TLP:BORR

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

Guía #StopRansomware

Publicación: Mayo 2023

habituales sobre derechos de autor. Para más información sobre el Protocolo del Semáforo, véase cisa.gov/tlp.

Cambiar registro

Versión	Fecha	Revisión/Cambio Descripción	Sección/Página afectada
1.0	Septiembre de 2020	Versión inicial	
2.0	Mayo de 2023	Ver "Novedades" en p.3	Actualizaciones

INTRODUCCIÓN

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

Estos incidentes de ransomware y violación de datos asociados pueden afectar gravemente a los procesos empresariales al dejar a las organizaciones incapaces de acceder a los datos necesarios para operar y prestar servicios de misión crítica. El impacto económico y reputacional del ransomware y la extorsión de datos ha demostrado ser un reto y costoso para las organizaciones de todos los tamaños a lo largo de la interrupción inicial y, a veces, la recuperación extendida.

Esta guía es una actualización de la Guía sobre ransomware de la Agencia Conjunta de Ciberseguridad y Seguridad de las Infraestructuras (CISA) y el Centro Interestatal de Análisis e Intercambio de Información (MS-ISAC) publicada en septiembre de 2020 (véase Novedades) y fue desarrollada a través del JRTF. Esta guía incluye dos recursos principales:

Esta guía ha sido elaborada por la U.S. Joint Ransomware Task Force (JRTF).

La JRTF, copresidida por CISA y el FBI, es un esfuerzo de colaboración entre agencias para combatir la creciente amenaza de los ataques de ransomware. La JRTF se puso en marcha en respuesta a una serie de ataques de ransomware de alto perfil contra infraestructuras críticas y agencias gubernamentales estadounidenses. La JRTF:

- Coordina y agiliza la respuesta del Gobierno de Estados Unidos a los ataques de ransomware y facilita el intercambio de información y la colaboración entre las agencias gubernamentales y los socios del sector privado.
- Garantiza la coordinación operativa de actividades como el desarrollo y el intercambio de mejores prácticas para prevenir y responder a los ataques de ransomware, la realización de investigaciones y operaciones conjuntas contra los autores de amenazas de ransomware, y el suministro de orientación y recursos a las organizaciones que han sido víctimas de ransomware.
- Representa un importante paso adelante

- Parte 1: Prácticas recomendadas para la prevención del ransomware y la extorsión de datos
- Parte 2: Lista de comprobación de la respuesta al ransomware y la extorsión de datos

La Parte 1 proporciona orientación a todas las organizaciones para reducir el impacto y la probabilidad de incidentes de ransomware y extorsión de datos, incluyendo las mejores prácticas para preparar, prevenir y mitigar estos incidentes. Las mejores prácticas de prevención se agrupan por vectores comunes de acceso inicial. La Parte 2 incluye una lista de comprobación de las mejores prácticas

para responder a estos incidentes.

Estas mejores prácticas y recomendaciones de prevención y respuesta ante el ransomware y la extorsión de datos se basan en los conocimientos operativos de CISA, MS-ISAC, la Agencia de Seguridad Nacional (NSA) y la Oficina Federal de Investigación (FBI), en lo sucesivo denominadas organizaciones autoras. El sitio

Los destinatarios de esta guía son los profesionales de las tecnologías de la información (TI), así como otras personas de una organización implicadas 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 y proteger sus instalaciones, personal y clientes de las amenazas a la seguridad cibernética y física y otros peligros:

- Únase a un centro sectorial de intercambio y análisis de información (ISAC), si cumple los requisitos, como:
    - MS-ISAC para entidades gubernamentales estatales, locales, tribales y territoriales (SLTT) de EE.UU. - learn.cisecurity.org/ms-isac-registration. La afiliación al MS-ISAC está abierta a representantes de los 50 estados, el Distrito de Columbia, los territorios de EE.UU., los gobiernos locales y tribales, las entidades públicas de educación K-12, las instituciones públicas de educación superior, las autoridades y cualquier otra entidad pública no federal de los Estados Unidos.
    - Centro de Análisis e Intercambio de Información sobre Infraestructuras Electorales (EI-ISAC) para Organizaciones Electorales de EE.UU. - learn.cisecurity.org/ei-isac-registration.

      Para más información, consulte el Consejo Nacional de ISAC.
- Póngase en contacto con CISA en CISA.JCDC@cisa.dhs.gov para colaborar en el intercambio de información, mejores prácticas, evaluaciones, ejercicios y mucho más.
- Póngase en contacto con su oficina local del FBI para obtener una lista de puntos de contacto (POC) en caso de incidente cibernético.

La colaboración con organizaciones homólogas y CISA permite a su organización recibir información crítica y oportuna en y acceder a servicios para gestionar el ransomware y otras ciberamenazas.

Novedades

Desde la publicación inicial de la Guía de ransomware en septiembre de 2020, los actores del ransomware han acelerado sus tácticas y técnicas.

Para mantener la pertinencia, añadir perspectiva y maximizar la eficacia de esta guía, se han introducido los siguientes cambios:

- Se han añadido el FBI y la NSA como coautores por sus contribuciones y su visión operativa.
- Incorporó la campaña #StopRansomware en el título.
- Se han añadido recomendaciones para prevenir los vectores de infección iniciales más comunes, incluidas las credenciales comprometidas y las formas avanzadas de

#StopRansomware es el esfuerzo de CISA y el FBI para publicar avisos para los defensores de la red que detallan información de defensa de la red relacionada con diversas variantes de ransomware y actores de amenazas. Visite stopransomware.gov para obtener más

ingeniería social.

- Recomendaciones actualizadas para abordar las copias de seguridad en la nube y la arquitectura de confianza cero (ZTA).
- Ampliación de la lista de comprobación de respuesta al ransomware con consejos de caza de amenazas para su detección y análisis.
- Las recomendaciones se ajustan a los objetivos intersectoriales de la CISA en materia de ciberseguridad (CPG).

Parte 1: Mejores prácticas de preparación, prevención y mitigación del ransomware y la extorsión de datos

Estas mejores prácticas recomendadas se alinean con las CPG desarrolladas por CISA y el Instituto Nacional de Normas y Tecnología (NIST). Las CPG proporcionan un conjunto mínimo de prácticas y protecciones que CISA y NIST recomiendan que todas las organizaciones implementen. CISA y NIST basaron las CPGs en marcos y guías de ciberseguridad existentes para proteger contra las amenazas, tácticas, técnicas y procedimientos más comunes e impactantes. Para más información sobre las CPG y las protecciones básicas recomendadas, visite CISA's Cross-Sector Cybersecurity Performance Goals.

Preparación para incidentes de ransomware y extorsión de datos

Consulte las mejores prácticas y referencias enumeradas en esta sección para ayudar a gestionar los riesgos que plantea el ransomware e impulsar una respuesta coordinada y eficaz para su organización en caso de incidente. Aplique estas prácticas en la mayor medida posible en función de la disponibilidad de recursos de la organización.

- **Mantener copias de seguridad fuera de línea y cifradas de los datos críticos**, y probar regularmente la disponibilidad e integridad de las copias de seguridad en un escenario de recuperación de desastres [CPG 2.R]. Prueba los procedimientos de copia de seguridad de forma regular. Es importante que las copias de seguridad se mantengan offline, ya que muchas variantes de ransomware intentan encontrar y posteriormente borrar o cifrar las copias de seguridad accesibles para hacer imposible su restauración a menos que se pague el rescate.

> 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, posiblemente sobrescribiendo los datos no

  - Mantener y actualizar regularmente "imágenes doradas" de sistemas críticos. Esto incluye mantener "plantillas" de imágenes que tengan un sistema operativo (SO) preconfigurado y aplicaciones de software asociadas que puedan desplegarse rápidamente para reconstruir un sistema, como una máquina virtual o un servidor [CPG 2.O].
    - Utilizar la infraestructura como código (IaC) para desplegar y actualizar los recursos de la nube y mantener copias de seguridad de los archivos de plantillas fuera de línea para volver a desplegar rápidamente los recursos. El código IaC debe estar controlado por versiones y los cambios en las plantillas deben auditarse.
    - Almacena el código fuente o los ejecutables aplicables con copias de seguridad sin conexión (así como los acuerdos de custodia y licencia). Reconstruir a partir de imágenes del sistema es más eficiente, pero algunas imágenes no se instalarán correctamente en hardware o plataformas diferentes; tener acceso independiente al software ayuda en estos casos.
  - Conserve el hardware de reserva para reconstruir los sistemas si no se prefiere reconstruir el sistema primario.

        - Considere la posibilidad de sustituir el hardware obsoleto que impide la restauración por hardware actualizado, ya que el hardware antiguo puede presentar obstáculos de instalación o compatibilidad al reconstruir a partir de imágenes.
    - Considere la posibilidad de utilizar una solución multi-nube para evitar la dependencia del proveedor en las copias de seguridad de nube a nube en caso de que todas las cuentas del mismo proveedor se vean afectadas.

        - Algunos proveedores de servicios en la nube ofrecen soluciones de almacenamiento inmutable que pueden proteger los datos almacenados sin necesidad de un entorno independiente. Utiliza el almacenamiento inmutable con precaución, ya que no cumple los criterios de conformidad de determinadas normativas y una mala configuración puede suponer un coste significativo.

- **Crear, mantener y ejercitar regularmente un plan básico de respuesta a incidentes cibernéticos (IRP) y un plan de comunicaciones asociado que incluya procedimientos de respuesta y notificación** para incidentes de ransomware y extorsión/violación de datos [CPG 2.S]. Garantizar la disponibilidad de una copia impresa del plan y una versión offline.
    - Asegúrese de que los procedimientos de notificación de violación de datos cumplen la legislación estatal aplicable. Consulte la Conferencia Nacional de Legislaturas Estatales: Security Breach Notification Laws para obtener información sobre las leyes de notificación de violaciones de datos de cada estado y consulte a un asesor jurídico cuando sea necesario.
    - En el caso de las filtraciones de información sanitaria electrónica, es posible que deba notificarlo a la Comisión Federal de Comercio (FTC) o al Departamento de Salud y Servicios Humanos (HHS) y, en algunos casos, a los medios de comunicación. Para más información, consulte la Regla de Notificación de Infracciones Sanitarias de la FTC y la Regla de Notificación de Infracciones del HHS.
    - En el caso de filtraciones que afecten a información de identificación personal (IIP), notifíquelo a las personas afectadas para que puedan tomar medidas para reducir la posibilidad de que su información sea utilizada indebidamente. Indique el tipo de información expuesta, recomiende medidas correctoras y facilite la información de contacto pertinente.
    - Notificar a las empresas de una infracción si se roba información de identificación personal almacenada en nombre de otras empresas.
    - Garantizar que el IRP y el plan de comunicación sean revisados y aprobados por escrito por el CEO, o equivalente, y que ambos sean revisados y comprendidos por toda la cadena de mando.
    - Revise la guía de respuesta a incidentes disponible, como la Lista de comprobación de respuesta a ransomware de esta guía y el Manual de respuesta a incidentes cibernéticos del sector público:
        - Ayude a su organización a organizarse mejor en torno a la respuesta a incidentes cibernéticos.
        - Borrador de las declaraciones de retención de incidentes cibernéticos.
        - Desarrollar un PIR cibernético.
    - Incluir en el plan de comunicación los procedimientos de comunicación de la organización, así como plantillas para las declaraciones de retención de incidentes cibernéticos. Llegar a un consenso sobre qué nivel de detalle es apropiado compartir dentro de la organización y con el público y cómo fluirá la información.

- **Implantar una arquitectura de confianza cero** para impedir el acceso no autorizado a datos y servicios. Hacer que la aplicación del control de acceso sea lo más granular posible. La ZTA

asume que una red está comprometida 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 sistemas y servicios de información.

Prevención y mitigación de incidentes de ransomware y extorsión de datos

Consulte las mejores prácticas y referencias enumeradas en esta sección para ayudar a prevenir y mitigar los incidentes de ransomware y extorsión de datos. Las mejores prácticas de prevención se agrupan por vectores de acceso inicial comunes de los actores del ransomware y la extorsión de datos.

Vector de acceso inicial: Vulnerabilidades y errores de configuración frente a Internet

- **Llevar a cabo un escaneo regular de vulnerabilidades para identificar y abordar las vulnerabilidades**, especialmente las de los dispositivos orientados a Internet, para limitar la superficie de ataque [CPG 1.E].
    - CISA ofrece un servicio gratuito de exploración de vulnerabilidades y otras evaluaciones gratuitas: cisa.gov/cyber-resource-hub [CPG 1.F].
- **Parchee y actualice periódicamente el software y los sistemas operativos a las últimas versiones disponibles**.
    - Dé prioridad a la aplicación oportuna de parches en los servidores orientados a Internet -que utilizan programas informáticos para procesar datos de Internet, como navegadores web, complementos de navegadores y lectores de documentos-, especialmente para detectar vulnerabilidades conocidas.
    - Las organizaciones autoras -conscientes de las dificultades que tienen las pequeñas y medianas empresas para mantener actualizados los servidores orientados a Internet- instan a migrar los sistemas a proveedores de nube "gestionados" de confianza para reducir, no eliminar, las funciones de mantenimiento de los sistemas de identidad y correo electrónico. Para más información, visite la página de información sobre ciberseguridad de la NSA Mitigar las vulnerabilidades de la nube.
- **Asegúrese de que todos los dispositivos locales, de servicios en la nube, móviles y personales (es decir, traiga su propio dispositivo [BYOD]) estén configurados correctamente y que las funciones de seguridad estén activadas**. Por ejemplo, desactive los puertos y protocolos que no se utilicen con fines empresariales (por ejemplo, el protocolo de escritorio remoto [RDP] - Protocolo de control de transmisión [TCP] Puerto 3389) [CPG 2.X].
    - Reduzca o elimine los despliegues manuales y codifique la configuración de los recursos en la nube mediante IaC. Pruebe las plantillas de IaC antes del despliegue con herramientas de análisis de seguridad estática para identificar errores de configuración y brechas de seguridad.
    - Compruebe de forma rutinaria si la configuración ha cambiado para identificar los recursos que se han modificado o introducido fuera del despliegue de plantillas, reduciendo así la probabilidad de que se introduzcan nuevas brechas de seguridad y configuraciones erróneas. Aproveche los servicios de los proveedores de la nube para automatizar o facilitar la auditoría de los recursos con el fin de garantizar una línea de base coherente.
- **Limite el uso de RDP y otros servicios de escritorio remoto**. Si el RDP es necesario, aplique las mejores prácticas. Los actores de amenazas a menudo obtienen acceso inicial a una red a través de servicios remotos expuestos y mal protegidos, y más tarde atraviesan la

red utilizando el cliente nativo de Windows RDP. Los actores de amenazas también suelen obtener acceso explotando redes privadas virtuales (VPN) o utilizando credenciales comprometidas. Consulte el CISA Advisory: Enterprise VPN Security.

- Audite la red en busca de sistemas que utilicen RDP, cierre los puertos RDP no utilizados, aplique bloqueos de cuentas tras un número determinado de intentos, aplique autenticación multifactor (MFA) y registre los intentos de inicio de sesión RDP.

- Actualice las VPN, los dispositivos de infraestructura de red y los dispositivos utilizados para acceder remotamente a los entornos de trabajo con los últimos parches de software y configuraciones de seguridad. Implemente MFA en todas las conexiones VPN para aumentar la seguridad. Si no se implementa MFA, exija a los teletrabajadores que utilicen contraseñas de 15 caracteres o más.

- **Deshabilite las versiones 1 y 2 del protocolo Server Message Block (SMB)** y actualice a la versión 3 (SMBv3) después de mitigar las dependencias existentes (por parte de los sistemas o aplicaciones existentes) que puedan romperse al deshabilitarlo. Los actores maliciosos utilizan SMB para propagar malware a través de las organizaciones, por lo que se debe endurecer SMBv3:
  - Bloquee o limite el tráfico SMB interno a los sistemas que requieren acceso. Esto debería limitar las intrusiones que se mueven lateralmente a través de su red.
  - Implemente la firma SMB. Esto debería evitar ciertos ataques de adversario en el medio y pass- the-hash. Para obtener más información, consulte Microsoft Mitigating New Technology Local Area Network (LAN) Manager (NTLM) Relay Attacks on Active Directory Certificate Services (AD CS) y Microsoft Overview of Server Message Block Signing.
  - Bloquee el acceso externo de SMB a su red bloqueando el puerto TCP `445` con los protocolos relacionados en los puertos `137-138` del Protocolo de Datagramas de Usuario (UDP) y el puerto TCP `139`.
  - Implemente el cifrado SMB con la Convención de Nomenclatura Universal (UNC) para los sistemas que admiten esta función. Esto debería limitar la posibilidad de ataques de escucha e interceptación.
  - Registre y supervise el tráfico SMB para ayudar a detectar comportamientos potencialmente anómalos.

Vector de acceso inicial: Credenciales comprometidas

- **Implantar una AMF resistente al phishing para todos los servicios**, en particular para el correo electrónico, las VPN y las cuentas que acceden a sistemas críticos [CPG 2.H]. Informar a la alta dirección cuando se descubran sistemas que no permitan la AMF, sistemas que no apliquen la AMF y usuarios que no estén registrados con la AMF.
  - **Considere la posibilidad de emplear una AMF sin** contraseña que sustituya las contraseñas por dos o más factores de verificación (por ejemplo, una huella dactilar, el reconocimiento facial, el pin del dispositivo o una clave criptográfica).
- **Considere la posibilidad de suscribirse a servicios de supervisión de credenciales** que vigilan la web oscura en busca de credenciales comprometidas.
- **Implantar sistemas de gestión de identidades y accesos (IAM)** para proporcionar a los administradores las herramientas y tecnologías necesarias para supervisar y gestionar las funciones y los privilegios de acceso de entidades de red individuales para aplicaciones locales y en la nube.
- **Implantar un control de acceso de confianza cero** creando políticas de acceso sólidas para restringir el acceso de usuario a recurso y de recurso a recurso. Esto es importante

para los recursos de gestión de claves en la nube.

- **Cambiar los nombres de usuario y contraseñas de administrador por defecto**. [CPG 2.A].
- **No utilices cuentas de acceso root para las operaciones cotidianas**. Cree usuarios, grupos y roles para llevar a cabo las tareas.
- **Implemente políticas de contraseñas que requieran contraseñas únicas de al menos 15 caracteres**. [CPG 2.B] [CPG 2.C].

  - Los gestores de contraseñas pueden ayudarle a desarrollar y gestionar contraseñas seguras. Asegure y limite el acceso a cualquier gestor de contraseñas en uso y active todas las funciones de seguridad disponibles en el producto en uso, como MFA.

- **Aplicar políticas de bloqueo de cuentas después de un cierto número de intentos fallidos de inicio de sesión**. Registrar y supervisar los intentos de inicio de sesión para el descifrado 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 hash potentes**.
- **Desactivar el almacenamiento de contraseñas en el navegador en la consola de administración de directivas de grupo**.
- **Implemente la solución de contraseña de administrador local (LAPS)** siempre que sea posible si su sistema operativo es anterior a Windows Server 2019 y Windows 10, ya que estas versiones no tienen LAPS integrado. **Nota:** Las organizaciones autoras recomiendan que las organizaciones actualicen a Windows Server 2019 y Windows 10 o superior.
- Protección contra el dumping del Servicio de Subsistema de Autoridad de Seguridad Local (LSASS):
  - **Implementar la regla de Reducción de Superficie de Ataque (ASR) para LSASS.**
  - **Implemente Credential Guard para Windows 10 y Server 2016**. Consulte Microsoft Manage Windows Defender Credential Guard para obtener más información. Para Windows Server 2012R2, habilite Protected Process Light (PPL) para Local Security Authority (LSA).
- **Eduque a todos los empleados sobre la seguridad adecuada de las contraseñas en su formación anual sobre seguridad**, haciendo hincapié en no reutilizar las contraseñas y no guardarlas en archivos locales.
- **Utilice Windows PowerShell Remoting, Remote Credential Guard o RDP** con modo de administración restringido cuando establezca una conexión remota para evitar la exposición directa de las credenciales.
- **Separar las cuentas de administrador de las cuentas de usuario** [CPG 2.E]. Sólo permite que las cuentas de administrador designadas sean usadas para propósitos 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 de nube, separe las funciones cuando la cuenta utilizada para aprovisionar/gestionar claves no tenga permiso para utilizar las claves y viceversa. Como esta estrategia introduce una sobrecarga de gestión adicional, no es apropiada en todos los entornos.

Vector de acceso inicial: Phishing

- **Implantar un programa de concienciación y formación sobre ciberseguridad para los usuarios** que incluya orientaciones sobre cómo identificar e informar de actividades sospechosas (por ejemplo, phishing) o incidentes [CPG 2.I].
- **Marcar los correos electrónicos externos en los clientes de correo electrónico**.
- **Implementar filtros en el gateway de correo electrónico para filtrar correos electrónicos** con indicadores maliciosos conocidos, como líneas de asunto maliciosas conocidas, y bloquear direcciones de Protocolo de Internet (IP) sospechosas

CISA ofrece una evaluación gratuita de campañas de phishing y otras evaluaciones gratuitas. Visite cisa.gov/cyber-resource-hub.

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 más información, consulte el post de Microsoft Protección antimalware en EOP.

  - Revise los tipos de archivos de su lista de filtros al menos semestralmente 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 phishing.
  - Los programas maliciosos suelen comprimirse en archivos protegidos por contraseña que eluden los escáneres antivirus y los filtros de correo electrónico.

- **Implantación de la política de autenticación, notificación y conformidad de mensajes basada en dominios (DMARC) y verificación** para reducir los costes. la posibilidad de mensajes falsos o modificados de dominios válidos. DMARC protege su dominio de la suplantación de identidad, pero no protege de los correos electrónicos entrantes que han sido suplantados, a menos que el dominio remitente también implemente DMARC. DMARC se basa en los protocolos ampliamente implantados Sender Policy Framework (SPF) y Domain Keys Identified Mail (DKIM), añadiendo una función de informes que permite a remitentes y receptores mejorar y supervisar la protección del dominio frente al correo electrónico fraudulento. Para más información sobre DMARC, consulte CISA Insights Enhance Email & Web Security y el blog del Center for Internet Security How DMARC Advances Email Security.

Malicious Domain Blocking and Reporting (MDBR) es un servicio gratuito para organizaciones SLTT financiado por CISA, MS-ISAC y EI-ISAC. Este servicio de seguridad totalmente gestionado impide que los sistemas informáticos se conecten a dominios web dañinos y protege contra las ciberamenazas,

- Malware,
- ransomware y
- Phishing.

Para inscribirse en el MDBR, visite cisecurity.org/ms-

- **Asegúrese de que las secuencias de comandos de macros están desactivadas para los archivos de Microsoft Office transmitidos por correo electrónico**. Estas macros pueden utilizarse para enviar ransomware [CPG 2.N]. **Nota: Las** versiones recientes de Office están configuradas por defecto para bloquear los archivos que contienen macros de Visual Basic para Aplicaciones (VBA) y mostrar una barra de confianza con una advertencia de que las macros están presentes y se han desactivado. Para obtener más información, consulte Microsoft's Las macros de Internet se bloquearán de forma predeterminada en Office. Consulte Bloquear la ejecución de macros en archivos de Office desde Internet de Microsoft para obtener instrucciones de configuración para desactivar las macros en archivos externos para versiones anteriores de Office.
- **Desactivar el alojamiento de scripts de Windows (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 su software antivirus y antimalware y sus firmas**. Asegúrese de que las herramientas configurado para escalar los avisos y indicadores para avisar al personal de seguridad. Las organizaciones autoras recomiendan utilizar una solución antivirus gestionada de forma centralizada. Esto permite detectar tanto el malware "precursor" como el ransomware.

CISA y MS-ISAC animan a las organizaciones SLTT a utilizar Albert IDS para mejorar una estrategia de defensa en profundidad. Albert sirve como una capacidad de alerta temprana para los gobiernos SLTT de EE.UU. y apoya la conciencia situacional y la defensa de la ciberseguridad a nivel nacional. Para más información sobre Albert, visite cisecurity.org/services/albert-network

    - Una infección de ransomware puede ser la prueba de una infección anterior no resuelta. compromiso de la red. Por ejemplo, muchas infecciones de ransomware son el resultado de infecciones de malware ya existentes, como QakBot, Bumblebee y Emotet.
    - En algunos casos, el despliegue del ransomware es el último paso en el compromiso de una red y se deja caer para ocultar actividades previas posteriores al compromiso, como el compromiso del correo electrónico empresarial (BEC).
- **Utilice listas de aplicaciones permitidas y/o soluciones de detección y respuesta de puntos finales (EDR)** en todos los activos para garantizar que sólo se puede ejecutar el software autorizado y que se bloquea todo el software no autorizado.
    - Para Windows, active Windows Defender Application Control (WDAC), AppLocker o ambos en todos los sistemas que admitan estas funciones.
        - WDAC está en continuo desarrollo, mientras que AppLocker sólo recibirá correcciones de seguridad. AppLocker se puede utilizar como complemento de WDAC, cuando WDAC se establece en el nivel más restrictivo posible, y AppLocker se utiliza para ajustar las restricciones para su organización.
    - Utilice listas de permisos en lugar de intentar enumerar y denegar todas las posibles permutaciones de aplicaciones en un entorno de red.
    - Considere la posibilidad de implantar EDR para los recursos basados en la nube.
- **Considere la posibilidad de implantar un sistema de detección de intrusiones (IDS)** para detectar la actividad de mando y control y otras actividades de red potencialmente maliciosas que se producen antes de la implantación del ransomware.
    - Asegurarse de que el IDS se supervisa y gestiona de forma centralizada. Configure correctamente las herramientas y dirija las advertencias y los indicadores al personal adecuado para que tome las medidas oportunas.
- **Supervise los indicadores de actividad y bloquee la creación de archivos maliciosos con la utilidad Sysmon de Windows**. A partir de Sysmon 14, la opción `FileBlockExecutable` puede utilizarse para bloquear la creación de ejecutables maliciosos, archivos de biblioteca de

vínculos dinámicos (DLL) y archivos de sistema que coincidan con valores hash específicos.

Vector de acceso inicial: Formas avanzadas de ingeniería social

- **Crear políticas que incluyan formación sobre ciberseguridad** sobre formas avanzadas de ingeniería social para el personal que tiene acceso a su red. La formación debe incluir consejos sobre cómo reconocer sitios web y resultados de búsqueda ilegítimos. También es importante repetir periódicamente la formación de concienciación sobre seguridad para mantener a su personal informado y alerta.
- **Implantar un Sistema de Nombres de Dominio (DNS) protector.** Al bloquear la actividad maliciosa de Internet en su origen, los servicios de DNS de protección pueden proporcionar un alto rendimiento de la red.
  seguridad para trabajadores remotos. Estos servicios de seguridad analizan las consultas DNS y toman medidas para mitigar amenazas -como malware, ransomware, ataques de phishing, virus, sitios maliciosos y spyware- aprovechando el protocolo y la arquitectura DNS existentes. Las SLTT pueden implantar el servicio MDBR sin coste alguno.
  Véase NSA's y CISA's Selecting a Protective DNS Service.
- **Considere la posibilidad de implantar navegadores aislados** para proteger los sistemas de programas maliciosos procedentes de la navegación web. Los navegadores aislados aíslan la máquina del código malicioso.

Entre las formas avanzadas de ingeniería social se incluyen:

- Envenenamiento por optimización de motores de búsqueda (SEO), también conocido como envenenamiento de búsqueda: cuando actores maliciosos crean sitios web maliciosos y utilizan tácticas de SEO para que aparezcan de forma destacada en los resultados de búsqueda. El envenenamiento SEO secuestra los resultados de los motores de búsqueda de sitios web populares e inyecta enlaces maliciosos para impulsar su posicionamiento en los resultados de búsqueda. Estos enlaces conducen a los usuarios desprevenidos a sitios de phishing, descargas de malware y otras ciberamenazas.
- Drive-by-downloads (sitios web impostores): cuando un usuario descarga involuntariamente código malicioso al visitar un sitio web aparentemente legítimo que es malicioso. Los actores maliciosos utilizan las descargas no autorizadas para robar y recopilar información personal, inyectar troyanos o introducir kits de exploits u otros programas maliciosos en los puntos finales. Los usuarios pueden visitar estos sitios respondiendo a un correo electrónico de phishing o haciendo clic en una ventana emergente engañosa.
- "Malvertising": publicidad maliciosa que los

Vector de acceso inicial: Terceros y proveedores de servicios gestionados

- **Considerar las prácticas de gestión de riesgos e higiene cibernética de terceros o servicios gestionados. (MSP)** 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 clientes [CPG 1.I].
    - Si un tercero o MSP es responsable de mantener y proteger las copias de seguridad de su organización, asegúrese de que siguen las mejores prácticas aplicables descritas anteriormente.

    Utilice el lenguaje contractual para formalizar sus requisitos de seguridad como mejor práctica.

Los actores maliciosos pueden aprovecharse de las relaciones de confianza que su organización mantiene con terceros y MSP.

- Los actores maliciosos pueden atacar a los MSP con el objetivo de comprometer a las organizaciones clientes de los MSP; pueden utilizar las conexiones de red de los MSP y el acceso a las organizaciones clientes como vector clave para propagar malware y ransomware.
- Los actores maliciosos pueden suplantar la identidad de entidades con las que su organización mantiene una relación de confianza, o utilizar cuentas de correo electrónico

- **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 su función o responsabilidades.
- **Considere la posibilidad de crear políticas de control de servicios (SCP) para los recursos basados en la nube con el fin de impedir que los usuarios o las funciones, en toda la organización, puedan acceder a servicios específicos o tomar acciones específicas dentro de los servicios.** Por ejemplo, el SCP puede utilizarse para restringir a los usuarios la posibilidad de eliminar registros, actualizar configuraciones de nube privada virtual (VPC) y cambiar configuraciones de registro.

Buenas prácticas generales y orientaciones sobre refuerzo

- **Asegúrese de que su organización cuenta con un** enfoque **integral de gestión de activos** [CPG 1.A].
    - Comprenda y haga inventario de los activos informáticos de su organización, lógicos (por ejemplo, datos, software) y físicos (por ejemplo, hardware).
    - Saber qué datos o sistemas son los más críticos para la salud y la seguridad, la generación de ingresos u otros servicios críticos, y comprender cualquier problema asociado.

    interdependencias (por ejemplo, "la lista de sistemas 'A' utilizada para realizar 'X' se

Consejo: Para facilitar el seguimiento de los activos, utilice la hoja de cálculo de seguimiento de activos de hardware y software de MS-ISAC.

almacena en el activo crítico 'B'"). Esto ayudará a su organización a determinar las prioridades de restauración en caso de que se produzca un incidente. Aplique controles o salvaguardas de seguridad más exhaustivos a los activos críticos. Esto requiere la coordinación de toda la organización.

- Asegúrese de que almacena la documentación de sus activos informáticos de forma segura y conserve copias de seguridad offline y físicas in situ.

- **Aplicar el principio de mínimo privilegio a todos los sistemas y servicios** para que los usuarios sólo tengan el acceso que necesitan para realizar su trabajo [CPG 2.E]. Los actores maliciosos a menudo aprovechan las cuentas privilegiadas para ataques de ransomware en toda la red.
    - Restringir los permisos de los usuarios para instalar y ejecutar aplicaciones de software.
    - Restrinja los permisos de usuario/rol para acceder o modificar los recursos basados en la nube.
    - Limitar las acciones que pueden realizar determinados usuarios/roles sobre las claves gestionadas por los clientes.
    - Bloquee el acceso remoto a las cuentas locales utilizando la directiva de grupo para restringir el inicio de sesión en la red por parte de las cuentas locales. Para obtener orientación, consulte Bloqueo del uso remoto de cuentas locales e identificadores de seguridad de Microsoft.
    - Utilice Windows Defender Remote Credential Guard y el modo de administración restringida para las sesiones RDP.
    - Elimine las cuentas y grupos innecesarios y restrinja el acceso root.
    - Controlar y limitar la administración local.
    - Audite Active Directory (AD) en busca de privilegios excesivos en cuentas y pertenencias a grupos.
    - Utilice el grupo de usuarios protegidos de AD en los dominios de Windows para proteger aún más las cuentas de usuarios con privilegios frente a los ataques pass-the-hash.
    - Audite trimestralmente las cuentas de usuario y de administrador en busca de cuentas inactivas o no autorizadas. Dé prioridad a la revisión de las cuentas de supervisión y gestión remotas de acceso público, incluidas las auditorías de los accesos de terceros concedidos a los MSP.

- **Asegúrese de que todas las máquinas virtuales e hipervisores** están actualizados y reforzados. Las nuevas tácticas de ransomware tienen como objetivo los servidores VMWare ESXi, que permiten cifrar rápidamente la infraestructura a escala.
- **Aproveche las mejores prácticas y active la configuración de seguridad en asociación con entornos en la nube, como** Microsoft Office 365.
    - Revise el modelo de responsabilidad compartida para la nube y asegúrese de que comprende en qué consiste la responsabilidad del cliente cuando se trata de la protección de activos.
    - Realice copias de seguridad de los datos con frecuencia; sin conexión o aproveche las copias de seguridad de nube a nube.
    - Active el registro de todos los recursos y establezca alertas para usos anormales.
    - Active la protección contra borrado o el bloqueo de objetos en los recursos de almacenamiento que suelen ser objetivo de ataques de ransomware (por ejemplo, almacenamiento de objetos, almacenamiento de bases de datos, almacenamiento de archivos y almacenamiento de bloques) para evitar que los datos se borren o sobrescriban, respectivamente.
    - Considere la posibilidad de activar el control de versiones para mantener almacenadas múltiples variantes de los objetos. Esto permite una recuperación más sencilla de acciones no intencionadas o malintencionadas.

- Cuando se admita, 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 protegerse contra otros ataques, como los ataques de repetición.
- Para obtener más información, consulte CISA Cybersecurity Advisory Microsoft Office 365 Security Recommendations.

- **Mitigar el uso malintencionado del** software de **acceso remoto y de supervisión y gestión remotas (RMM)**:
    - Audite las herramientas de acceso remoto de su red para identificar el software RMM actual o autorizado.
    - Revise los registros de ejecución del software RMM para detectar usos anómalos, o software RMM ejecutándose como un ejecutable portátil.
    - Utilice software de seguridad para detectar casos en los que el software RMM sólo se carga en la memoria.
    - Exija que las soluciones RMM autorizadas sólo se utilicen desde dentro de su red a través de soluciones de acceso remoto aprobadas, como VPN o interfaces de escritorio virtual (VDI).
    - Bloquee las conexiones entrantes y salientes en los puertos y protocolos comunes de RMM en el perímetro de la red.
- **Emplear medios lógicos o físicos de segmentación de red implementando** ZTA y separando varias unidades de negocio o recursos departamentales de TI dentro de su organización y mantener la separación entre TI y 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 prevenir o limitar el movimiento lateral por parte de actores maliciosos. La segmentación de la red puede volverse ineficaz si se viola por error del usuario o por no adherirse a las políticas de la organización (por ejemplo, conectar medios de almacenamiento extraíbles u otros dispositivos a múltiples segmentos).
- **Elabore y actualice periódicamente diagramas de red exhaustivos que describan los sistemas y flujos de datos dentro de la red o redes de su organización** (véase la Figura 1) [CPG 2.P]. Esto es útil en estado estacionario y puede ayudar al personal de respuesta a incidentes a entender dónde centrar sus esfuerzos. Ver Figura 2 y Figura 3 para representaciones de una red plana (no segmentada) y de una red segmentada con las mejores prácticas.
    - El diagrama debe incluir representaciones de las principales redes, cualquier esquema específico de direccionamiento IP y la topología general de la red, incluidas las conexiones de red, las interdependencias y el acceso concedido a terceros, MSP y conexiones de nube desde puntos finales externos e internos.
    - Asegúrese de almacenar de forma segura la documentación de la red y conserve copias de seguridad offline y en papel in situ.

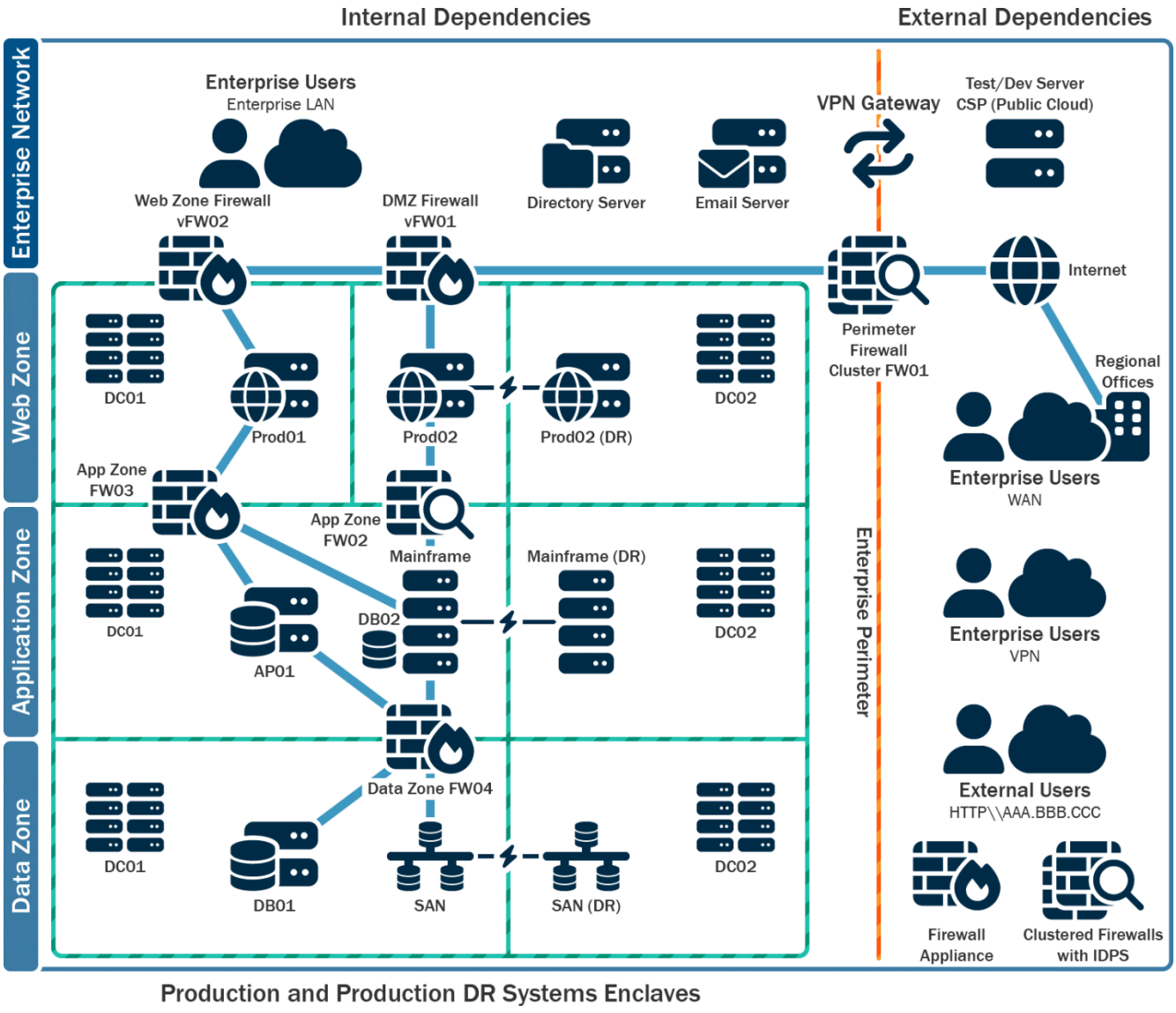

Figura 1: Ejemplo de diagrama de red

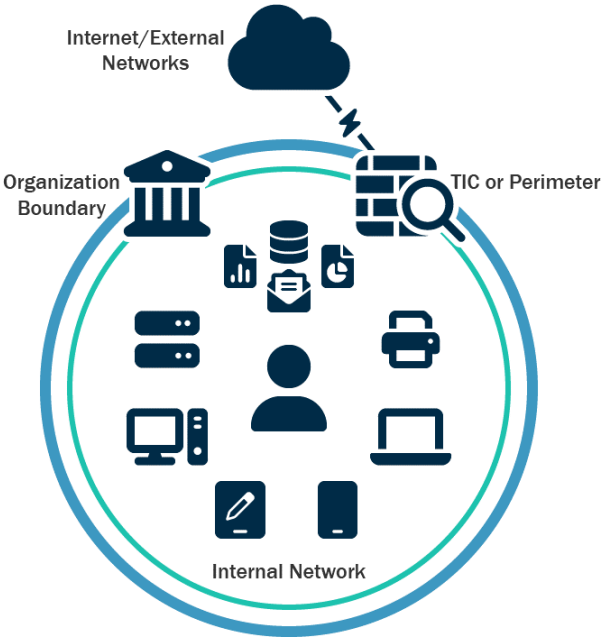

Figura 2: Red plana (no segmentada)

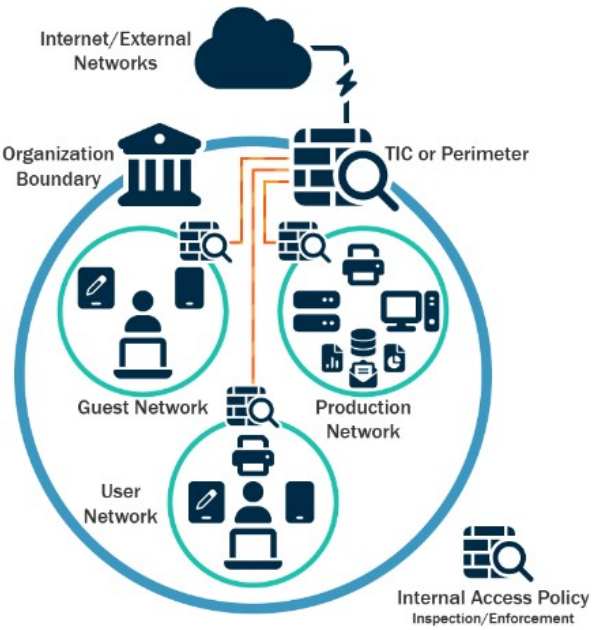

Figura 3: Red segmentada

- **Restrinja el uso de PowerShell a usuarios específicos caso por caso mediante la directiva de grupo**. Normalmente, sólo los usuarios o administradores que gestionan una red o un sistema operativo Windows pueden utilizar PowerShell. PowerShell es un lenguaje de línea de comandos, shell y scripting multiplataforma que forma parte de Microsoft Windows. Los actores de amenazas utilizan PowerShell para desplegar ransomware y ocultar sus actividades maliciosas. Para más información, consulte la hoja informativa conjunta sobre ciberseguridad Mantener PowerShell: Medida de seguridad para usar 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, utilizando la versión más reciente, tienen activados los registros de módulos, bloques de secuencias de comandos y transcripciones (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 de supervisión y respuesta a incidentes de la empresa.
        - Los registros de PowerShell contienen datos valiosos, incluida la interacción histórica con el sistema operativo y el registro, así como posibles tácticas, técnicas y procedimientos del uso de PowerShell por parte de un actor de amenazas.
        - Dos registros que registran la actividad de PowerShell son el registro "PowerShell Windows Event" y el registro "PowerShell Operational". 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 comprobarse periódicamente para confirmar si se han borrado los datos de registro o si se ha desactivado el registro. Establezca el

tamaño de almacenamiento permitido para ambos registros lo más grande posible.

- **Asegure los controladores de dominio (DC)**. Los actores maliciosos a menudo utilizan los DC como punto de partida para propagar el ransomware por toda la red. Para proteger los DC:
    - Utilice la última versión de Windows Server soportada por su organización en los DCs. Las versiones más recientes del sistema operativo Windows Server tienen integradas más funciones de seguridad, incluso para Active Directory. Para obtener orientación sobre la configuración de las funciones de seguridad disponibles, consulte Microsoft's Best Practices for Securing Active Directory.
        - Las organizaciones autoras recomiendan utilizar Windows Server 2019 o superior y Windows 10 o superior, ya que cuentan con funciones de seguridad, como las protecciones LSASS con Windows Credential Guard, Windows Defender y Antimalware Scan Interface (AMSI), no incluidas en el sistema operativo anterior
    - Asegúrese de que los centros de distribución reciben parches con regularidad. Aplique parches para vulnerabilidades críticas lo antes posible.
    - Utilice herramientas de pruebas de penetración de código abierto, como BloodHound, para verificar la seguridad del controlador de dominio.
    - Asegúrese de que se instala el mínimo software o agentes en los DC, ya que pueden aprovecharse para ejecutar código arbitrario en el sistema.
    - Restrinja el acceso a los DCs al grupo de Administradores. Los usuarios dentro de este grupo deben ser limitados y tener cuentas separadas utilizadas para operaciones diarias con permisos no administrativos. Para obtener más información, consulte Seguridad de las cuentas y grupos administrativos de Active Directory de Microsoft.
        - Las cuentas de administrador designadas sólo deben utilizarse con fines administrativos. Asegúrese de que en los DC no se revisen correos electrónicos, 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. Los servidores con conectividad a Internet pueden utilizarse para extraer las actualizaciones necesarias en lugar de permitir el acceso a Internet a los DC.
    - Implemente una solución de gestión de acceso privilegiado (PAM) en los DC para ayudar a gestionar y supervisar el acceso privilegiado. Las soluciones PAM también pueden registrar y alertar del uso para detectar actividades inusuales.
    - Considere desactivar 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 (por ejemplo, SAML, OIDC o Kerberos) para la autenticación con cifrado AES-256 bits. Si NTLM debe estar habilitado:
        - Active la Protección ampliada para autenticación (EPA) para evitar algunos ataques de retransmisión NTLM. Para obtener más información, consulte Microsoft Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS).

- Active la auditoría NTLM para garantizar que sólo se envían respuestas NTLMv2 a través de la red. Deben tomarse medidas para garantizar que se rechazan las respuestas LM y NTLM, si es posible.

- Habilite protecciones adicionales para la Autenticación LSA para prevenir la inyección de código capaz de adquirir credenciales del sistema. Antes de activar estas protecciones, ejecute auditorías para asegurarse de que conoce los programas que se verán afectados por la activación de esta protección.

- **Conserve y proteja adecuadamente los registros de dispositivos de red, hosts locales y servicios en la nube**. Esto apoya el triaje y la remediación de eventos de ciberseguridad. Los registros pueden ser analizados para determinar el impacto de los eventos y determinar si se ha producido un incidente [CPG 2.T].
  - Establecer una gestión centralizada de registros utilizando una herramienta de gestión de eventos e información de seguridad [CPG 2.U]. Esto permite a una organización correlacionar los registros de los dispositivos de seguridad de la red y del host. Al revisar los registros de múltiples fuentes, una organización puede clasificar un evento individual y determinar su impacto en la organización.
  - Mantenga y haga copias de seguridad de los registros de los sistemas críticos durante un mínimo de un año, si es posible.
- **Establezca una línea de base de seguridad del tráfico de red normal y ajuste los dispositivos de red para detectar comportamientos anómalos**. Ajuste los productos basados en host para detectar binarios anómalos, movimientos laterales y técnicas de persistencia.
  - Considere la posibilidad de utilizar el registro de transacciones empresariales -como el registro de la actividad relacionada con aplicaciones específicas o críticas- para el análisis del comportamiento.
- **Realizar evaluaciones periódicas** para garantizar que los procesos y procedimientos están actualizados y pueden ser seguidos por el personal de seguridad y los usuarios finales.

Parte 2: Lista de comprobación de la respuesta al ransomware y la 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 comprobación. Asegúrese de pasar por los **tres primeros pasos en secuencia.**

Detección y análisis

Consulte las mejores prácticas y referencias que figuran a continuación para ayudar a gestionar el riesgo que plantea el ransomware y apoyar la respuesta coordinada y eficaz de su organización ante un incidente de ransomware. Aplique estas prácticas en la mayor medida posible en

Las organizaciones autoras no recomiendan pagar rescates. Pagar el rescate no garantizará que sus datos se descifren, que sus sistemas o datos dejen de estar en peligro o 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, véase el memorando de la Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro de Estados Unidos de septiembre de 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. El aviso actualizado establece que la Oficina de Control de Activos Extranjeros del Tesoro (OFAC) consideraría "factores atenuantes" en las acciones de aplicación relacionadas. Póngase en contacto con su oficina

TLP:BORR

función de la disponibilidad de recursos de la organización.

- ☐ **1. Determinar qué sistemas se han visto afectados y aislarlos inmediatamente.**

  ellos.

  - ☐ Si varios sistemas o subredes

    Si la red se ve afectada, desconéctela a nivel de conmutador. Puede que no sea factible desconectar sistemas individuales durante un incidente.

- □ Dé prioridad al aislamiento de los sistemas críticos que son esenciales para las operaciones diarias.
- □ Si no es posible desconectar temporalmente la red de forma inmediata, localice el cable de red (por ejemplo, ethernet) y desconecte los dispositivos afectados de la red o retírelos de la Wi-Fi para contener la infección.
- □ En el caso de los recursos en la nube, realice una instantánea de los volúmenes para obtener una copia en un momento dado que pueda revisarse posteriormente para una investigación forense.
- □ Después de un compromiso inicial, los actores maliciosos pueden monitorear la actividad o las comunicaciones de su organización para entender si sus acciones han sido detectadas. Aísle los sistemas de forma coordinada y utilice métodos de comunicación fuera de banda, como llamadas telefónicas, para evitar que los agresores sepan que han sido descubiertos y que se están tomando medidas de mitigación. No hacerlo podría provocar que los actores se muevan lateralmente para preservar su acceso o desplieguen ransomware ampliamente antes de que las redes queden fuera de línea.

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

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

☐ **3. 3. Clasificación de los sistemas afectados para su restauración y recuperación.**

- □ Identifique y priorice los sistemas críticos 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 críticos que incluya los sistemas de información fundamentales para la salud y la seguridad, la generación de ingresos u otros servicios críticos, así como los sistemas de los que dependen.
- □ Lleve un registro de los sistemas y dispositivos que no se perciben como afectados, de modo que puedan ser despriorizados para su restauración y recuperación. De este modo, su empresa podrá retomar su actividad de forma más eficiente.

☐ **4. Examinar los sistemas de detección o prevención existentes en la organización (por ejemplo, antivirus, EDR, IDS, sistema de prevención de intrusiones) y los registros.** Esto puede poner de manifiesto la existencia de otros sistemas o programas maliciosos implicados en las primeras fases del ataque.

- □ Busque pruebas de malware precursor, como Bumblebee, Dridex, Emotet, QakBot o Anchor. Un evento de ransomware puede ser la prueba de un compromiso de red anterior no resuelto.
    - Los operadores de estas variantes avanzadas de malware suelen vender el

acceso a una red. En ocasiones, los actores maliciosos utilizan este acceso para filtrar datos y amenazan con hacerlos públicos antes de pedir un rescate por la red para extorsionar a la víctima y presionarla para que pague.

- Los ciberdelincuentes suelen soltar variantes de ransomware para ocultar la actividad posterior al ataque. Hay que tener cuidado de identificar este tipo de malware antes de reconstruir las copias de seguridad para evitar que continúen las amenazas.

☐ **5. Reúnase con su equipo para desarrollar y documentar una comprensión inicial de lo ocurrido basada en el análisis inicial.**

☐ **6. Iniciar actividades de caza de amenazas.**

☐ Para entornos empresariales, compruebe:

- Cuentas AD recién creadas o cuentas con privilegios escalados y actividad reciente relacionada con cuentas privilegiadas como Administradores de Dominio.
- inicios de sesión anómalos en dispositivos VPN u otros inicios de sesión sospechosos.
- Modificaciones en los puntos finales que puedan afectar a las copias de seguridad, las instantáneas, el registro en diario de los discos o las configuraciones de arranque. Busque el uso anómalo de 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 habitual del ransomware para impedir la recuperación del sistema.
- Indicios de la presencia de la baliza/cliente Cobalt Strike. Cobalt Strike es una suite de software comercial de pruebas de penetración. Los actores maliciosos suelen nombrar los procesos de Windows de Cobalt Strike con los mismos nombres que los procesos legítimos de Windows para ofuscar su presencia y complicar las investigaciones.
- Señales de cualquier uso inesperado de software de supervisión y gestión remota (RMM) (incluidos los ejecutables portátiles que no están instalados). Los actores maliciosos suelen utilizar el software RMM para mantener la persistencia.
- Cualquier ejecución inesperada de PowerShell o uso de PsTools suite.
- Signos de enumeración de credenciales AD y/o LSASS que se vuelcan (por ejemplo, Mimikatz o `NTDSutil.exe`).
- Señales de comunicaciones inesperadas de punto a punto (incluidos los servidores).
- Posibles indicios de filtración de datos de la red. Entre las herramientas comunes para la exfiltración de datos se incluyen Rclone, Rsync, varios servicios de almacenamiento de archivos basados en web (también utilizados por los actores de amenazas para implantar malware/herramientas en la red afectada) y FTP/SFTP.
- Servicios recién creados, tareas programadas inesperadas, software instalado inesperado, etc.

☐ Para entornos en nube:

- Habilite herramientas para detectar y evitar modificaciones en los recursos de IAM, seguridad de red y protección de datos.
- Utilice la automatización para detectar problemas comunes (por ejemplo, desactivación de funciones, introducción de nuevas reglas de cortafuegos) y

tome medidas automatizadas en cuanto se produzcan. Por ejemplo, si se crea una nueva regla de cortafuegos que permite el tráfico abierto (0.0.0.0/0), se puede realizar una acción automatizada para desactivar o eliminar esta regla y enviar notificaciones al usuario que la creó, así como al equipo de seguridad para que

concienciación. Esto ayudará a evitar la fatiga por alerta y permitirá al personal de seguridad centrarse en los problemas críticos.

Informes y notificaciones

Nota: consulte la sección Información de contacto al final de esta guía para obtener información detallada sobre cómo informar y notificar incidentes de ransomware.

- ☐ **7.** Siga los requisitos de notificación descritos en su plan de comunicación y respuesta a incidentes cibernéticos para **involucrar a los equipos internos y externos y a las partes interesadas** con una comprensión de lo que pueden proporcionar para ayudarle a mitigar, responder y recuperarse del incidente.
  - ☐ Comparta la información de que dispone para recibir asistencia oportuna y pertinente. Mantenga informados a la dirección y a los altos cargos mediante actualizaciones periódicas a medida que evolucione la situación. Las partes interesadas relevantes pueden incluir su departamento de TI, proveedores de servicios de seguridad gestionados, compañía de seguros cibernéticos y líderes departamentales o electos [CPG 4.A].
  - ☐ Notifique el incidente a la CISA, a la oficina local del FBI, al Centro de Denuncias de Delitos en Internet (IC3) del FBI o a su oficina local, y considere la posibilidad de solicitar ayuda.
    Oficina de campo del Servicio Secreto de EE.UU.
  - ☐ Según proceda, coordinarse con el personal de comunicación e información pública para garantizar que se comparte información precisa.

Si se necesita una identificación o análisis ampliado, CISA, MS- ISAC y las fuerzas de seguridad locales, estatales o federales pueden estar interesadas en cualquiera de los siguientes datos que su organización determine que puede compartir legalmente:

- Archivo ejecutable recuperado.
- Copias del archivo Léame - NO ELIMINE el archivo o puede que no sea posible el descifrado.
- Captura de memoria viva (RAM) de sistemas con signos adicionales de compromiso (uso de kits de herramientas de explotación, actividad RDP, archivos adicionales encontrados localmente).
- Imágenes de sistemas infectados con signos adicionales de compromiso (uso de kits de herramientas de explotación, actividad RDP, archivos adicionales encontrados localmente).
- Muestras de malware.
- Nombres de programas maliciosos identificados en su red.
- Muestras de archivos encriptados.
- Archivos de registro (por ejemplo, registros de eventos de Windows de sistemas comprometidos, registros de cortafuegos).
- Scripts PowerShell encontrados que se han ejecutado en la red.
- Cuentas de usuario creadas en AD o máquinas añadidas a la red durante la explotación.
- Direcciones de correo electrónico utilizadas por los atacantes y cualquier correo electrónico de phishing asociado.
- Otras cuentas de comunicación utilizadas por los atacantes.
- Una copia de la nota de rescate.
- Importe del rescate y si se pagó.
- Monederos Bitcoin utilizados por los atacantes.
- Monederos Bitcoin utilizados para pagar el rescate, si procede.
- Copias de cualquier comunicación con los atacantes.

internamente con su organización y externamente con el público.

☐ **8.** Si el incidente ha dado lugar a una violación de datos, **siga los requisitos de notificación establecidos en sus planes de comunicación y respuesta a incidentes cibernéticos.**

Contención y erradicación

Si no parece posible adoptar medidas iniciales de mitigación:

☐ **9. Tomar una imagen del sistema y una captura de memoria de una muestra de dispositivos afectados.**
(por ejemplo, estaciones de trabajo, servidores, servidores virtuales y servidores en la nube). Recopilar todos los registros pertinentes, así como muestras de cualquier binario de malware "precursor" y observables asociados o indicadores de compromiso.
(por ejemplo, direcciones IP sospechosas de comando y control, entradas de registro sospechosas u otros archivos relevantes detectados). Los contactos que se indican a continuación pueden ayudarle a realizar estas tareas.

- ☐ Preservar las pruebas de naturaleza muy volátil -o de conservación limitada- para evitar su pérdida o manipulación (por ejemplo, la memoria del sistema,
  Registros de seguridad de Windows, datos en búferes de registro de cortafuegos).

Previa solicitud voluntaria, CISA y MS-ISAC (para organizaciones SLTT) pueden ayudar con el análisis de correos electrónicos de phishing, medios de almacenamiento, registros y/o malware sin coste alguno para ayudar a las organizaciones a comprender la causa raíz de un incidente.

- CISA - Centro de Análisis Avanzado de Malware: malware.us-cert.gov/
- MS-ISAC - Plataforma de análisis de código malicioso (sólo organizaciones SLTT):

☐ **10. Consulte a las fuerzas de seguridad federales, incluso si es posible adoptar medidas paliativas, sobre los posibles descifradores disponibles,** ya que los investigadores de seguridad pueden haber descubierto fallos de cifrado para algunas variantes de ransomware y haber publicado herramientas de descifrado o de otro tipo.

Seguir tomando medidas para contener y mitigar el incidente:

☐ **11. Busque orientaciones fiables** (por ejemplo, publicadas por fuentes como el Gobierno de EE, MS-ISAC, o un proveedor de seguridad de confianza) para la variante concreta de ransomware y siga los pasos adicionales recomendados para identificar y contener los sistemas o redes que se haya confirmado que están afectados.

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

☐ **12. Identifique los sistemas y cuentas implicados en la violación inicial.** Esto puede incluir cuentas de correo electrónico.

☐ **13.** Sobre la base de los detalles de la violación o compromiso determinados anteriormente, **contener los sistemas asociados que puedan utilizarse para un acceso no autorizado posterior o continuado.** Las brechas a menudo implican la exfiltración masiva de credenciales. Proteger las redes y otras fuentes de información del acceso no autorizado continuado basado en credenciales puede incluir:

- □ Desactive las redes privadas virtuales, los servidores de acceso remoto, los recursos de inicio de sesión único y los activos basados en la nube u otros activos de cara al público.

☐ **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 Gestión de equipos > Sesiones y las listas de Archivos abiertos en los servidores asociados para determinar el usuario o 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 comprobar si hay conexiones de red RDP satisfactorias.
- □ Revise el registro de seguridad de Windows, los registros de eventos SMB y los registros relacionados que puedan identificar eventos significativos de autenticación o acceso.
- □ Ejecute un software de captura de paquetes, como Wireshark, en el servidor impactado con un filtro para identificar las direcciones IP implicadas en la escritura activa o el cambio de nombre de archivos (por ejemplo, smb2.filename contiene cryptxxx).

☐ **15. Realizar un análisis ampliado para identificar los mecanismos de persistencia "outside-in" y "inside-out".**

- □ La persistencia externa puede incluir el acceso autenticado a sistemas externos a través de cuentas fraudulentas, puertas traseras en sistemas perimetrales, explotación de vulnerabilidades externas, etc.
- □ La persistencia desde dentro hacia fuera puede incluir implantes de malware en la red interna o una variedad de modificaciones al estilo de vivir fuera de la red (por ejemplo, el uso de herramientas comerciales de pruebas de penetración como Cobalt Strike; el uso de la suite PsTools, incluido PsExec, para instalar y controlar malware de forma remota y recopilar información relativa a -o realizar la gestión remota de- sistemas Windows; el uso de scripts PowerShell).
- □ La identificación puede implicar el despliegue de soluciones EDR, auditorías de cuentas locales y de dominio, el examen 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. Reconstruir los sistemas basándose en la priorización de los servicios críticos** (por ejemplo, salud y seguridad o servicios generadores de ingresos), utilizando imágenes estándar preconfiguradas, si es posible. 17. Utilizar la infraestructura como plantillas de código para reconstruir los recursos en la nube.

☐ **17. Emitir restablecimientos de contraseñas para todos los sistemas afectados y abordar cualquier vulnerabilidad asociada y brecha en la seguridad o visibilidad** una vez que el entorno haya sido completamente limpiado y reconstruido, incluyendo cualquier cuenta

asociada impactada y la eliminación o remediación de mecanismos de persistencia maliciosos. Esto puede incluir la aplicación de parches, la actualización de software y la adopción de otras precauciones de seguridad no tomadas anteriormente. Actualice las claves de cifrado gestionadas por el cliente según sea necesario.

☐ **18. La autoridad de TI o de seguridad de TI designada declara el incidente de ransomware finalizado** en función de los criterios establecidos, que pueden incluir la adopción de las medidas anteriores o la búsqueda de ayuda externa**.**

Recuperación y actividad posterior al incidente

☐ **19. Reconectar los sistemas y restaurar los datos a partir de copias de seguridad encriptadas fuera de línea, basándose en una priorización de los servicios críticos.**

- ☐ 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) con fines de recuperación, asegúrese de que sólo se añaden sistemas limpios.

☐ **20. 20. Documentar las lecciones aprendidas del incidente y de las actividades de respuesta asociadas** para actualizar -y perfeccionar- las políticas, planes y procedimientos de la organización y orientar futuros ejercicios de los mismos.

☐ **21. Considere la posibilidad de compartir las lecciones aprendidas y los indicadores de compromiso relevantes con 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 actividades relacionadas.

Lo que puede esperar:

- Orientaciones específicas para ayudar a evaluar y remediar los incidentes de ransomware.
- Asistencia remota para identificar el alcance de la amenaza y recomendaciones sobre estrategias de contención y mitigación adecuadas (en función de la variante de ransomware específica).
- Análisis de correos electrónicos de phishing, 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 implicar la recopilación de artefactos del incidente, incluidas imágenes del sistema y muestras de malware.

Contactos de Federal Asset Response

A petición voluntaria, la respuesta de los activos federales incluye la prestación de asistencia técnica a las entidades afectadas para proteger sus activos, mitigar las vulnerabilidades y reducir los impactos de los incidentes cibernéticos; la identificación de otras entidades que puedan estar en riesgo y la evaluación de su riesgo a las mismas vulnerabilidades o similares; la evaluación de los riesgos potenciales para el sector o la región, incluidos los posibles efectos en cascada, y el desarrollo de cursos de acción para mitigar estos riesgos; facilitar el intercambio de información y la coordinación operativa con la respuesta a las amenazas; y proporcionar orientación sobre la mejor manera de utilizar los recursos y capacidades federales de manera oportuna y eficaz para acelerar la recuperación.

CISA:	cisa.gov/informe Central@cisa.gov o llame al (888) 282-0870 Asesor de Ciberseguridad (cisa.gov/cisa-regions): [Introduzca el número de teléfono y la dirección de correo electrónico de su CISA CSA local].
MS-ISAC:	Para los SLTT, envíe un correo electrónico a soc@msisac.org o llame al (866) 787-4722

Contactos federales de respuesta a amenazas

A petición voluntaria, o previa notificación a los socios, la respuesta federal a la amenaza incluye la realización de la actividad de investigación policial y de seguridad nacional apropiada en el lugar de la entidad afectada; la recogida de pruebas y la recopilación de inteligencia; la atribución; la vinculación de incidentes relacionados; la identificación de otras entidades afectadas; la identificación de oportunidades de persecución de la amenaza y de interrupción; el desarrollo y la ejecución de cursos de acción para mitigar la amenaza inmediata; y la facilitación del intercambio de información y la coordinación operativa con la respuesta de los activos.

FBI:	fbi.gov/contact-us/field-offices [Introduzca el número de teléfono y la dirección de correo electrónico de su oficina local del FBI].
USSS:	secretservice.gov/contact/field-offices/ [Introduzca el número de teléfono

y la dirección de correo electrónico de su oficina local del USSS].

Otros contactos federales de respuesta

NSA: DIB_Defense@cyber.nsa.gov (para Consultas sobre la Base Industrial de Defensa y Servicios de Ciberseguridad)

Otros contactos de respuesta

Considere rellenar la Tabla 1 para utilizarla en caso de que su organización se vea afectada por el ransomware. Considere la posibilidad de ponerse en contacto con estas organizaciones para obtener asistencia de mitigación y respuesta o para recibir una notificación.

Tabla 1: Información de los contactos de respuesta

Contactos de respuesta:		
Póngase en contacto con	**24x7 Información de contacto**	**Funciones y responsabilidades**
Equipo de seguridad TI/TI - Notificación centralizada de ciberincidentes		
Líderes departamentales o elegidos		
Fuerzas y cuerpos de seguridad estatales y locales		
Centro de Fusión		
Proveedores de servicios gestionados/de seguridad		
Ciberseguro		

RECURSOS

Recursos gratuitos CISA

- El intercambio de información con el CISA y el MS-ISAC (para organizaciones SLTT) es bidireccional. Esto incluye las mejores prácticas y la información de defensa de la red en relación con las tendencias y variantes del ransomware, así como el malware precursor del ransomware.
- Las evaluaciones técnicas u orientadas a las políticas ayudan a las organizaciones a comprender cómo pueden mejorar sus defensas para evitar la infección por ransomware: cisa.gov/cyber-resource-hub.
    - Las evaluaciones incluyen análisis de vulnerabilidades sin coste alguno.
- 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 CISA aconsejan sobre las mejores prácticas y le conectan con los recursos de CISA para gestionar el ciberriesgo.
- Cyber Security Evaluation Tool (CSET) guía a los propietarios y operadores de activos a través de un proceso sistemático de evaluación de la tecnología operativa (OT) y de TI. CSET incluye la Ransomware Readiness Assessment (RRA), una autoevaluación basada en un conjunto escalonado de prácticas para ayudar a las organizaciones a evaluar en qué medida están equipadas para defenderse y recuperarse de un incidente de ransomware.

Contactos:

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

Referencias rápidas sobre ransomware

- StopRansomware.gov: un sitio web gubernamental que ofrece recursos y alertas sobre ransomware.
- Security Primer - Ransomware (MS-ISAC)-describe campañas oportunistas y estratégicas de ransomware, vectores de infección comunes y recomendaciones de buenas prácticas.
- Institute for Security + Technology (IST) Blueprint for Ransomware Defense: un plan de acción para la mitigación, respuesta y recuperación del ransomware para pequeñas y medianas empresas.

Recursos adicionales

- Arquitectura de confianza cero del NIST
- CISA: Arquitectura Técnica de Referencia de Seguridad en la Nube
- CISA: Proyecto Aplicaciones Empresariales Seguras en la Nube (SCuBA)
- CISA: Guía de mitigación y refuerzo para MSP y pequeñas y medianas empresas
- CISA: Protección frente a las ciberamenazas para los proveedores de servicios gestionados y sus clientes
- NSA: Mitigación de vulnerabilidades en la nube (NSA)

DESCARGO DE RESPONSABILIDAD

La información y las opiniones contenidas en este documento se facilitan "tal cual" y sin garantías de ningún tipo. La referencia en este documento a cualquier producto, proceso o servicio comercial específico por su nombre comercial, marca registrada, fabricante u otro, no constituye ni implica su aprobación, recomendación o favorecimiento por parte del Gobierno de los Estados Unidos, y esta guía no se utilizará con fines publicitarios o de aprobación de productos.

PROPÓSITO

Este documento se ha elaborado en cumplimiento de las misiones de ciberseguridad de los autores, incluidas sus responsabilidades de identificar y difundir amenazas, y de desarrollar y publicar especificaciones y mitigaciones de ciberseguridad. Esta información puede compartirse ampliamente para llegar a todas las partes interesadas apropiadas.