades reguladoras de conformidad con la ley.
    - Asegúrese de que el director ejecutivo (CEO, por sus siglas en inglés) o alguien equivalente revise y apruebe el IRP y el plan de comunicaciones por escrito, y que ambos se revisen y comprendan en toda la cadena de mando.
    - Revise la orientación de respuesta a incidentes disponible, como la lista de cotejo para respuestas a ransomware de esta guía y el "Manual de respuesta a incidentes cibernéticos" de la Asociación Estadounidense de Energía Pública (American Public Power Association), para lo siguiente:
        - Ayudar a su organización a organizarse mejor en torno a la respuesta a incidentes cibernéticos.
        - Crear un borrador de declaraciones de retención de incidentes cibernéticos.
        - Desarrollar un plan de respuesta a incidentes cibernéticos.
    - En el plan de comunicaciones, incluya los procedimientos de comunicación de la organización, así como plantillas para las declaraciones de retención de incidentes cibernéticos. Llegue a un consenso sobre qué nivel de detalle es apropiado compartir dentro de la organización y con el público, y cómo fluirá la información.

- **Implemente una arquitectura de confianza cero** para evitar el acceso no autorizado a datos y servicios. Haga que la aplicación del control de acceso sea lo más detallada posible. La ZTA asume que una red se puso en riesgo y proporciona una colección de conceptos e ideas diseñados para minimizar la incertidumbre a la hora de aplicar decisiones de acceso precisas y con los mínimos privilegios por solicitud en los servicios y sistemas de información.

## Prevención y mitigación de incidentes de ransomware y extorsión de datos

Consulte las prácticas recomendadas y las referencias que se indican en esta sección para ayudar a prevenir y mitigar incidentes de ransomware y extorsión de datos. Las prácticas recomendadas de prevención se agrupan en vectores de acceso inicial comunes de agentes de ransomware y extorsión de datos.

### *Vector de acceso inicial: configuraciones incorrectas y vulnerabilidades conectadas a Internet*

- **No exponga servicios, como el protocolo de escritorio remoto, en la web**. Si estos servicios deben exponerse, aplique los controles compensatorios adecuados para evitar las formas comunes de mal uso y explotación. Todas las aplicaciones del sistema operativo y los protocolos de red que sean innecesarios deben estar deshabilitados en activos conectados a Internet. [CPG 2.W]

- **Realice análisis periódicos de vulnerabilidades a fin de identificar y abordar las vulnerabilidades**, especialmente en dispositivos conectados a Internet, para limitar la superficie de ataque [CPG 1.E].
    - La CISA ofrece un servicio de análisis de vulnerabilidades sin costo y otras evaluaciones gratuitas: cisa.gov/cyber-resource-hub [CPG 1.F].
- **Corrija el software y los sistemas operativos, y actualícelos a las últimas versiones disponibles de forma periódica**.
    - Priorice la corrección oportuna de los servidores con conexión que operan software para el procesamiento de datos de Internet, como navegadores web, extensiones del navegador y lectores de documentos, especialmente para las vulnerabilidades explotadas conocidas.
    - Las organizaciones autoras, conscientes de las dificultades que tienen las pequeñas y medianas empresas para mantener actualizados los servidores conectados a Internet, instan a migrar los sistemas a proveedores de nube "administrados" y confiables con el propósito de reducir (no eliminar) las funciones de mantenimiento del sistema para los sistemas de identidad y correo electrónico. Para obtener más información, visite la página de información sobre ciberseguridad de la NSA: Mitigación de vulnerabilidades en la nube.
- **Asegúrese de que todos los dispositivos en las instalaciones, de servicios en la nube, móviles y personales (p. ej., "traiga su propio dispositivo" [BYOD, por sus siglas en inglés]) estén configurados correctamente y que las características de seguridad estén habilitadas**. Por ejemplo, deshabilite los puertos y protocolos que no se utilizan con fines comerciales (como el protocolo de escritorio remoto [RDP, por sus siglas en inglés]: puerto `3389` del protocolo de control de transmisión [TCP, por sus siglas en inglés]) [CPG 2.X].
    - Reduzca o elimine las implementaciones manuales y codifique la configuración de recursos de la nube a través de IaC. Pruebe las plantillas de IaC antes de la implementación con herramientas de análisis de seguridad estáticas para identificar las configuraciones incorrectas y las deficiencias de seguridad.
    - Compruebe periódicamente si hay cambios en la configuración para identificar recursos que se cambiaron o introdujeron fuera de la implementación de plantillas, lo que reduce la probabilidad de que se introduzcan nuevas deficiencias de seguridad y configuraciones incorrectas. Aproveche los servicios de los proveedores de nube para automatizar o facilitar los recursos de auditoría a fin de garantizar una referencia coherente.
- **Limite el uso de RDP y otros servicios de escritorio remoto**. Si el RDP es necesario, aplique las prácticas recomendadas. Los agentes de amenazas a menudo obtienen acceso inicial a una red a través de servicios remotos expuestos y mal asegurados, y, luego, atraviesan la red utilizando el cliente de RDP nativo de Windows. Los agentes de amenazas también suelen obtener acceso explotando redes privadas virtuales (VPN, por sus siglas en inglés) o utilizando credenciales puestas en riesgo. Consulte el aviso de la CISA, Seguridad de la VPN empresarial.
    - Realice una auditoría de la red para detectar sistemas que utilicen RDP, cierre los puertos de RPD sin utilizar, implemente bloqueos de cuenta tras un número específico de intentos, aplique la autenticación de múltiples factores (MFA, por sus siglas en inglés) y registre los intentos de inicio de sesión con el RDP.
    - Actualice las VPN, los dispositivos de infraestructura de red y los dispositivos que se utilizan para acceder de forma remota a los entornos de trabajo con las últimas correcciones de software y configuraciones de seguridad.
    - Implemente la MFA en todas las conexiones de VPN para aumentar la seguridad. Si no se implementa la MFA, exija a los teletrabajadores que utilicen contraseñas de 15 o más caracteres.

- Deshabilite la versión 1 del protocolo del bloque de mensajes del servidor (SMB) y actualícelo a la versión 3 (SMBv3) después de mitigar las dependencias establecidas (en sistemas o aplicaciones existentes), ya que pueden fallar al deshabilitarse. SMBv3 se lanzó por primera vez como parte de las actualizaciones de Microsoft Windows 8 y Windows Server 2012, Apple OS X 10.10 y el núcleo de Linux 3.12.
- Refuerce SMBv3 implementando la siguiente orientación, ya que los agentes maliciosos utilizan el SMB para propagar el malware entre las organizaciones.
    - Exija el uso de SMBv 3.1.1. Esta versión contiene protecciones de seguridad mejoradas, incluida la integridad de la autenticación previa, el cifrado del estándar de cifrado avanzado (AES, por sus siglas en inglés) mejorado y la criptografía de firma. El protocolo SMBv 3.1.1 es compatible de forma nativa con el núcleo de Linux, Apple y Windows, así como con muchos otros sistemas de almacenamiento externos. En Microsoft Windows 10 y Windows Server 2019, Windows 11 Preview Build 25951 y versiones posteriores, puede exigir las protecciones de SMBv 3.1.1, como la negociación de dialectos con clientes. Para obtener más información, consulte la página de Microsoft: Protección del tráfico SMB contra la interceptación | Usar SMB 3.1.1 y La administración de dialectos de SMB ahora es compatible en Windows Insider.
    - Bloquee las comunicaciones del SMB innecesarias:
        - Bloquee el acceso externo del SMB hacia y desde las redes de la organización mediante el bloqueo del puerto 445 del TCP de entrada y salida en los cortafuegos perimetrales de Internet. Bloquee los puertos `137`, `138` y `139` del TCP. **Nota:** SMBv2 y las versiones posteriores no utilizan los datagramas NetBIOS. El hecho de continuar usando SMBv2 no presenta riesgos significativos, así que puede usarse cuando sea necesario. Se recomienda actualizarlo a SMBv3 cuando sea posible.
        - Bloquee o limite el tráfico interno de SMB para que las comunicaciones solo se produzcan entre sistemas que lo requieran. Por ejemplo, los dispositivos Windows necesitan comunicaciones del SMB con controladores de dominio para obtener la directiva de grupo, pero la mayoría de las estaciones de trabajo de Windows no necesitan acceder a otras estaciones de trabajo de Windows.
        - Configure los sistemas de Microsoft Windows y Windows Server para que requieran el protocolo de seguridad de Internet (IPsec, por sus siglas en inglés) basado en Kerberos para las comunicaciones laterales del SMB, a fin de evitar que los agentes maliciosos accedan a comunicaciones mediante SMB detectando sistemas que no sean miembros de los dominios de Microsoft Active Directory de una organización.
        - Deshabilite el servicio de servidor de SMB (“Servidor”) en los dispositivos Microsoft Windows y Windows Server en los casos en que no sea necesario acceder de forma remota a los archivos o nombrar interfaces de programación de aplicaciones (API, por sus siglas en inglés) de canalización.
        - Para obtener más información, consulte la página de Microsoft Proteger el tráfico SMB en Windows Server.
    - Considere exigir el cifrado de SMB. Para garantizar que los clientes de SMB 3.1.1 siempre utilicen el cifrado de SMB, debe deshabilitar el servidor de SMB 1.0. Para obtener más información, consulte la página de Microsoft Mejoras de seguridad SMB | Habilitación del cifrado SMB y Menor desempeño después de habilitar el cifrado o la firma de SMB.
    - Si el cifrado de SMB no está habilitado, solicite la firma de SMB tanto para el cliente como para el servidor de SMB en todos los sistemas. Esto evitará ciertos ataques de adversario en el medio y de paso de hash.
      Para obtener más información sobre la firma de SMB, consulte la página de Microsoft Introducción a la firma del bloque de mensajes del servidor.

- Requiera la autenticación de Kerberos reforzando la convención de nomenclatura universal (UNC, por sus siglas en inglés). Ciertos sistemas operativos, como Microsoft Windows 10, Windows Server 2016 y versiones posteriores, refuerzan automáticamente la UNC para las conexiones al dominio de Microsoft Active Directory a través de los recursos compartidos SYSVOL y NETLOGON. Además, los administradores de red pueden configurar manualmente el refuerzo de la UNC para servidores y recursos compartidos en cualquier sistema operativo Microsoft Windows compatible. Para obtener más información, consulte la página de Microsoft Una vulnerabilidad en la directiva de grupo podría permitir la ejecución remota de código. El uso de direcciones de protocolo de Internet (IP, por sus siglas en inglés) para conectarse a los servidores de SMB producirá el uso de la autenticación NTLM, a menos que también configure el uso de nombres principales de servicios (SPN, por sus siglas en inglés) de Kerberos con direcciones IP. Consulte la página de Microsoft Configuración de Kerberos para direcciones IP.
- Utilice SMB a través del protocolo Conexiones UDP rápidas en Internet (QUIC, por sus siglas en inglés). Los clientes de Microsoft Windows 11, Windows Server 2022 Datacenter: Azure Edition y Android con un cliente de SMB de terceros admiten el uso de SMB a través de QUIC, una alternativa de SMB a través de TCP. El protocolo QUIC siempre está cifrado con Seguridad de la capa de transporte (TLS, por sus siglas en inglés) 1.3 y utiliza la autenticación de certificado para encapsular todo el tráfico del SMB, incluida la propia autenticación del SMB, dentro de un transporte similar a la VPN. SMB a través de QUIC permite a los usuarios móviles conectarse de forma segura a través de la Internet pública a los recursos perimetrales de SMB, como los servidores en el borde de las redes organizacionales que no están completamente detrás de un cortafuegos, pero también funciona en redes internas que requieren la mayor seguridad de transporte del SMB. Para obtener más información, consulte la página de Microsoft SMB a través de QUIC.
- Registre y supervise el tráfico del SMB [CPG 2.T] para ayudar a detectar comportamientos potencialmente anormales y dañinos.

### *Vector de acceso inicial: credenciales puestas en riesgo*

- **Implemente la MFA resistente a la suplantación de identidad para todos los servicios**, en particular para el correo electrónico, las VPN y las cuentas que acceden a sistemas fundamentales [CPG 2.H]. Informe a la alta dirección si descubre sistemas que no permiten o no aplican la MFA, así como usuarios que no están inscritos en la MFA.
    - **Considere emplear una MFA sin contraseña** que reemplace las contraseñas con dos o más factores de verificación (p. ej., una huella digital, el reconocimiento facial, el pin del dispositivo o una clave criptográfica).
- **Considere suscribirse a servicios de supervisión de credenciales** que supervisen la Internet oscura en busca de credenciales puestas en riesgo.
- **Implemente sistemas de administración de identidades y accesos (IAM, por sus siglas en inglés)** a fin de proporcionar a los administradores las herramientas y tecnologías necesarias para supervisar y administrar las funciones y los privilegios de acceso de entidades de red individuales para aplicaciones en las instalaciones y en la nube.
- **Implemente un control de acceso de confianza cero** mediante la creación de políticas de acceso sólidas para restringir el acceso tanto de usuario a recurso como de recurso a recurso. Esto es importante para los recursos de administración de claves en la nube.
- **Cambie los nombres de usuario y las contraseñas de administrador predeterminados** [CPG 2.A].
- **No utilice cuentas de acceso raíz para las operaciones diarias**. Cree usuarios, grupos y funciones para llevar a cabo tareas.

- **Implemente políticas de contraseñas que requieran contraseñas únicas de al menos 15 caracteres** [CPG 2.B] [CPG 2.C].
    - Los administradores de contraseñas pueden ayudarlo a desarrollar y administrar contraseñas seguras. Asegure y limite el acceso a cualquier administrador de contraseñas que se están utilizando y habilite todas las características de seguridad disponibles en el producto en uso, como la MFA.
- **Aplique políticas de bloqueo de cuentas después de una cierta cantidad de intentos fallidos de inicio de sesión**. Registre y supervise los intentos de inicio de sesión para detectar el descifre de contraseñas por fuerza bruta y la pulverización de contraseñas [CPG 2.G].
- **Almacene las contraseñas en una base de datos segura y utilice algoritmos de hash sólidos**.
- **Deshabilite la opción para guardar contraseñas en el navegador en la consola de administración de directivas de grupo**.
- **Implemente la solución de contraseña de administrador local (LAPS, por sus siglas en inglés)** siempre que sea posible si su sistema operativo es anterior a Windows Server 2019 y Windows 10, ya que estas versiones no tienen la LAPS integrada. **Nota:** Las organizaciones autoras recomiendan que las organizaciones actualicen el sistema a Windows Server 2019 y Windows 10 o una versión superior.
- Implemente protecciones contra el vuelco del Servicio de Subsistema de Autoridad de Seguridad Local (LSASS, por sus siglas en inglés):
    - **Implemente la regla de reducción de la superficie de ataque (ASR, por sus siglas en inglés) para el LSASS.**
    - **Implemente Credential Guard para Windows 10 y Server 2016**. Consulte la página de Microsoft Administrar Credential Guard de Windows Defender para obtener más información. En el caso de Windows Server 2012R2, habilite la verificación ligera de proceso protegido (PPL, por sus siglas en inglés) para la autoridad de seguridad local (LSA, por sus siglas en inglés).
- **Eduque a todos los empleados sobre la seguridad adecuada de las contraseñas en su capacitación anual sobre seguridad** y haga hincapié en no reutilizar las contraseñas ni guardarlas en archivos locales.
- **Cuando sea posible, utilice Windows PowerShell Remoting, Remote Credential Guard o RDP** con el modo de administrador restringido al establecer una conexión remota para evitar la exposición directa de las credenciales.
- **Separe las cuentas de administrador de las cuentas de usuario** [CPG 2.E]. Solo permita que las cuentas de administrador designadas se utilicen con fines administrativos. Si un usuario individual necesita derechos administrativos sobre su estación de trabajo, utilice una cuenta separada que no tenga acceso administrativo a otros hosts, como servidores. Para algunos entornos en la nube, separe las funciones cuando la cuenta utilizada para aprovisionar/administrar claves no tenga permiso para utilizar las claves y viceversa. Como esta estrategia introduce una sobrecarga de administración adicional, no es apropiada en todos los entornos.

### *Vector de acceso inicial: suplantación de identidad*

- **Implemente un programa de concienciación y capacitación sobre ciberseguridad para los usuarios** que incluya orientación sobre cómo identificar e informar actividades sospechosas (p. ej., suplantación de identidad) o incidentes [CPG 2.I].
- **Marque los correos electrónicos externos en los clientes de correo electrónico**.

La CISA ofrece una evaluación de campañas de suplantación de identidad sin costo, así como otras evaluaciones gratuitas. Visite cisa.gov/cyber-resource-hub.

- **Implemente filtros en la puerta de enlace de correos electrónicos para filtrar los correos electrónicos** con indicadores maliciosos conocidos, como las líneas de asunto maliciosas conocidas, y bloquear las direcciones de protocolo de Internet (IP) sospechosas en el cortafuegos [CPG 2.M].
- **Habilite los filtros de archivos adjuntos comunes para restringir los tipos de archivos que suelen contener malware** y que no deben enviarse por correo electrónico. Para obtener más información, consulte la publicación de Microsoft Protección antimalware en Exchange Online Protection (EOP).
    - Revise los tipos de archivos de su lista de filtros al menos cada semestre y añada otros tipos de archivos que se hayan convertido en vectores de ataque. Por ejemplo, los archivos adjuntos de OneNote con malware incrustado se han utilizado recientemente en campañas de suplantación de identidad.
    - El malware suele comprimirse en archivos protegidos con contraseña que eluden el análisis antivirus y los filtros de correos electrónicos.
- **Implemente la política y verificación de autenticación basada en dominios para mensajes, informes y conformidad (DMARC, por sus siglas en inglés)** a fin de reducir la posibilidad de que se falsifiquen o modifiquen correos electrónicos de dominios válidos. La DMARC protege su dominio de la falsificación, pero no brinda protección contra los correos electrónicos entrantes que se han falsificado, a menos que el dominio remitente también implemente una DMARC. La DMARC se basa en los protocolos ampliamente implementados del marco de directivas de remitente (SPF, por sus siglas en inglés) y de correo identificado con claves de dominio (DKIM, por sus siglas en inglés), y añade una función de informe que permite a remitentes y receptores mejorar y supervisar la protección del dominio contra el correo electrónico fraudulento. Para obtener más información sobre la DMARC, consulte Mejorar la seguridad de la web y de correos electrónicos de CISA Insights y el blog Cómo la DMARC potencia la seguridad de correos electrónicos del Center for Internet Security.

    Bloqueo e informes de dominios maliciosos (MDBR, por sus siglas en inglés) es un servicio sin costo para organizaciones SLTT que financian la CISA, el MS-ISAC y el EI-ISAC. Este servicio de seguridad totalmente administrado impide que los sistemas informáticos se conecten a dominios web dañinos y brinda protección contra las amenazas cibernéticas, entre las que se incluyen las siguientes:

    - malware;
    - ransomware;
    - suplantación de identidad.

    Para registrarse y recibir el servicio MDBR, visite cisecurity.org/ms-isac/services/mdbr/.
- **Asegúrese de que los scripts de macros estén deshabilitados para los archivos de Microsoft Office transmitidos por correo electrónico**. Estas macros se pueden utilizar para distribuir ransomware [CPG 2.N]. **Nota:** Las versiones recientes de Office están configuradas por defecto para bloquear archivos que contengan macros de Visual Basic para Aplicaciones (VBA, por sus siglas en inglés) y mostrar una barra de confianza con una advertencia de que las macros están presentes y se han deshabilitado. Para obtener más información, consulte la página de Microsoft Las macros de Internet se bloquearán por defecto en Office. Consulte la página de Microsoft Bloquear la ejecución de macros en archivos de Office desde Internet a fin de obtener instrucciones de configuración para deshabilitar las macros en archivos externos, en el caso de versiones anteriores de Office.
- **Deshabilite Windows Script Host (WSH)**. El alojamiento de scripts de Windows proporciona un entorno en el que los usuarios pueden ejecutar scripts o realizar tareas.

### *Vector de acceso inicial: infección de malware precursor*

- **Utilice actualizaciones automáticas para el software y las firmas antivirus y antimalware**. Asegúrese de que las herramientas estén correctamente configuradas para proporcionar advertencias e indicadores a fin de notificar al personal de seguridad. Las organizaciones autoras recomiendan utilizar una solución antivirus administrada centralmente. Esto permite la detección de malware y ransomware "precursor".

> La CISA y el MS-ISAC recomiendan a las organizaciones SLTT utilizar el sistema de detección de intrusiones (IDS, por sus siglas en inglés) Albert para mejorar la estrategia de defensa en profundidad. Albert funciona como una capacidad de advertencia temprana para los Gobiernos SLTT de EE. UU. y apoya la conciencia situacional y la defensa de la ciberseguridad a nivel nacional. Para obtener más información sobre Albert, visite cisecurity.org/services/albert-network-monitoring/.

    - Una infección de ransomware puede ser la prueba de un riesgo de la red previo y no resuelto. Por ejemplo, muchas infecciones de ransomware son el resultado de infecciones de malware existentes, como QakBot, Bumblebee y Emotet.
    - En algunos casos, la implementación de ransomware es el último paso del riesgo de la red, y se instala para ocultar las anteriores actividades posteriores a la puesta en riesgo, como la puesta en riesgo del correo electrónico empresarial (BEC, por sus siglas en inglés).

- **Utilice listas de aplicaciones permitidas o soluciones de detección y respuesta de puntos de conexión (EDR, por sus siglas en inglés)** en todos los activos para garantizar que solo el software autorizado sea ejecutable y se bloquee todo el software no autorizado.
    - En el caso de Windows, habilite "Control de aplicaciones" de Windows Defender (WDAC, por sus siglas en inglés), AppLocker o ambas opciones en todos los sistemas que admitan estas características.
        - El WDAC está en desarrollo continuo, mientras que AppLocker solo recibirá correcciones de seguridad. AppLocker se puede utilizar como complemento del WDAC, si el WDAC está configurado en el nivel más restrictivo posible, y AppLocker se utiliza para ajustar las restricciones de su organización.
    - Utilice las listas de permitidos en lugar de intentar enumerar y denegar todas las permutaciones posibles de las aplicaciones en un entorno de red.
    - Considere implementar soluciones de EDR para los recursos basados en la nube.
- **Considere implementar un sistema de detección de intrusiones (IDS)** para detectar la actividad de mando y control, así como otra actividad de red potencialmente maliciosa, que se produce antes de la implementación del ransomware.
    - Asegúrese de que el IDS se administre y supervise de forma centralizada. Configure correctamente las herramientas y dirija las advertencias y los indicadores al personal adecuado para que tome medidas al respecto.
- **Supervise los indicadores de actividad y bloquee la creación de archivos de malware con la utilidad Sysmon de Windows**. A partir de Sysmon 14, la opción `FileBlockExecutable` se puede utilizar para bloquear la creación de ejecutables maliciosos, archivos de biblioteca de enlaces dinámicos (DLL, por sus siglas en inglés) y archivos del sistema que coincidan con valores de hash específicos.

### *Vector de acceso inicial: formas avanzadas de ingeniería social*

- **Cree políticas para incluir la capacitación de concientización de ciberseguridad** sobre las formas avanzadas de ingeniería social para el personal que tenga acceso a su red. La capacitación debe incluir consejos sobre cómo reconocer páginas web y resultados de búsqueda ilegítimos. También es importante que repita periódicamente la capacitación de concientización de seguridad para mantener a su personal informado y alerta.
- **Implemente un sistema de nombres de dominio (DNS, por sus siglas en inglés) de protección.** Mediante el bloqueo de la actividad maliciosa de Internet en la fuente, los servicios de DNS de protección pueden brindar una alta seguridad de red para los trabajadores remotos. Estos servicios de seguridad analizan las consultas de DNS y toman medidas para mitigar las amenazas (como malware, ransomware, ataques de suplantación de identidad, virus, sitios maliciosos y spyware), y para ello aprovechan la arquitectura y el protocolo de DNS existentes. Las entidades SLTT pueden implementar el servicio MDBR sin costo. Consulte el documento de la NSA y la CISA Selección de un servicio de DNS de protección.
- **Considere implementar navegadores de espacio aislado** para proteger los sistemas del malware que se origina en la navegación web. Los navegadores de espacio aislado aíslan el equipo host del código malicioso.

Entre las formas avanzadas de ingeniería social, se incluyen las siguientes:

- Envenenamiento de optimización de motores de búsqueda (SEO, por sus siglas en inglés), también conocido como envenenamiento de búsqueda: cuando agentes maliciosos crean páginas web maliciosas y utilizan tácticas de SEO para que aparezcan de manera destacada en los resultados de búsqueda. El envenenamiento de SEO secuestra los resultados de los motores de búsqueda de páginas web populares e inyecta enlaces maliciosos para mejorar su ubicación en los resultados de búsqueda. Luego, estos enlaces llevan a los usuarios desprevenidos a sitios de suplantación de identidad, descargas de malware y otras amenazas cibernéticas.
- Descargas malintencionadas (páginas web impostoras): cuando un usuario descarga involuntariamente código malicioso visitando una página web aparentemente legítima que es maliciosa. Los agentes maliciosos utilizan las descargas malintencionadas para robar y recopilar información personal, inyectar troyanos o introducir conjuntos de vulnerabilidades u otro malware en los puntos de conexión. Los usuarios pueden visitar estos sitios respondiendo a un correo electrónico de suplantación de identidad o haciendo clic en una ventana emergente engañosa.
- “Publicidad malintencionada”: publicidad maliciosa que utilizan los ciberdelincuentes para inyectar malware en las computadoras de los usuarios cuando visitan páginas web maliciosas o hacen clic en un anuncio en línea. La publicidad malintencionada también puede dirigir a los usuarios a una página web dañada donde pueden robar sus datos o se puede descargar malware en su computadora. La publicidad malintencionada puede aparecer en cualquier lugar, incluso en los sitios que visita como parte de su navegación web diaria.
- Hacerse pasar por empleados: los agentes de ransomware se han hecho pasar por personal informático de la empresa o personal del servicio de asistencia en llamadas telefónicas o mensajes SMS para obtener las credenciales de los empleados y conseguir acceso a la red.

### *Vector de acceso inicial: terceros y proveedores de servicios administrados*

- **Considere las prácticas de higiene cibernética y administración de riesgos de terceros o proveedores de servicios administrados (MSP, por sus siglas en inglés)** en los que confía su organización para cumplir su misión. Los MSP han sido un vector de infección de ransomware que ha afectado a numerosas organizaciones de clientes [CPG 1.I].
    - Si un tercero o MSP es responsable de mantener y asegurar las copias de seguridad de su organización, asegúrese de que siga las prácticas recomendadas aplicables que se describen más arriba. Utilice el lenguaje contractual para formalizar sus requisitos de seguridad como práctica recomendada.

Los agentes maliciosos pueden explotar las relaciones de confianza que su organización tiene con terceros y MSP.

- Los agentes maliciosos pueden atacar a los MSP con la meta de poner en riesgo a las organizaciones de clientes de los MSP; pueden utilizar las conexiones de red de los MSP y acceder a las organizaciones de clientes como vector clave para propagar malware y ransomware.
- Los agentes maliciosos pueden falsificar la identidad de entidades con las que su organización tiene una relación de confianza, así como utilizar las cuentas de correo electrónico puestas en riesgo que están asociadas con dichas entidades, para realizar la suplantación de identidad contra sus usuarios, lo que permite el riesgo de la red y la divulgación de información.

- **Garantice el uso del mínimo privilegio y la separación de funciones a la hora de configurar el acceso de terceros**. Los terceros y los MSP solo deben tener acceso a los dispositivos y servidores que estén dentro de sus funciones o responsabilidades.
- **Considere crear políticas de control de servicios (SCP, por sus siglas en inglés) para recursos basados en la nube a fin de evitar que los usuarios o las funciones, en toda la organización, puedan acceder a servicios específicos o realizar acciones específicas dentro de los servicios.** Por ejemplo, la SCP se puede utilizar para impedir que los usuarios eliminen registros, actualicen las configuraciones de la nube privada virtual (VPC, por sus siglas en inglés) y cambien las configuraciones de registro.

## Prácticas recomendadas generales y orientación para el refuerzo

- **Asegúrese de que su organización tenga un enfoque integral de administración de activos** [CPG 1.A].
    - Comprenda los activos informáticos de su organización, tanto lógicos (p. ej., datos, software) como físicos (p. ej., hardware), y haga un inventario.
    - Sepa qué datos o sistemas son más fundamentales para la salud y la seguridad, la generación de ingresos u otros servicios fundamentales, y comprenda cualquier interdependencia asociada (p. ej., "la lista del sistema 'A' que se utiliza para realizar 'X' está almacenada en el activo fundamental 'B'"). Esto ayudará a su organización a determinar las prioridades de restauración en caso de que ocurra un incidente. Aplique controles de seguridad o protecciones más integrales a los activos fundamentales. Esto requiere coordinación en toda la organización.
    - Asegúrese de almacenar la documentación del activo informático de forma segura y mantenga copias de seguridad sin conexión y copias físicas en el sitio.

**Consejo:** Para facilitar el monitoreo de activos, utilice el recurso del MS-ISAC Hoja de cálculo para el monitoreo de activos de hardware y software.

- **Aplique el principio de privilegio mínimo a todos los sistemas y servicios** para que los usuarios solo tengan el acceso que necesitan para realizar su trabajo [CPG 2.E]. Los agentes maliciosos suelen aprovechar las cuentas privilegiadas para realizar ataques de ransomware en toda la red.
    - Restrinja los permisos de los usuarios para instalar y ejecutar aplicaciones de software.
    - Restrinja los permisos de usuario o función para acceder a los recursos basados en la nube o modificarlos.
    - Limite las acciones que ciertos usuarios o funciones pueden realizar en las claves administradas por el cliente.
    - Bloquee el acceso remoto a las cuentas locales a través de la directiva de grupo para restringir el inicio de sesión en la red por parte de las cuentas locales. Para obtener orientación, consulte las páginas de Microsoft Bloqueo del uso remoto de las cuentas locales e Identificadores de seguridad.
    - Utilice Remote Credential Guard de Windows Defender y el modo de administrador restringido para las sesiones de RDP.
    - Quite las cuentas y los grupos innecesarios, y restrinja el acceso raíz.
    - Controle y limite la administración local.
    - Realice auditorías de Active Directory (AD, por sus siglas en inglés) para detectar los excesos de privilegios en cuentas y afiliaciones a grupos.
    - Utilice el grupo de usuarios protegidos de AD en los dominios de Windows a fin de asegurar aún más las cuentas de usuarios privilegiados contra los ataques de paso de hash.
    - Realice auditorías trimestrales de las cuentas de usuario y administrador para detectar cuentas inactivas o no autorizadas. Priorice la revisión de las cuentas de supervisión y administración remota que sean de acceso público; esto incluye las auditorías del acceso externo otorgado a MSP.

- **Asegúrese de que se actualicen y refuercen todos los hipervisores y la infraestructura informática asociada, como los componentes de red y almacenamiento**. Las estrategias de ransomware emergentes han comenzado a atacar a los servidores de VMware ESXi, a los hipervisores y a otras herramientas y sistemas centralizados, lo que permite el cifrado rápido de la infraestructura a escala. Para obtener más información sobre la resistencia al ransomware y el refuerzo de VMware y otra infraestructura de virtualización, consulte los siguientes recursos:
    - Publicación especial del NIST (SP 800-125A, revisión 1): Recomendaciones de seguridad para plataformas de hipervisor basadas en el servidor
    - VMware: Refuerzo y configuración de seguridad de la infraestructura de la nube

- **Aproveche las prácticas recomendadas y habilite la configuración de seguridad en asociación con los entornos en la nube**, como Microsoft Office 365.
    - Revise el modelo de responsabilidad compartida para la nube y asegúrese de comprender en qué consiste la responsabilidad del cliente cuando se trata de protección de activos.
    - Haga una copia de seguridad de los datos con frecuencia; puede hacerla sin conexión o puede aprovechar las copias de seguridad de nube a nube.
    - Habilite el registro de todos los recursos y establezca alertas para usos anormales.
    - Habilite la protección contra eliminaciones o el bloqueo de objetos en los recursos de almacenamiento que suelen ser objetivo de ataques de ransomware (p. ej., almacenamiento de objetos, de bases de datos, de archivos y de bloques) a fin de evitar que los datos se eliminen o se sobrescriban, respectivamente.
    - Considere habilitar el control de versiones para mantener múltiples variantes de objetos almacenados. Esto permite una recuperación más sencilla de acciones involuntarias o maliciosas.

  - Si es compatible, al utilizar el acceso programático personalizado a la nube, utilice solicitudes de interfaz de programación de aplicaciones (API) firmadas para verificar la identidad del solicitante, proteger los datos en tránsito y brindar protección contra otros ataques, como los ataques de reproducción.
  - Para obtener más información, consulte el aviso sobre ciberseguridad de la CISA Recomendaciones de seguridad de Microsoft Office 365.

- **Mitigue el uso malicioso del software de acceso remoto y el de supervisión y administración remota (RMM, por sus siglas en inglés)**:
  - Realice una auditoría de las herramientas de acceso remoto en su red para identificar el software de RMM actual o autorizado.
  - Revise los registros de ejecución del software de RMM para detectar un uso anormal o software de RMM ejecutándose como ejecutable portátil.
  - Utilice un software de seguridad para detectar instancias de software de RMM que solo se cargan en la memoria.
  - Exija que las soluciones de RMM autorizadas solo se utilicen desde su red a través de soluciones de acceso remoto aprobadas, como VPN o interfaces de escritorio virtual (VDI, por sus siglas en inglés).
  - Bloquee las conexiones entrantes y salientes en puertos y protocolos de RMM comunes en el perímetro de la red.

- **Emplee medios lógicos o físicos de segmentación de la red implementando** la ZTA y separando varias unidades de negocios o recursos informáticos departamentales dentro de su organización. Además, mantenga la separación entre la tecnología de la información y la tecnología operativa [CPG 2.F]. La segmentación de la red puede ayudar a contener el impacto de cualquier intrusión que afecte a su organización y a prevenir o limitar el movimiento lateral por parte de agentes maliciosos. Las organizaciones deben utilizar la diligencia debida al segmentar redes y asegurarse de que las políticas de seguridad de la red estén implementadas y se cumplan, ya que la segmentación puede volverse inefectiva si se infringe por error del usuario o por el incumplimiento de las políticas (p. ej., conectar medios de almacenamiento extraíbles u otros dispositivos a múltiples segmentos).

- **Desarrolle y actualice periódicamente diagramas de red completos que describan los sistemas y los flujos de datos dentro de las redes de su organización** (consulte la Figura 1) [CPG 2.P]. Esto es útil en un estado constante y puede ayudar al personal de respuesta a incidentes a comprender en qué área debe centrar sus esfuerzos. Consulte la Figura 2 y la Figura 3 para ver representaciones de una red plana (no segmentada) y de una red segmentada según las prácticas recomendadas.
  - El diagrama debe incluir representaciones de las redes principales, cualquier esquema de direccionamiento IP específico y la topología general de la red, como las conexiones de red, las interdependencias y el acceso concedido a terceros, los MSP y las conexiones a la nube desde puntos de conexión externos e internos.
  - Asegúrese de almacenar de forma segura la documentación de la red y mantenga copias de seguridad sin conexión y copias impresas en el sitio.

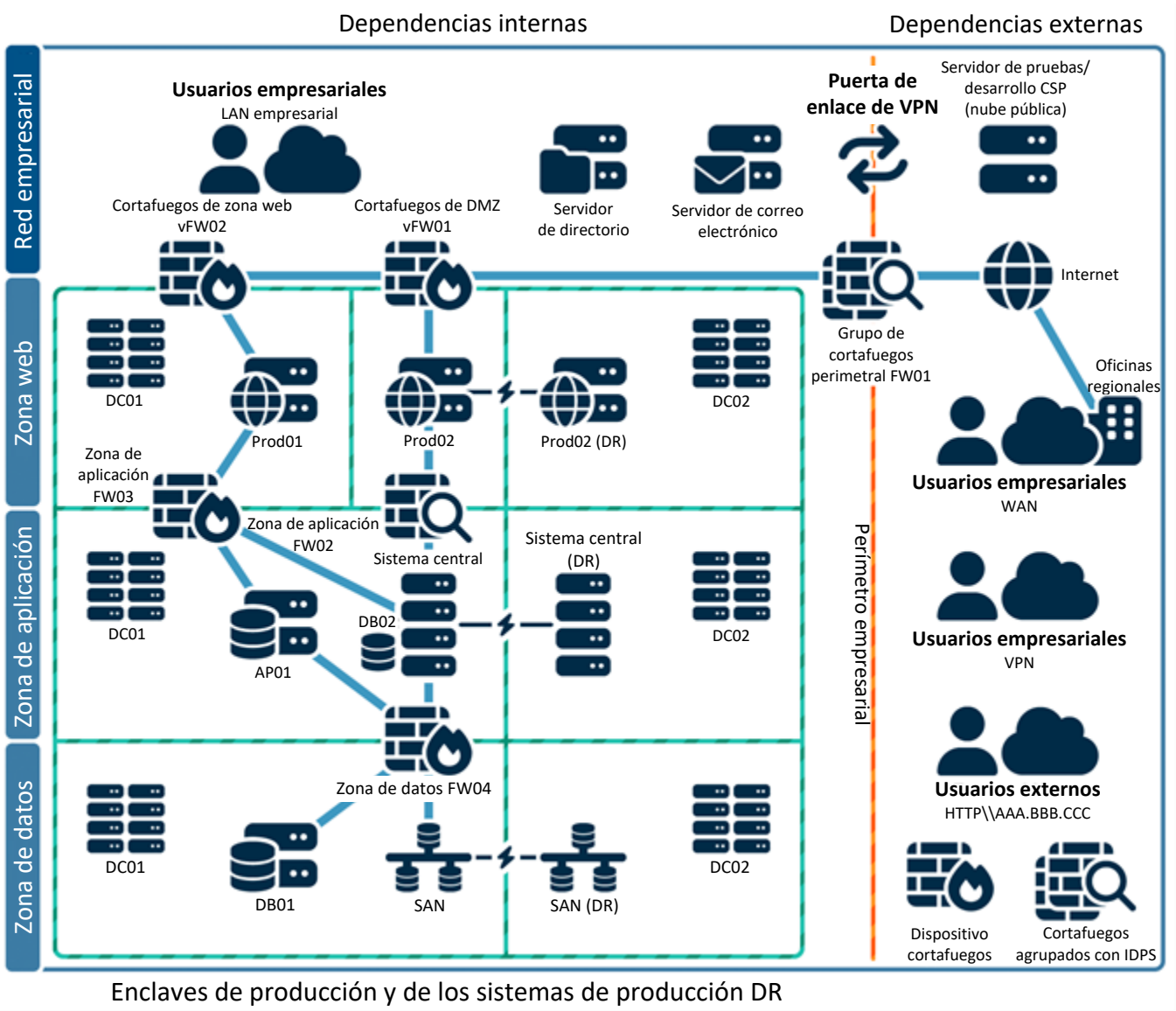


*Figura 1: Ejemplo de diagrama de red*

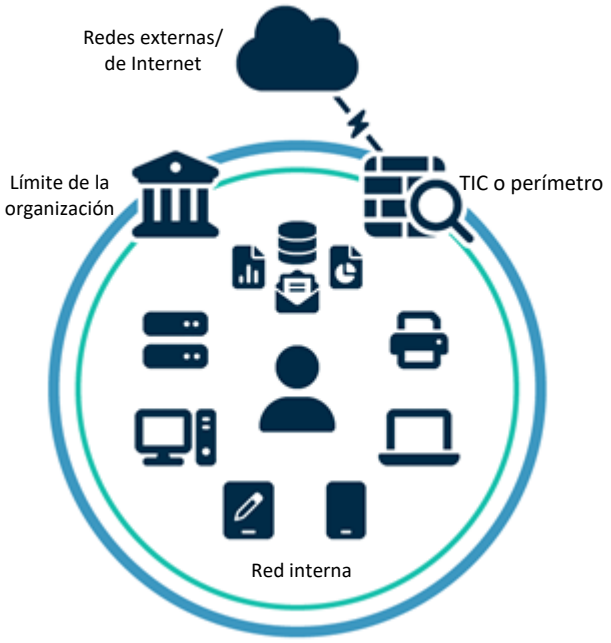


*Figura 2:* Red plana (no segmentada)

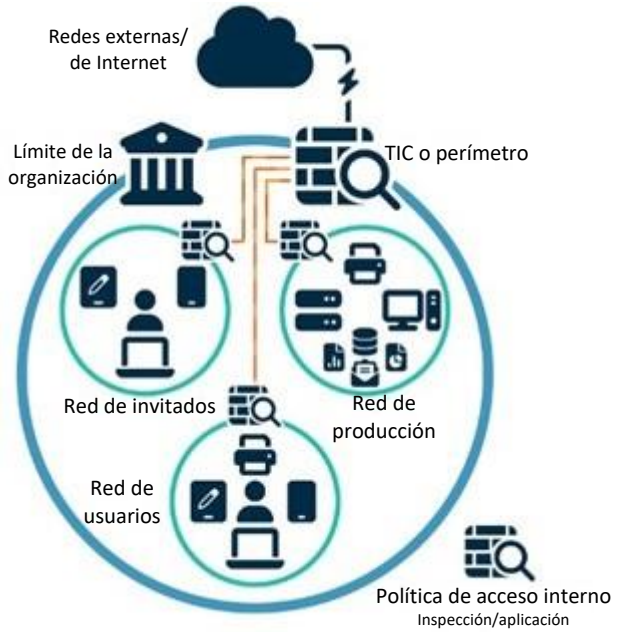


*Figura 3:* Red *segmentada*

- **Restrinja el uso de PowerShell a usuarios específicos, determinados caso por caso, mediante la directiva de grupo**. Por lo general, solo los usuarios o administradores que administran una red o un sistema operativo Windows pueden utilizar PowerShell. PowerShell es un lenguaje multiplataforma, de línea de comandos, de shell y de scripting que forma parte de Microsoft Windows. Los agentes de amenazas utilizan PowerShell para implementar ransomware y ocultar sus actividades maliciosas. Para obtener más información, consulte la hoja de información conjunta de ciberseguridad Cómo mantener PowerShell: medidas de seguridad para implementar y adoptar.
    - Actualice Windows PowerShell o PowerShell Core a la última versión y desinstale todas las versiones anteriores de PowerShell.
    - Asegúrese de que las instancias de PowerShell que utilizan la versión más reciente tengan habilitado el módulo, el bloque de scripts y el registro de transcripción (registro mejorado).
        - Los registros de Windows PowerShell anteriores a la versión 5.0 son inexistentes o no registran suficientes detalles para ayudar en las actividades empresariales de supervisión y respuesta a incidentes.
        - Los registros de PowerShell contienen datos valiosos, entre los que se incluyen la interacción histórica con el sistema operativo y el registro, así como las tácticas, las técnicas y los procedimientos posibles del uso de PowerShell por parte de un agente de amenazas.
        - Dos registros que reflejan la actividad de PowerShell son el registro “Evento de Windows PowerShell” y el registro “Operaciones de PowerShell”. Las organizaciones autoras recomiendan activar estos dos registros de eventos de Windows con un período de retención de al menos 180 días.
        - Estos registros deben revisarse periódicamente para confirmar si los datos del registro se eliminaron o si se desactivó el registro. Configure el tamaño de almacenamiento permitido para ambos registros de manera que tengan el mayor tamaño posible.

- **Asegure los controladores de dominio (DC, por sus siglas en inglés)**. Los agentes maliciosos suelen atacar y utilizar los DC como punto de partida para propagar el ransomware en toda la red. Para asegurar los DC, haga lo siguiente:
    - Utilice la última versión de Windows Server compatible con su organización en los DC. Las versiones más recientes del sistema operativo Windows Server tienen más características de seguridad integradas, incluso para Active Directory. Para obtener orientación sobre cómo configurar las características de seguridad disponibles, consulte la página de Microsoft Prácticas recomendadas para asegurar Active Directory.
        - Las organizaciones autoras recomiendan utilizar Windows Server 2019 o una versión superior, o bien Windows 10 o una versión superior, ya que tienen características de seguridad, como protecciones del LSASS con Windows Credential Guard, Windows Defender y Antimalware Scan Interface (AMSI), que no se incluyen en sistemas operativos anteriores.
    - Asegúrese de que los DC se corrijan periódicamente. Aplique correcciones para las vulnerabilidades fundamentales lo antes posible.
    - Utilice herramientas de prueba de penetración de código abierto, como BloodHound o PingCastle, para verificar la seguridad del controlador de dominio.
    - Asegúrese de que se instale el software o los agentes mínimos en los DC, ya que estos se pueden aprovechar para ejecutar código arbitrario en el sistema.
    - Restrinja el acceso a los DC al grupo de administradores. Los usuarios dentro de este grupo deben ser limitados y tener cuentas separadas utilizadas para las operaciones diarias con permisos no administrativos. Para obtener más información, consulte la página de Microsoft Cómo asegurar las cuentas y los grupos administrativos de Active Directory.
        - Las cuentas de administrador designadas solo deben utilizarse con fines administrativos. Asegúrese de que en los DC no se revisen correos electrónicos, no se navegue por Internet ni se realicen otras actividades de alto riesgo.
    - Configure los cortafuegos del host del DC para impedir el acceso a Internet. Normalmente, los DC no necesitan acceso directo a Internet. Se pueden utilizar servidores con conectividad a Internet para obtener las actualizaciones necesarias en lugar de permitir el acceso a Internet a los DC.
    - Implemente una solución de administración de acceso privilegiado (PAM, por sus siglas en inglés) en los DC para ayudar a administrar y supervisar el acceso privilegiado. Las soluciones de PAM también pueden registrar el uso y emitir alertas sobre este para detectar actividad inusual.
    - Considere deshabilitar o limitar la autenticación NTLM y WDigest si es posible. Incluya su uso como criterio para priorizar la actualización de sistemas heredados o para segmentar la red. En su lugar, utilice protocolos de federación modernos (p. ej., lenguaje de marcado de aserción de seguridad [SAML, por sus siglas en inglés], OpenID Connect [OIDC] o Kerberos) para la autenticación con cifrado del AES de 256 bits https://cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf. Si es necesario habilitar la autenticación NTLM, haga lo siguiente:
        - Habilite la protección ampliada para la autenticación (EPA, por sus siglas en inglés) a fin de evitar algunos ataques de retransmisión de NTLM. Para obtener más información, consulte la página de Microsoft Cómo mitigar los ataques de retransmisión de NTLM en los Servicios de certificados de Active Directory (AD CS, por sus siglas en inglés).
        - Habilite la auditoría de NTLM para asegurarse de que solo se envíen respuestas de NTLMv2 a través de la red. Se deben tomar medidas para garantizar que se rechacen las respuestas de NTLM y LM si es posible.

  - Habilite protecciones adicionales para la autenticación de LSA a fin de evitar la inyección de código capaz de adquirir credenciales del sistema. Antes de habilitar estas protecciones, realice auditorías de `lsass.exe` para garantizar que comprenda los programas que se verán afectados por la habilitación de esta protección.

- **Conserve y asegure adecuadamente los registros de los dispositivos de red, los hosts locales y los servicios en la nube**. Esto apoya la clasificación y la corrección de los eventos de ciberseguridad. Los registros se pueden analizar para determinar el impacto de los eventos y establecer si se ha producido un incidente [CPG 2.T].
  - Configure la administración de registros centralizada utilizando una herramienta de administración de eventos e información de seguridad [CPG 2.U]. Esto permite a una organización relacionar los registros de los dispositivos de seguridad de la red y del host. Mediante la revisión de registros de varias fuentes, una organización puede clasificar un evento individual y determinar su impacto en la organización.
  - Mantenga los registros de los sistemas fundamentales durante un mínimo de un año y haga copias de seguridad de estos si es posible.

- **Establezca una referencia de seguridad del tráfico normal de la red y ajuste los dispositivos de red para detectar comportamientos anómalos**. Ajuste los productos basados en el host para detectar binarios anómalos, movimientos laterales y técnicas de persistencia.
  - Considere utilizar el registro de transacciones comerciales, como el registro de actividades relacionadas con aplicaciones específicas o fundamentales, para llevar a cabo análisis del comportamiento.

- **Realice evaluaciones periódicas** con el fin de garantizar que los procesos y los procedimientos estén actualizados y puedan seguirlos el personal de seguridad y los usuarios finales.
- **Habilite la prevención del seguimiento** para limitar los vectores que las redes publicitarias y los rastreadores pueden utilizar para monitorear la información del usuario.
- **Habilite la protección contra errores de tecleo en páginas web** para limitar la posibilidad de iniciar sesión en páginas web falsificadas u otros posibles enlaces maliciosos que podrían poner en riesgo un navegador.
- **Habilite un antivirus (AV) basado en el navegador** para llevar a cabo un análisis activo mientras navega como una capa adicional de defensa.
- **Bloquee las notificaciones de la página web por defecto** para limitar la capacidad del sitio de monitorear datos del usuario que puedan explotarse.

# Parte 2: Lista de cotejo para respuestas a ransomware y extorsión de datos

Si su organización es víctima de ransomware, siga su IRP aprobado. Las organizaciones autoras recomiendan encarecidamente responder utilizando la siguiente lista de cotejo. Asegúrese de seguir los **primeros tres pasos en secuencia.**

**Las organizaciones autoras no recomiendan pagar rescate**. Pagar un rescate no garantizará que sus datos se descifren, que sus sistemas o datos ya no estén en riesgo ni que sus datos no se filtren.

Además, el pago de rescates puede plantear riesgos de sanciones. Para obtener información sobre los posibles riesgos de sanciones, consulte el memorando de septiembre de 2021 de la Oficina de Control de Activos Extranjeros (OFAC, por sus siglas en inglés) del Departamento del Tesoro de EE. UU. (U.S. Department of the Treasury), Aviso actualizado sobre posibles riesgos de sanciones por facilitar pagos de ransomware. El aviso actualizado establece que la Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro consideraría "factores atenuantes" en las acciones de aplicación relacionadas. Comuníquese con su oficina local de la FBI, en consulta con la OFAC, para obtener orientación sobre los factores de sanción atenuantes después de un ataque.

## Detección y análisis

Consulte las prácticas recomendadas y las referencias que se indican a continuación para ayudar a administrar el riesgo que plantea el ransomware y apoyar la respuesta coordinada y eficiente de su organización a un incidente de ransomware. Aplique estas prácticas en la mayor medida posible, según la disponibilidad de recursos organizacionales.

- ☐ **1. Determine qué sistemas se vieron afectados y aíslelos de inmediato.**
  - ☐ Si varios sistemas o subredes parecen afectados, desconecte la red en el nivel del conmutador. Puede que no sea factible desconectar sistemas individuales durante un incidente.
  - ☐ Priorice el aislamiento de sistemas fundamentales que son esenciales para las operaciones diarias.
  - ☐ Si no es posible desconectar la red temporalmente de forma inmediata, localice el cable de red (p. ej., ethernet) y desconecte los dispositivos afectados de la red o quítelos del wifi para contener la infección.
  - ☐ En el caso de los recursos en la nube, tome una instantánea de los volúmenes para obtener una copia de un momento determinado que pueda revisarse posteriormente para una investigación forense.
  - ☐ Después de un riesgo inicial, los agentes maliciosos pueden supervisar la actividad o las comunicaciones de su organización para comprender si se han detectado sus acciones. Aísle los sistemas de manera coordinada y utilice métodos de comunicación fuera de banda, como llamadas telefónicas, para evitar informar a los agentes que se los ha descubierto y que se están tomando medidas de mitigación. Al no hacerlo, podría provocar que los agentes se muevan de forma lateral para preservar su acceso o que implementen ransomware ampliamente antes de que se desconecten las redes.

- ☐ **2. Apague los dispositivos si no puede desconectarlos de la red para evitar una mayor propagación de la infección de ransomware.**

  **Nota:** Este paso evitará que su organización mantenga artefactos de infección de ransomware y posibles pruebas almacenadas en la memoria volátil. **Debe llevarse a cabo únicamente si no es posible apagar temporalmente la red o desconectar los hosts afectados de la red** utilizando otros medios.

☐ **3. Clasifique los sistemas afectados para la restauración y recuperación.**
- ☐ Identifique y priorice sistemas fundamentales para su restauración en una red limpia y confirme la naturaleza de los datos alojados en los sistemas afectados.
  - Priorice la restauración y recuperación basándose en una lista predefinida de activos fundamentales que incluya los sistemas de información fundamentales para la salud y la seguridad, la generación de ingresos u otros servicios fundamentales, así como los sistemas de los que dependen.
- ☐ Mantenga un registro de los sistemas y dispositivos que no se perciben como afectados a fin de que se les pueda quitar prioridad para la restauración y recuperación. Esto permite que su organización vuelva a funcionar de una manera más eficiente.

☐ **4. Examine los registros y los sistemas existentes de detección o prevención de la organización (p. ej., antivirus, EDR, IDS, sistema de prevención de intrusiones).** Esto puede poner de manifiesto la existencia de otros sistemas o malware involucrados en las primeras fases del ataque.
- ☐ Busque pruebas de “instaladores de malware” precursores, como Bumblebee, Dridex, Emotet, QakBot o Anchor. Un evento de ransomware puede ser la prueba de un riesgo de la red previo y no resuelto.
  - Los operadores de estas variantes avanzadas de malware suelen vender el acceso a una red. En ocasiones, los agentes maliciosos utilizan este acceso para exfiltrar datos y, luego, amenazan con publicarlos antes de pedir un rescate a la red para extorsionar aún más a la víctima y presionarla a que pague.
  - Los agentes maliciosos suelen implementar variantes de ransomware para ocultar la actividad posterior al riesgo. Se debe tener cuidado para identificar al instalador de malware antes de realizar la reconstrucción a partir de copias de seguridad para evitar que los riesgos continúen.

☐ **5. Consulte con su equipo para desarrollar y documentar una comprensión inicial de lo que ocurrió basándose en el análisis inicial.**

☐ **6. Inicie actividades de búsqueda de amenazas.**
- ☐ En el caso de entornos empresariales, verifique lo siguiente:
  - Cuentas de AD recién creadas o cuentas con privilegios elevados y actividad reciente relacionada con cuentas privilegiadas, como administradores de dominio.
  - Inicios de sesión anómalos en dispositivos de VPN u otros inicios de sesión sospechosos.
  - Modificaciones de puntos de conexión que puedan deteriorar las copias de seguridad, las instantáneas, el registro en diario de los discos o las configuraciones de arranque. Busque un uso anómalo de las herramientas integradas de Windows, como `bcdedit.exe`, `fsutil.exe` (deletejournal), `vssadmin.exe`, `wbadmin.exe` y `wmic.exe` (shadowcopy o shadowstorage). El uso indebido de estas herramientas es una técnica de ransomware común para inhibir la recuperación del sistema.
  - Indicios de la presencia de la señal/cliente de Cobalt Strike. Cobalt Strike es un paquete de software comercial de pruebas de penetración. Los agentes maliciosos suelen nombrar los procesos de Windows de Cobalt Strike con los mismos nombres que los procesos de Windows legítimos para ofuscar su presencia y complicar las investigaciones.

- Señales de cualquier uso inesperado de software de supervisión y administración remota (RMM) (incluidos los ejecutables portátiles que no están instalados). Los agentes maliciosos suelen utilizar el software de RMM para mantener la persistencia.
- Cualquier ejecución inesperada de PowerShell o uso del conjunto PsTools.
- Signos de enumeración de credenciales de AD o LSASS que se vuelcan (p. ej., Mimikatz, `Sysinternals ProcDump` o `NTDSutil.exe`).
- Señales de comunicaciones inesperadas entre puntos de conexión (incluidos los servidores), por ejemplo, el envenenamiento del protocolo de resolución de direcciones (ARP, por sus siglas en inglés) de un punto de conexión o el tráfico de comando y control retransmitido entre puntos de conexión.
- Posibles señales de que se están exfiltrando datos de la red, que pueden incluir lo siguiente:
    - Cantidad anormal de datos salientes a través de cualquier puerto. El software de código abierto puede canalizar datos a través de varios puertos y protocolos. Por ejemplo, los agentes de ransomware han utilizado Chisel para canalizar el shell seguro (SSH, por sus siglas en inglés) a través del puerto `443` del protocolo de transferencia de hipertexto seguro (HTTPS, por sus siglas en inglés). Los agentes de ransomware también han utilizado Cloudflared para hacer mal uso de los túneles de Cloudflare a fin de canalizar las comunicaciones a través del HTTPS.
    - La presencia de Rclone, Rsync y diversos servicios de almacenamiento de archivos basados en la web, y del protocolo de transferencia de archivos (FTP, por sus siglas en inglés) y del protocolo de transferencia segura de archivos (SFTP, por sus siglas en inglés), que son herramientas comunes para la exfiltración de datos (y también las utilizan los agentes de amenazas para implantar malware o herramientas en las redes afectadas).
- Servicios recién creados, tareas programadas inesperadas, software instalado imprevisto, archivos inusuales creados, procesos legítimos con procesos secundarios inesperados, etc.

☐ En el caso de los entornos en la nube, haga lo siguiente:

- Habilite herramientas para detectar y evitar las modificaciones en recursos de IAM, seguridad de la red y protección de datos.
- Utilice la automatización para detectar problemas comunes (p. ej., deshabilitación de características, introducción de nuevas reglas del cortafuegos) y tomar medidas automatizadas apenas ocurran. Por ejemplo, si se crea una nueva regla del cortafuegos que permite el tráfico abierto (`0.0.0.0/0`), se puede tomar una medida automatizada para deshabilitar o eliminar esta regla y enviar notificaciones al usuario que la creó, así como al equipo de seguridad para que esté al tanto. Esto ayudará a evitar la fatiga de alertas y permitirá que el personal de seguridad se concentre en cuestiones fundamentales.

## Informes y notificaciones

**Nota:** Consulte la sección "Información de contacto" al final de esta guía para obtener detalles sobre cómo informar y notificar incidentes de ransomware.

- ☐ **7.** Siga los requisitos de notificación descritos en su plan de comunicaciones y respuesta a incidentes cibernéticos para **interactuar con los equipos internos y externos, y con las partes interesadas** e informarles qué pueden proporcionarle para ayudarlo a mitigar el incidente, responder a este y recuperarse de dicho incidente.
  - ☐ Comparta la información que tiene a su disposición para recibir asistencia oportuna y relevante. Mantenga a la administración y a los líderes sénior informados mediante actualizaciones periódicas a medida que se desarrolla la situación. Las partes interesadas relevantes pueden incluir su Departamento Informático, los proveedores de servicios de seguridad administrados, la compañía de seguros cibernéticos y los líderes departamentales o electos [CPG 4.A].
  - ☐ Informe el incidente y considere solicitar asistencia a la CISA, su oficina local de la FBI, el Centro de Denuncias de Delitos en Internet (IC3, por sus siglas en inglés) de la FBI o su oficina local del Servicio Secreto de EE. UU. (U.S. Secret Service).
  - ☐ Según corresponda, coordínese con el personal de comunicaciones y de información pública para garantizar que se comparta información precisa de manera interna con su organización y de manera externa con el público.

Si se necesita una identificación o un análisis extendidos, la CISA, el MS-ISAC y la Policía local, estatal o federal pueden estar interesados en cualquiera de la siguiente información que su organización determine que puede compartir legalmente:

- Archivo ejecutable recuperado.
- Copias del archivo Léame. NO QUITE el archivo, de lo contrario, puede ser imposible descifrarlo.
- Captura de memoria activa (memoria de acceso aleatorio [RAM, por sus siglas en inglés]) de los sistemas con señales adicionales de riesgo (uso de conjuntos de herramientas de vulnerabilidades, actividad de RDP, archivos adicionales encontrados localmente).
- Imágenes de sistemas infectados con señales adicionales de riesgo (uso de conjuntos de herramientas de vulnerabilidades, actividad de RDP, archivos adicionales encontrados localmente).
- Muestras de malware.
- Nombres de malware identificados en su red.
- Muestras de archivos cifrados.
- Archivos de registro (p. ej., registros de eventos de Windows de sistemas puestos en riesgo, registros del cortafuegos).
- Scripts de PowerShell encontrados que se hayan ejecutado en la red.
- Cuentas de usuario creadas en AD o equipos agregados a la red durante la explotación.
- Direcciones de correo electrónico que hayan utilizado los atacantes y cualquier correo electrónico de suplantación de identidad asociado.
- Otras cuentas de comunicación que hayan utilizado los atacantes.
- Una copia de la nota de rescate.
- El monto del rescate y si se pagó.
- Monederos Bitcoin que hayan utilizado los atacantes.
- Monederos Bitcoin utilizados para pagar el rescate, si corresponde.
- Copias de cualquier comunicación con los atacantes.

☐ **8.** Si el incidente produjo una filtración de datos, **siga los requisitos de notificación descritos en su plan de comunicaciones y respuesta a incidentes cibernéticos.**

## Contención y erradicación

**Si no parece posible adoptar medidas iniciales de mitigación:**

☐ **9. Tome una imagen del sistema y una captura de memoria de una muestra de los dispositivos afectados (p. ej., estaciones de trabajo, servidores, servidores virtuales y servidores en la nube).** Recopile cualquier registro relevante, así como muestras de cualquier binario de malware "precursor" y elementos observables o indicadores de riesgo asociados (p. ej., direcciones IP de comando y control sospechosas, entradas de registro sospechosas u otros archivos relevantes detectados). Los contactos que figuran a continuación pueden ayudarlo a realizar estas tareas.

- ☐ Preserve las pruebas que sean de naturaleza muy volátil (o de retención limitada) para evitar pérdidas o alteraciones (p. ej., memoria del sistema, registros de seguridad de Windows, datos en los búferes de registro del cortafuegos).

Tras un pedido voluntario, la CISA y el MS-ISAC (para organizaciones SLTT) pueden ayudar con el análisis de correos electrónicos de suplantación de identidad, medios de almacenamiento, registros o malware sin costo para ayudar a las organizaciones a comprender la causa raíz de un incidente.

- Centro de Análisis Avanzado de Malware (Advanced Malware Analysis Center) de la CISA: malware.us-cert.gov/
- Plataforma de análisis de código malicioso del MS-ISAC (solo para organizaciones SLTT): cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/

☐ **10. Consulte a la Policía federal, incluso si es posible adoptar medidas de mitigación, sobre posibles descifradores disponibles,** ya que los investigadores de seguridad pueden haber descubierto fallas de cifrado para algunas variantes de ransomware y haber publicado herramientas de descifre o de otro tipo.

**Para seguir tomando medidas a fin de contener y mitigar el incidente:**

☐ **11. Busque orientación fiable** (p. ej., publicada por ciertas fuentes, como el Gobierno de EE. UU., el MS-ISAC o un proveedor de seguridad acreditado) para la variante de ransomware en particular y siga cualquier paso recomendado adicional a fin de identificar y contener los sistemas o las redes que se haya confirmado que se vieron afectados.

- ☐ Elimine o deshabilite la ejecución de binarios de ransomware conocidos; esto minimizará el daño y el impacto en sus sistemas. Elimine otros archivos y valores de registro asociados conocidos.

☐ **12. Identifique los sistemas y las cuentas involucrados en la vulneración inicial.** Esto puede incluir cuentas de correo electrónico.

☐ **13.** Según los detalles sobre la vulneración o el riesgo determinados más arriba, **contenga los sistemas asociados que puedan utilizarse para un acceso no autorizado posterior o continuo.** Las vulneraciones, a menudo, implican una exfiltración masiva de credenciales. El aseguramiento de las redes y de otras fuentes de información contra el acceso no autorizado y continuo basado en credenciales puede incluir lo siguiente:

- ☐ Deshabilite las redes privadas virtuales, los servidores de acceso remoto, los recursos de inicio de sesión único y los activos públicos basados en la nube o de otro tipo.

☐ **14.** Si una estación de trabajo infectada está cifrando datos del lado del servidor, **siga los pasos de identificación rápida del cifrado de datos del lado del servidor.**

- ☐ Revise Administración de equipos > Sesiones y las listas de Archivos abiertos en los servidores asociados para determinar el usuario o el sistema que accede a esos archivos.
- ☐ Revise las propiedades de los archivos cifrados o las notas de rescate para identificar usuarios específicos que puedan estar asociados a la propiedad de los archivos.
- ☐ Revise el registro de eventos de `TerminalServices-RemoteConnectionManager` para verificar si hay conexiones de red del RDP satisfactorias.
- ☐ Revise el registro de seguridad de Windows, los registros de eventos de SMB y los registros relacionados que puedan identificar eventos importantes de autenticación o acceso.
- ☐ Ejecute un software de captura de paquetes, como Wireshark, en el servidor afectado con un filtro para identificar las direcciones IP involucradas en la escritura activa o el cambio de nombre de archivos (p. ej., `smb2.filename contains cryptxxx`).

☐ **15. Realice un análisis extendido para identificar los mecanismos de persistencia de interacción indirecta y de interacción directa.**

- ☐ La persistencia de interacción indirecta puede incluir el acceso autenticado a los sistemas externos a través de cuentas no autorizadas, las puertas traseras en los sistemas perimetrales, la explotación de las vulnerabilidades externas, etc.
- ☐ La persistencia de interacción directa puede incluir implantes de malware en la red interna o una variedad de modificaciones al estilo “living-off-the-land” (p. ej., el uso de herramientas comerciales de pruebas de penetración, como Cobalt Strike; el uso del conjunto PsTools, incluido PsExec, para instalar y controlar malware de forma remota, y recopilar información relativa a los sistemas Windows o realizar su administración remota; el uso de scripts de PowerShell).
- ☐ La identificación puede implicar la implementación de soluciones de EDR, auditorías de cuentas locales y de dominio, la revisión de los datos encontrados en los sistemas de registro centralizados o un análisis forense más profundo de sistemas específicos una vez que se ha trazado el movimiento dentro del entorno.

☐ **16. Reconstruya los sistemas con base en la priorización de los servicios fundamentales** (p. ej., salud y seguridad o servicios generadores de ingresos) mediante el uso de imágenes estándar preconfiguradas si es posible. Utilice la infraestructura como plantillas de código para reconstruir los recursos en la nube.

☐ **17. Emita restablecimientos de contraseña para todos los sistemas afectados y aborde cualquier vulnerabilidad asociada y deficiencia en la seguridad o visibilidad** una vez que el entorno se haya limpiado y reconstruido completamente, lo que incluye cualquier cuenta afectada asociada y la eliminación o la corrección de los mecanismos de persistencia maliciosos. Esto puede incluir aplicar correcciones, actualizar el software y tomar otras precauciones de seguridad que no se hayan adoptado previamente. Actualice las claves de cifrado administradas por el cliente según sea necesario.

☐ **18. La autoridad de tecnología de la información o de seguridad informática designada declara finalizado el incidente de ransomware** según criterios establecidos, que pueden incluir seguir los pasos anteriores o buscar asistencia externa**.**

## Recuperación y actividad posterior al incidente

- ☐ **19. Reconecte los sistemas y restaure los datos a partir de copias de seguridad cifradas sin conexión, con base en una priorización de los servicios fundamentales.**
  - ☐ Tenga cuidado de no reinfectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva red de área local virtual (VLAN, por sus siglas en inglés) con fines de recuperación, asegúrese de que solo se agreguen sistemas limpios.

- ☐ **20. Documente las conclusiones obtenidas a partir del incidente y las actividades de respuesta asociadas** para actualizar y perfeccionar las políticas, los planes y los procedimientos de la organización, y orientar futuros ejercicios relacionados con ellos.

- ☐ **21. Considere compartir las conclusiones y los indicadores de riesgo relevantes con la CISA o el ISAC de su sector** para beneficiar a otros dentro de la comunidad.

# Información de contacto

En respuesta a cualquier incidente cibernético, las agencias federales llevarán a cabo la respuesta a las amenazas, la respuesta a los activos y el apoyo de inteligencia y las actividades relacionadas.

**Qué puede esperar:**

- Orientación específica para ayudar a evaluar y corregir incidentes de ransomware.
- Asistencia remota para identificar el alcance del riesgo y recomendaciones sobre estrategias de contención y mitigación adecuadas (en función de la variante de ransomware específica).
- Análisis de correos electrónicos de suplantación de identidad, medios de almacenamiento, registros y malware basados en envíos voluntarios. Se pueden realizar análisis forenses de todo el disco en función de las necesidades.
- Asistencia en la realización de una investigación criminal, que puede involucrar la recopilación de artefactos del incidente, como imágenes del sistema y muestras de malware.

## Contactos de respuesta federal a los activos

Ante una solicitud voluntaria, la respuesta federal a los activos incluye brindar asistencia técnica a las entidades afectadas para proteger sus activos, mitigar las vulnerabilidades y reducir los impactos de los incidentes cibernéticos; identificar otras entidades que puedan estar en riesgo y evaluar su riesgo de vulnerabilidades iguales o similares; evaluar los riesgos potenciales para el sector o la región, incluidos los posibles efectos en cascada, y desarrollar medidas para mitigar estos riesgos; facilitar el intercambio de información y la coordinación operativa con la respuesta a amenazas; y brindar orientación sobre la mejor manera de utilizar los recursos y las capacidades federales de manera oportuna y efectiva para acelerar la recuperación.

| | |
|---|---|
| **CISA:** | cisa.gov/report<br><br>Central@cisa.gov o llame al (888) 282-0870<br><br>Asesor de ciberseguridad (cisa.gov/cisa-regions): [Ingrese la dirección de correo electrónico y el número de teléfono del asesor de ciberseguridad (CSA, por sus siglas en inglés) de la CISA de su localidad]. |
| **MS-ISAC:** | Para entidades SLTT, envíe un correo electrónico a soc@msisac.org o llame al (866) 787-4722 |

## Contactos de respuesta federal a las amenazas

Ante una solicitud voluntaria, o tras la notificación a los socios, la respuesta federal a amenazas incluye llevar a cabo actividades adecuadas de investigación policial y de seguridad nacional en el sitio de la entidad afectada, recabar pruebas y recopilar información, proporcionar atribución, vincular incidentes relacionados, identificar otras entidades afectadas, identificar oportunidades de persecución de la amenaza e interrupción, desarrollar y ejecutar medidas para mitigar la amenaza inmediata, y facilitar el intercambio de información y la coordinación operativa con la respuesta a activos.

| | |
|---|---|
| **FBI:** | fbi.gov/contact-us/field-offices [Ingrese el número de teléfono y la dirección de correo electrónico del POC de su oficina local de la FBI]. |
| **Servicio Secreto de EE. UU. (USSS, por sus siglas en inglés):** | Centro de Denuncias de Delitos en Internet (IC3) de la FBI en ic3.gov<br>secretservice.gov/contact/field-offices/ [Ingrese el número de teléfono y la dirección de correo electrónico del POC de su oficina local del USSS]. |

## Otros contactos de respuesta federal

**NSA:** Servicios del Centro de Colaboración de Ciberseguridad (Cybersecurity Collaboration Center) e información de contacto

### Otros contactos de respuesta

Considere la posibilidad de completar la Tabla 1 para su uso en caso de que su organización se vea afectada por el ransomware. Considere comunicarse con estas organizaciones para obtener asistencia de mitigación y respuesta o para recibir notificaciones.

*Tabla 1: Información de los contactos de respuesta*

| **Contactos de respuesta:** | | |
|---|---|---|
| **Contacto** | **Información de contacto 24x7** | **Roles y responsabilidades** |
| **Equipo de tecnología de la información/seguridad informática: informes centralizados de incidentes cibernéticos** | | |
| **Líderes departamentales o electos** | | |
| **Policía estatal y local** | | |
| **Centro de fusión** | | |
| **Proveedores de servicios de seguridad/administrados** | | |
| **Seguros cibernéticos** | | |

# RECURSOS

## Recursos gratuitos de la CISA

- El intercambio de información con la CISA y el MS-ISAC (para las organizaciones SLTT) es bidireccional. Esto incluye las prácticas recomendadas y la información de defensa de redes en relación con las tendencias y las variantes de ransomware, así como el malware que es precursor del ransomware.
- Las evaluaciones técnicas u orientadas a políticas ayudan a las organizaciones a comprender cómo pueden mejorar su defensa para evitar la infección de ransomware: cisa.gov/cyber-resource-hub.
    - Las evaluaciones incluyen el análisis gratuito de vulnerabilidades.
- Los ejercicios cibernéticos evalúan o ayudan a desarrollar un plan de respuesta a incidentes cibernéticos en el contexto de un escenario de incidente de ransomware: cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.
- Los asesores de ciberseguridad de la CISA brindan asesoramiento sobre las prácticas recomendadas y lo conectan con los recursos de la CISA para administrar los riesgos cibernéticos.
- La herramienta de evaluación de ciberseguridad (CSET, por sus siglas en inglés) guía a los propietarios y operadores de activos a través de un proceso sistemático de evaluación de la tecnología operativa (OT, por sus siglas en inglés) y la tecnología de la información. La CSET incluye la Evaluación de preparación para ransomware (RRA, por sus siglas en inglés), una autoevaluación basada en un conjunto escalonado de prácticas con el propósito de ayudar a las organizaciones a evaluar qué tan bien equipadas están para defenderse y recuperarse de un incidente de ransomware.

### *Contactos:*

- Organizaciones SLTT y del sector privado: CISA.JCDC@cisa.dhs.gov

## Referencias rápidas sobre ransomware

- StopRansomware.gov: una página web gubernamental que ofrece recursos y alertas sobre ransomware.
- Cartilla de seguridad sobre el ransomware (MS-ISAC): describe las campañas oportunistas y estratégicas de ransomware, los vectores de infección comunes y las sugerencias de prácticas recomendadas.
- Plan de defensa contra el ransomware del Instituto de Seguridad y Tecnología (IST, por sus siglas en inglés): un plan de acción para la mitigación y la recuperación del ransomware, así como la respuesta a este, para pequeñas y medianas empresas.

## Recursos adicionales

- NIST: Arquitectura de confianza cero
- CISA: Arquitectura de referencia técnica de seguridad en la nube
- CISA: Proyecto de Aplicaciones Empresariales Seguras en la Nube (SCuBA, por sus siglas en inglés)
- CISA: Medidas de mitigación y orientación para el refuerzo para MSP y pequeñas y medianas empresas
- CISA: Protección contra amenazas cibernéticas para proveedores de servicios administrados y sus clientes
- NSA: Mitigación de las vulnerabilidades de la nube (NSA)

## DESCARGO DE RESPONSABILIDAD DE RESPALDO

La información y opiniones contenidas en este documento se proporcionan “tal cual” y sin garantías. En este documento, la referencia a cualquier producto, proceso o servicio comercial específico por nombre comercial, marca registrada o fabricante no constituye ni implica su respaldo, recomendación o preferencia por parte del Gobierno de Estados Unidos, y esta orientación no se utilizará con fines publicitarios ni de promoción de productos.

## PROPÓSITO

Este documento se desarrolló para promover las misiones de seguridad cibernética de los autores, lo que incluye las responsabilidades de estas de identificar y difundir amenazas, y de desarrollar y publicar especificaciones y medidas de seguridad cibernética para mitigar amenazas. Esta información se puede compartir ampliamente para llegar a todas las partes interesadas apropiadas.

## AGRADECIMIENTOS

Microsoft contribuyó a esta guía conjunta.