NISTIR 8374

Gestión de riesgo de ransomware:

un perfil de marco de ciberseguridad

William C. Barker
William Fisher
Karen Scarfone
Murugiah Souppaya

Esta publicación está disponible sin costo en:
https://doi.org/10.6028/NIST.IR.8374.spa

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8374

Gestión de riesgo de ransomware:

un perfil de marco de ciberseguridad

William C. Barker
Dakota Consulting
Silver Spring, MD

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

William Fisher
División de Ciberseguridad Aplicada
Laboratorio de Tecnología Informática

Murugiah Souppaya
División de Seguridad Informática
Laboratorio de Tecnología Informática

Esta publicación está disponible sin costo en:
https://doi.org/10.6028/NIST.IR.8374.spa

Febrero 2022

Departamento de Comercio de los Estados Unidos de América
Gina M. Raimondo, secretaria

Instituto Nacional de Normas y Tecnología de los Estados Unidos
James K. Olthoff, en el ejercicio de las funciones y obligaciones no exclusivas del subsecretario de comercio para el Instituto Nacional de Normas y Tecnología y director del Instituto Nacional de Normas y Tecnología

Reporte Interno 8374 o Interagencia del Instituto Nacional de Normas y Tecnología
31 páginas (febrero 2022)

Esta publicación está disponible sin costo en:
https://doi.org/10.6028/NIST.IR.8374.spa

Envíe comentarios sobre esta publicación a: ransomware@nist.gov

Instituto Nacional de Normas y Tecnología de los Estados Unidos
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Disclaimer

Informes sobre tecnología de sistemas informáticos

El Laboratorio de Tecnología Informática (Information Technology Laboratory ITL) en el Instituto Nacional de Normas y Tecnología (NIST) promueve el bienestar público y económico de los Estados Unidos brindando liderazgo técnico para la infraestructura de medición y estándares de la nación. ITL desarrolla pruebas, métodos de pruebas, datos de referencia, implementación de prueba de conceptos y análisis técnico para avanzar el desarrollo y el uso productivo de la tecnología informática. Las responsabilidades de ITL incluyen el desarrollo de normas y pautas administrativas, técnicas, físicas y de gestión para la privacidad y seguridad costo-efectiva de información no relacionada con la seguridad nacional en los sistemas de información federales.

Resumen

El *ransomware* es un tipo de ataque malicioso donde los atacantes cifran los datos de una organización y exigen un pago para restablecer el acceso. Los atacantes también pueden robar la información de una organización y exigir un pago adicional para que no se divulgue la información a las autoridades, la competencia o al público. Este perfil de *ransomware* identifica los objetivos de seguridad del Marco de ciberseguridad versión 1.1 que apoyan la identificación, la protección, la detección, la respuesta y la recuperación de eventos de *ransomware.* El perfil puede usarse como una guía para la gestión de riesgos de eventos de *ransomware.* Esto incluye el apoyo para medir el nivel de preparación de una organización para contrarrestar amenazas de *ransomware* y para enfrentar las consecuencias potenciales de eventos.

Palabras clave

Marco de ciberseguridad, detectar, identificar, proteger, *ransomware*, recuperar, responder, riesgo, seguridad.

Reconocimientos

Los autores desean agradecer a todas las personas y organizaciones que contribuyeron a la creación de este documento.

Aviso de divulgación de patentes

AVISO: ITL ha solicitado que los titulares de reivindicaciones de patente cuyo uso pueda ser necesario para el cumplimiento de la orientación o los requisitos de esta publicación den a conocer dichas reivindicaciones de patente a ITL. Sin embargo, los titulares de patentes no están obligados a responder a las solicitudes de ITL de identificación de patentes, e ITL no ha llevado a cabo una búsqueda para identificar qué patentes, si las hubiere, pueden aplicarse a esta publicación.

A la fecha de publicación y subsiguientes solicitudes de identificación de reivindicaciones de patentes cuyo uso pueda requerirse para cumplimiento de las recomendaciones o requerimientos de esta publicación, no se ha identificado ninguna reivindicación de patente a ITL.

ITL no hace ninguna declaración explícita o tácita de que no se requieren licencias para evitar infringir patentes en el uso de esta publicación.

Tabla de contenido

1 Introducción

Este perfil de *ransomware* puede ayudar a las organizaciones y a las personas a gestionar el riesgo de eventos de *ransomware.* Esto incluye el apoyo para medir el nivel de preparación de una organización para contrarrestar amenazas de *ransomware* y para enfrentar las consecuencias potenciales de eventos. El perfil también puede utilizarse para identificar oportunidades para la mejora de la ciberseguridad para apoyar el bloqueo de *ransomware.* Este perfil mapea objetivos de seguridad desde el Marco para la mejora de la infraestructura crítica de ciberseguridad *(Framework for Improving Critical Infrastructure Cybersecurity)*, versión 1.1 [1] (también conocido como Marco de ciberseguridad de NIST) a las capacidades y medidas de seguridad que ayudan a identificar, proteger, detectar, responder y recuperarse de eventos de *ransomware*.

1.1 El desafío del *ransomware*

El ransomware es un tipo de *malware* que cifra los datos de una organización y exige pagos como condición para restablecer el acceso a esos datos. *El ransomware* también puede utilizarse para robar la información de una organización y exigir un pago adicional para no divulgar la información a las autoridades, la competencia o el público. Los ataques de *ransomware* son dirigidos a los datos o la infraestructura crítica de la organización, interrumpiendo o parando operaciones y presentan un dilema para la gerencia: pagar el rescate y esperar que los atacantes mantengan su palabra en cuanto a restablecer el acceso y no divulgar los datos o no pagar el rescate y ellos mismos intentar restablecer las operaciones. Los métodos que el *ransomware* utiliza para obtener acceso a los sistemas de información de una organización son comunes a los ciberataques de manera más amplia, pero están dirigidos a exigir que se pague un rescate. Las técnicas que se utilizan para promulgar el *ransomware* continuarán cambiando a medida que los atacantes busquen constantemente nuevas maneras de presionar a sus víctimas.

Los ataques de *ransomware* difieren de otros eventos de ciberseguridad en los que el acceso a la información como propiedad intelectual, datos de tarjetas de crédito o información de identificación personal puede obtenerse furtivamente y luego exfiltrarse con fines de monetización. En su lugar, el *ransomware* presenta una amenaza con un efecto inmediato sobre las operaciones empresariales. Durante un evento de *ransomware,* puede que las organizaciones tengan poco tiempo para mitigar o remediar el efecto, restablecer los sistemas o comunicarse a través de canales necesarios empresariales, de asociados o de relaciones públicas. Por este motivo, es especialmente crítico que las organizaciones estén preparadas. Esto incluye educar a los usuarios de cibersistemas, equipos de respuesta y tomadores de decisiones empresariales sobre la importancia de evitar y gestionar potenciales riesgos antes de que ocurran, y de los procesos y procedimientos para hacerlo.

Afortunadamente, las organizaciones pueden seguir pasos recomendados para prepararse y reducir la posibilidad de ataques de *ransomware* exitosos. Esto incluye lo siguiente: *identificar* y *proteger* datos, sistemas y dispositivos críticos; *detectar* eventos de *ransomware* tan pronto como sea posible (preferiblemente antes de que el *ransomware* sea distribuido); y prepararse para *responder* y *recuperarse* de cualquier evento de *ransomware* que sí ocurra. Hay muchos recursos disponibles para apoyar a las organizaciones en estos esfuerzos. Estos incluyen información del Instituto Nacional de Normas y Tecnología de los Estados Unidos (NIST), del

Buró Federal de Investigaciones (FBI), y del Departamento de Seguridad Nacional (DHS). Se enumeran recursos adicionales de NIST en el apéndice A de este documento.

Las medidas y capacidades de seguridad en la Tabla 1 de este perfil apoyan un abordaje detallado a la prevención y mitigación de eventos de *ransomware.* En el entendido de que llevar a cabo todas estas medidas puede estar fuera del alcance de algunos, el recuadro a continuación incluye pasos preventivos básicos que una organización puede llevar a cabo ahora para protegerse de la amenaza de *ransomware.* No todas estas medidas serán aplicables a las situaciones de todas las organizaciones. La orientación en este informe aborda las mejores prácticas más que un conjunto de requerimientos regulatorios o legales.

SUGERENCIAS BÁSICAS DE *RANSOMWARE*

Aún sin llevar a cabo todas las medidas descritas en este Perfil de ransomware, hay algunos pasos preventivos básicos que una organización puede llevar a cabo ahora para protegerse y recuperarse de la amenaza de ransomware. Estos incluyen:

1. **Educar a los empleados sobre cómo evitar infecciones de *ransomware.***
   - **No abrir archivos o hacer clic en enlaces de fuentes desconocidas** salvo que primero ejecute una verificación de antivirus o revise cuidadosamente los enlaces.
   - **Evitar usar sitios web personales y aplicaciones personales,** como correo electrónico, chat y medios sociales, desde los computadores del trabajo.
   - **No conectar dispositivos que son propiedad personal a las redes del trabajo sin previa autorización.**
2. **Evitar tener vulnerabilidades en sistemas que el *ransomware* pueda aprovechar.**
   - **Mantener los sistemas importantes completamente actualizados con parches.** Correr verificaciones programadas para identificar los parches disponibles e instalarlos tan pronto como sea posible.
   - **Emplear principios de cero confianza en todos los sistemas en red.** Administrar el acceso a todas las funciones de red y segmentar redes internas donde sea práctico para evitar que prolifere el *malware* entre sistemas que son objetivos potenciales.
   - **Permitir únicamente la instalación y ejecución de aplicaciones autorizadas.** Configurar los sistemas operativos y/o software de terceros para que sólo corran aplicaciones autorizadas. Esto también puede apoyarse en la adopción de una política de revisión, luego entonces agregando o eliminando aplicaciones autorizadas a una lista de aplicaciones permitidas.
   - **Informar a sus proveedores de tecnología sobre sus expectativas** (por ejemplo, en el texto de contratos) para que apliquen medidas que desincentiven ataques de *ransomware.*
3. **Rápidamente detectar y parar ataques e infecciones de *ransomware.***
   - **Utilizar software de detección de *malware* como software de antivirus en todo momento.** Configurarlo para que automáticamente escanee correos electrónicos y dispositivos removibles.

- **Monitorear continuamente** los servicios de directorio (y otras fuentes primarias de usuarios) en busca de indicadores de compromiso (IOC) o un ataque activo.
- **Bloquear el acceso a recursos no confiables de sitios web.** Utilizar productos o servicios que bloquean el acceso a nombres de servidores, direcciones IP o puertos y protocolos que se sabe que son maliciosos o se sospeche que son indicadores de actividad maliciosa de sistemas. Esto incluye utilizar productos y servicios que brinden protección de integridad para el componente de dominio de las direcciones (por ejemplo, hacker@poser.com).

4. **Hacer que sea más difícil que el *ransomware* se propague.**
   - **Utilizar cuentas de usuario estándar** con autenticación multifactorial en vez de cuentas con privilegios administrativos siempre que sea posible.
   - **Introducir retrasos de autenticación o configurar bloqueo de cuentas automático** como una defensa en contra de intentos automatizados para adivinar contraseñas.
   - **Asignar y gestionar la autorización de credenciales** para todos los activos y software empresariales y periódicamente verificar que cada cuenta solo tenga el acceso necesario siguiendo los principios del menor privilegio.
   - **Almacenar datos en un formato inmutable** (para que la base de datos no sobrescriba automáticamente datos más viejos cuando nuevos datos estén disponibles).
   - **Permitir el acceso externo a los recursos de redes internos únicamente vía conexiones seguras de red privada virtual (VPN).**
5. **Hacer que sea más sencillo recuperar información almacenada a partir de un evento de *ransomware* futuro.**
   - **Crear un plan de recuperación de incidentes.** Desarrollar, implementar y practicar regularmente un plan de recuperación de incidentes con roles y estrategias definidos para la toma de decisión. Esto puede ser parte de un plan de continuidad de operaciones. Este plan debe identificar servicios de misión crítica y otros servicios esenciales de la empresa para permitir la priorización de la recuperación y planes de continuidad del negocio para esos servicios críticos.
   - **Hacer respaldos de los datos, asegurar los respaldos y probar la restauración.** Planificar, implementar y probar cuidadosamente una estrategia de respaldo de datos y restauración —y asegurar y aislar respaldos de datos importantes.
   - **Mantener sus contactos.** Mantener una lista actualizada de contactos internos y externos para el caso de ataques de *ransomware,* incluyendo recursos de las fuerzas del orden, asesoría legal y respuesta a incidentes.

1.2 Audiencia

El Perfil de *ransomware* está dirigido a cualquier organización con recursos de ciberseguridad que pueda estar sujeta a ataques de *ransomware,* independientemente del sector o tamaño. Cualquier organización, incluyendo las pequeñas o medianas empresas (pymes), pequeñas agencias federales y otras organizaciones pequeñas y operadoras de sistemas de control

industriales (ICS) o tecnologías operativas (OT), puede aprovechar estas recomendaciones y también se le alienta a considerar revisar el Marco de ciberseguridad.

Muchas de estas acciones pueden llevarse a cabo sin gastos considerables de recursos. Pueden obtener un valor las organizaciones que:

- están familiarizadas con el Marco de ciberseguridad del NIST, y es posible que ya lo hayan adoptado, para ayudar a identificar, evaluar y administrar los riesgos de seguridad cibernética y desean mejorar sus posturas de riesgo al abordar las preocupaciones de *ransomware*, o
- no están familiarizadas con el Marco de ciberseguridad pero que desean implementar marcos de gestión de riesgos para enfrentar las amenazas de *ransomware*.

1.3 Recursos de orientación adicionales

Además de los recursos mencionados anteriormente en esta sección, el Centro Nacional de Excelencia de Ciberseguridad (NCCoE) de NIST ha producido recomendaciones para apoyar la mitigación de amenazas de *ransomware.* NIST tiene muchos otros recursos que, aunque no sean específicos para *ransomware,* contienen información valiosa sobre la identificación, la protección, la detección, la respuesta y la recuperación de eventos de *ransomware.* Vea la sección de Referencias para una lista de referencias y el apéndice A de este perfil para una lista más extensa de los recursos de NIST.

2 Perfil de *ransomware*

El Perfil de *ransomware* alinea los requerimientos, objetivos, apetito por el riesgo y recursos de prevención y mitigación de *ransomware* de las organizaciones con los elementos del Marco de ciberseguridad de NIST. Debería ayudar a las organizaciones a identificar y priorizar oportunidades para mejorar su seguridad y resiliencia de ataques de *ransomware.* Las organizaciones pueden usar este documento como una guía para establecer el perfil del estado de su propia preparación. Hacerlo los ayudará a determinar su "perfil" o estado actual y establecer un "perfil objetivo" para identificar brechas.

Tabla 1 define el Perfil de *ransomware*. Las primeras dos columnas enumeran categorías y subcategorías importantes del Marco de ciberseguridad que las organizaciones pueden usar como resultados objetivo para sus programas de gestión de riesgo de *ransomware.* La tercera columna explica brevemente cómo cada subcategoría ayuda a identificar, proteger, detectar, responder y recuperarse de eventos de *ransomware*.

Este perfil también cita "Referencias informativas". Estas son secciones específicas de estándares, pautas y prácticas comunes entre sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada subcategoría. Las Referencias informativas en el Marco de ciberseguridad son ilustrativas y no exhaustivas. Están basadas en las recomendaciones intersectoriales referenciadas más frecuentemente durante el proceso de desarrollo del marco.

Por ejemplo, la segunda columna de Tabla 1 cita requerimientos relevantes de dos de las referencias informativas incluidas en el Marco de ciberseguridad: Organización Internacional para la Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements [Tecnología informática —técnicas de seguridad— sistemas de gestión de seguridad informática —requerimientos]* [2] y NIST SP 800-53 Revisión 5, *Security and Privacy Controls for Information Systems and Organizations [Controles de seguridad y privacidad para sistemas informáticos y organizaciones]* [3].

El Marco de ciberseguridad enumera referencias informativas adicionales para cada subcategoría. Estas referencias serán actualizadas eventualmente en versiones en línea de este documento guía.

Las cinco funciones del Marco de ciberseguridad utilizadas para organizar las categorías son:

- **Identificar:** desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de sistemas, personas, activos, datos y capacidades. Las actividades en la función de identificar son fundamentales para el uso efectivo del marco. Comprender el contexto empresarial, los recursos que apoyan las funciones críticas y los riesgos de ciberseguridad relacionados permite a una organización enfocarse y priorizar sus esfuerzos, de acuerdo con su estrategia de gestión de riesgo y necesidades empresariales.

- **Proteger:** desarrollar e implementar protecciones apropiadas para garantizar la entrega de servicios críticos. La función de proteger apoya la capacidad de limitar o contener el efecto de un evento potencial de ciberseguridad.
- **Detectar:** desarrollar e implementar actividades apropiadas para identificar cuando ocurra un evento de ciberseguridad. La función de detectar permite el descubrimiento oportuno de eventos de ciberseguridad.
- **Responder:** desarrollar e implementar actividades apropiadas para tomar acción en relación con un incidente de ciberseguridad detectado. La función de responder apoya la capacidad de contener el efecto de un incidente potencial de ciberseguridad.
- **Recuperar:** desarrollar e implementar actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquiera capacidades o servicios que hayan sido afectados debido a un incidente de ciberseguridad. La función de recuperar apoya la recuperación oportuna hacia operaciones normales para reducir el efecto de un incidente de ciberseguridad.

Tabla 1: Perfil de gestión de riesgo de *ransomware*:

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Identificar		
Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, sistemas e instalaciones que permiten que la organización logre sus fines empresariales son identificados y gestionados de acuerdo con su relativa importancia a los objetivos organizacionales y a la estrategia de riesgo de la organización.	**ID.AM-1:** se hace el inventario de los sistemas y dispositivos físicos dentro de la organización **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 5** CM-8, PM-5	Un inventario de dispositivos físicos debe llevarse a cabo, revisarse y mantenerse para asegurar que estos dispositivos no son vulnerables a *ransomware.* También es beneficioso tener un inventario de hardware durante las fases de recuperación después de un ataque de *ransomware,* en caso de que sea necesaria una reinstalación de aplicaciones.
	ID.AM-2: se hace inventario de las aplicaciones y plataformas de software **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 5** CM-8, PM-5	Los inventarios de software pueden hacer seguimiento de información como el nombre y la versión del software, los dispositivos en donde está instalado actualmente, última fecha de actualización de los parches instalados y vulnerabilidades conocidas actualmente. Esta información apoya la remediación de vulnerabilidades que pueden aprovecharse en ataques de *ransomware.*

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	ID.AM-3: se mapean los flujos de datos y la comunicación organizacional **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 5** AC-4, CA-3, CA-9, PL-8	Esto ayuda a enumerar qué información o procesos están en riesgo, en caso de que los atacantes se muevan lateralmente dentro de un entorno.
	ID.AM-4: se catalogan los sistemas de información externos **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 5** AC-20, SA-9	Esto es importante para la planificación de comunicaciones a asociados y acciones posibles para desconectarse temporalmente de sistemas externos en respuesta a eventos de *ransomware.* Identificar estas conexiones también ayudará a las organizaciones a planificar la implementación de controles de seguridad e identificar áreas donde los controles puedan compartirse con terceros.
	ID.AM-5: se priorizan recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) con base en su clasificación, criticidad y valor comercial **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 5** CP-2, RA-2, RA-9, SC-6	Esto es esencial para comprender el verdadero alcance y efecto de los eventos de ransomware —y es importante en la planificación de contingencias para futuros eventos de *ransomware*, respuestas a emergencias y acciones de recuperación. Ayuda a los que responden a incidentes y operaciones a priorizar recursos y apoya la planificación de contingencia para futuros eventos de *ransomware,* respuesta a emergencias y acciones de recuperación. Si hay un sistema de control industrial asociado (ICS), sus funciones críticas deben incluirse en la respuesta a emergencias y las acciones de recuperación.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	ID.AM-6: se establecen los roles y responsabilidades de ciberseguridad para la fuerza laboral completa y las partes interesadas de terceros (por ejemplo, proveedores, clientes, asociados) **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 5** CP-2, PM-11, PS-7	Es importante que todos en la organización comprendan sus roles y responsabilidades para la prevención de eventos de *ransomware* y, si corresponde, para responder y recuperarse de eventos de *ransomware.* Estos roles y responsabilidades deben documentarse formalmente en un plan de respuesta a incidentes. El plan de respuesta a incidentes debe especificar prácticas regulares del plan (por ejemplo, al menos anualmente llevar a cabo simulaciones de mesa de respuesta incidentes).
Entorno empresarial (ID.BE): se revisan y priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza como información para las decisiones de gestión de riesgo, los roles y las responsabilidades de ciberseguridad.	**ID.BE-2:** se identifica y comunica el lugar que ocupa la organización en lo que respecta a infraestructura crítica y su sector industrial **ISO/IEC 27001:2013** Cláusula 4.1 **NIST SP 800-53 Rev. 5** PM-8	Esto permite a los equipos de respuesta a incidentes de seguridad informática comprender mejor el lugar que ocupa la organización objetivo en el entorno de infraestructura crítica y les permite reaccionar de manera oportuna en el caso de efectos intersectoriales. También alienta a la organización y a sus partes interesadas externas a considerar los efectos aguas abajo del ataque de *ransomware.*
	ID.BE-3: se establecen y comunican las prioridades para la misión, los objetivos y las actividades organizacionales **NIST SP 800-53 Rev. 5** PM-11, SA-14	Esto ayuda a los que responden a incidentes y operaciones a priorizar recursos. Apoya la planificación de contingencia para futuros eventos de *ransomware,* respuesta a emergencias y acciones de recuperación.
	ID.BE-4: se establecen las funciones críticas y las dependencias para la entrega de servicios críticos **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 5** CP-8, PE-9, PE-11, PM-8, SA-20	Esto ayuda a identificar componentes críticos secundarios y terciarios en el apoyo de las funciones empresariales principales de la organización. Es necesario para priorizar planes de contingencia para eventos y respuestas de emergencia futuros para los eventos de *ransomware.* Si hay un ICS asociado, sus funciones críticas deben incluirse en las acciones de recuperación y respuesta a emergencias.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Gobernanza (ID.GV): se comprenden las políticas, procedimientos y procesos para gestionar y monitorear los requerimientos regulatorios, legales, de riesgo, ambientales y operativos y se utilizan como información para la gestión de riesgo de ciberseguridad.	**ID.GV-1:** se establece y comunica la política organizacional de ciberseguridad **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 5** AC-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, PE-01, PL-01, PM-01, RA-01, SA-01, SC-01, SI-01	Establecer y comunicar políticas necesarias para evitar o mitigar eventos de *ransomware* es esencial y fundamental para todas las otras actividades de prevención y mitigación. Donde sea práctico, estas políticas deben revisarse periódicamente para reflejar la naturaleza dinámica del riesgo y la realidad de los ajustes continuos necesarios.
	ID.GV-3: se comprenden y gestionan los requerimientos regulatorios y legales relacionados con la ciberseguridad, incluyendo obligaciones de libertades civiles y privacidad **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 5** CA-07, RA-02	Esto es necesario para desarrollar políticas de ciberseguridad y establecer prioridades en la planificación de contingencias para la respuesta a eventos de *ransomware* futuros.
	ID.GV-4: los procesos de gobernanza y gestión de riesgos abordan los riesgos de ciberseguridad **ISO/IEC 27001:2013** Cláusula 6 **NIST SP 800-53 Rev. 5** PM-3, PM-7, PM-9, PM-10, PM-11, SA-2	Los riesgos de *ransomware* deben tomarse en cuenta en la gobernanza de la gestión de riesgo organizacional con el fin de establecer políticas de ciberseguridad adecuadas.
Evaluación de riesgos (ID.RA): la organización comprende el riesgo de la ciberseguridad para las operaciones organizacionales (incluyendo la misión, las funciones, la imagen o reputación) y las personas.	**ID.RA-1:** se identifican y documentan las vulnerabilidades de activos **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	Identificar y documentar las vulnerabilidades de los activos de la organización es crucial en el desarrollo de planes para las vulnerabilidades y para priorizar la mitigación o eliminación de esas vulnerabilidades. Estas acciones también son clave para la planificación de contingencias para la evaluación y respuesta a eventos de *ransomware* futuros y reducirá la probabilidad de un ataque de *ransomware* exitoso.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	ID.RA-2: se recibe información de amenazas cibernética desde foros y fuentes de intercambio de información **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 5** PM-15, PM-16, SI-5	Recibir y utilizar información de amenazas cibernéticas proveniente de fuentes de intercambio de información puede reducir la exposición a ataques de *ransomware* y facilitar la detección temprana de nuevas amenazas.
	ID.RA-4: se identifican las probabilidades y efectos potenciales sobre el negocio **ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2 **NIST SP 800-53 Rev. 5** PM-9, PM-11, RA-2, RA-3, SA-20	Comprender los efectos potenciales de eventos de *ransomware* en el negocio es necesario para apoyar el análisis de costo-beneficio de la ciberseguridad así como para establecer prioridades de las actividades en los planes de respuesta y recuperación de *ransomware.* Comprender los efectos potenciales en el negocio también apoya las decisiones de respuesta a emergencias en el caso de un ataque de *ransomware.*
	ID.RA-6: las respuestas a riesgos son identificadas y priorizadas **ISO/IEC 27001:2013** Cláusula 6.1.3 **NIST SP 800-53 Rev. 5** PM-4, PM-9	Los gastos asociados con la respuesta y la recuperación de eventos de *ransomware* están directamente afectados por la efectividad de la planificación de contingencias para las respuestas a los riesgos.
Estrategia de gestión de riesgo (ID.RM): se establecen las prioridades, restricciones, tolerancias a riesgo y suposiciones y se utilizan para apoyar las decisiones de riesgos operativos.	**ID.RM-1:** las partes interesadas organizacionales establecen, gestionan y acuerdan los procesos de gestión de riesgo **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 5** PM-4, PM-9	Establecer y hacer cumplir las políticas, los roles y las responsabilidades organizacionales depende de que las partes interesadas acuerden e implementen procesos de gestión de riesgo efectivos. Los procesos deben tomar en cuenta el riesgo de un evento de *ransomware.* Debe revisarse periódicamente que estas políticas reflejen la naturaleza dinámica del riesgo y la realidad de ajustes necesarios en el tiempo.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Gestión de riesgo de la cadena de suministro (ID.SC): se establecen las prioridades, restricciones, tolerancias a riesgo y suposiciones y se utilizan para apoyar las decisiones de riesgos asociados con la gestión de riesgo de la cadena de suministros. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministros.	**ID.SC-5:** se llevan a cabo la planificación y prueba de respuestas y recuperación con los proveedores y terceros proveedores. **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 5** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9	La planificación de contingencia de *ransomware* debe coordinarse con los proveedores y terceros proveedores y debe incluir pruebas de las actividades planificadas. El plan debe incluir un escenario en el que la organización, sus proveedores y terceros proveedores son todos afectados por el *ransomware.*

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Proteger		
Gestión de identidad, autenticación y control de acceso (PR.AC): el acceso a los activos físicos y lógicos e instalaciones asociadas es limitado a los usuarios, procesos y dispositivos autorizados y se gestiona de acorde a la evaluación de riesgo de un acceso no autorizado a las actividades y transacciones autorizadas.	**PR.AC-1:** se emiten, gestionan, verifican, revocan y auditan identidades y credenciales para dispositivos, usuarios y procesos autorizados **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 5** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	La mayoría de los ataques de *ransomware* se llevan a cabo a través de conexiones de red y los ataques de *ransomware* frecuentemente comienzan con credenciales comprometidas (por ejemplo, captura o intercambio no autorizado de contraseñas y credenciales de inicio de sesión). La gestión de credenciales es esencial, aunque no es la única mitigación necesaria.
	PR.AC-3: se gestiona el acceso remoto **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, SC-15	La mayoría de los ataques de *ransomware* se llevan a cabo remotamente. La gestión de privilegios asociados con el acceso remoto puede ayudar a mantener la integridad de los sistemas y los archivos de datos para proteger de la inserción de código malicioso y la exfiltración de datos. El uso de la autenticación multifactorial es una manera clave —de fácil implementación— para reducir la probabilidad de que una cuenta se vea comprometida.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	PR.AC-4: se gestionan los permisos y autorizaciones de acceso, incorporando los principios de menor privilegio y separación de obligaciones **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	Muchos eventos de *ransomware* ocurren al comprometer las credenciales de usuarios o invocar procesos que tienen acceso privilegiado innecesario a los sistemas. Este es un paso muy importante de gestión para prevenir estos eventos.
	PR.AC-5: se protege la integridad de la red (por ejemplo, segregación de redes, segmentación de redes) **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 5** AC-4, AC-10, SC-7	La segregación o segmentación de redes puede limitar el alcance de los eventos de *ransomware* al evitar que el *malware* prolifere entre los potenciales sistemas objetivo (por ejemplo, pasar de un sistema de control o tecnología operativa (OT) desde una red de tecnología informática (IT) empresarial). Es crítico separar las redes de IT y OT y validar regularmente su independencia. Esto no sólo reduce el riesgo de que los sistemas de OT se vean comprometidos, sino también permite que las operaciones críticas de bajo nivel continúen mientras los sistemas de IT del negocio se recuperan del *ransomware.* Esto es particularmente importante para las funciones críticas ICS, incluyendo los Sistemas Instrumentados de Seguridad (SIS).
	PR.AC-6: se validan las identidades y se vinculan a credenciales y se reconfirman a través de interacciones **ISO/IEC 27001:2013** A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	Las credenciales comprometidas son vectores de ataque habituales en eventos de *ransomware.* Las identidades deben validarse y luego vincularse a una credencial (por ejemplo, la autenticación de dos factores de personas autorizadas formalmente) para limitar la probabilidad de que las credenciales sean comprometidas o emitidas a una persona no autorizada.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Concientización y capacitación (PR.AT): se brinda capacitación de concientización sobre ciberseguridad al personal y asociados de la organización y se les capacita para llevar a cabo sus obligaciones y responsabilidades relacionadas con la ciberseguridad de acuerdo con las políticas, los procedimientos y los acuerdos relacionados.	**PR.AT-1:** se capacita e informa a todos los usuarios **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 5** AT-2, PM-13	La mayoría de los ataques de *ransomware* son posibles debido a que hay usuarios que utilizan prácticas inseguras, administradores que implementan configuraciones inseguras o desarrolladores que no tienen la suficiente capacitación en seguridad.
Seguridad de los datos (PR.DS) Se gestionan la información y los registros (datos) de acuerdo con la estrategia de riesgo de la organización para proteger la confidencialidad, la integridad y la disponibilidad de la información.	**PR.DS-4:** se mantiene la capacidad adecuada para garantizar la disponibilidad **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 5** AU-4, CP-2, SC-5	Garantizar la disponibilidad adecuada de datos puede reducir los efectos del *ransomware.* Esto incluye la capacidad de mantener respaldos de datos fuera del sitio y fuera de línea, probar tiempos promedios de recuperación y redundancia de sistemas donde sea necesario.
	PR.DS-5: se implementan protecciones para evitar fugas de datos **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 5** AU-4, CP-2, SC-5	La extorsión doble —exigir pago tanto para recuperar el acceso a datos como para no vender o publicar los datos en otro sitio— es habitual, así que las soluciones de prevención de fuga de información son importantes.
	PR.DS-6: se utilizan mecanismos de verificación de integridad para verificar la integridad de la información, el software y el firmware **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 5** SC-16, SI-7	Los mecanismos de verificación de integridad pueden detectar actualizaciones de software alteradas que pueden utilizarse para introducir un *malware* que permita eventos de *ransomware.*
	PR.DS-7: el (los) entorno(s) de desarrollo y pruebas están separados del entorno de producción **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 5** CM-2	Mantener los entornos de desarrollo y pruebas separados de los entornos de producción puede evitar que el *ransomware* circule de los sistemas de desarrollo y pruebas a los sistemas de producción.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Procedimientos y procesos de protección de la información (PR.IP): se mantienen las políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso gerencial y la coordinación entre entidades organizacionales), los procesos y los procedimientos y se utilizan para gestionar la protección de activos y sistemas informáticos.	**PR.IP-1:** se crea y mantiene una configuración de sistemas de control industriales/tecnología informática como base de referencia incorporando principios de seguridad (por ejemplo, concepto de la menor funcionalidad) **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 5** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	Las bases de referencia son útiles para establecer el conjunto de funciones que un sistema necesita llevar a cabo para que pueda evaluarse cualquier desviación con respecto a esa base de referencia en lo relativo a su riesgo cibernético potencial. Los cambios a la configuración no autorizados pueden usarse como un indicador de un ataque malicioso, que puede conducir a la introducción de *ransomware.*
	PR.IP-3: los procesos de control de cambios de configuración están implementados **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 5** CM-3, CM-4, SA-10	Los procesos adecuados de control de cambios de configuración pueden ayudar en el cumplimiento de actualizaciones de seguridad oportunas de software, a mantener los valores de configuración de seguridad necesarios y desalentar el reemplazo de código con productos que contengan un *malware* o que no cumplan las políticas de gestión de acceso.
	PR.IP-4: se llevan a cabo, mantienen y prueban respaldos de información **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 5** CP-4, CP-6, CP-9	Los respaldos regulares que son mantenidos y probados son esenciales para la recuperación oportuna y relativamente sin complicaciones de los eventos de *ransomware.* Los respaldos deben mantenerse seguros para garantizar que el *ransomware* no los corrompa o que el atacante no los elimine. Los respaldos deben almacenarse fuera de línea.
	PR.IP-9: los planes de respuesta (respuesta a incidentes y continuidad del negocio) y planes de recuperación (recuperación de incidentes y recuperación de desastres) están implementados y gestionados **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 5** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	Los planes de respuesta y recuperación deben incluir eventos de *ransomware.* Una copia del plan de respuesta debe mantenerse fuera de línea para el caso en que el incidente elimine el acceso a copias digitales almacenadas en la red afectada. Los eventos de *ransomware* deben priorizarse apropiadamente durante el triaje de incidentes con el objetivo de contención inmediata para prevenir la propagación del *ransomware.*

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	PR.IP-10: se prueban los planes de respuesta y recuperación **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 5** CP-4, IR-3, PM-14	Los planes de recuperación y respuesta de *ransomware* deben probarse periódicamente para garantizar que los supuestos y procesos de riesgos y respuestas están actualizados en relación con las amenazas de *ransomware* que evolucionan. Las pruebas de planes de respuesta y recuperación deben incluir cualquier ICS asociado. Los procesos deben actualizarse y mantenerse para que correspondan con las necesidades y estructuras organizacionales cambiantes así como con los nuevos tipos y tácticas de *ransomware.* Las pruebas sirven de capacitación para las personas que deberán ejecutar el plan.
Mantenimiento (PR.MA): el mantenimiento y la reparación de componentes de sistemas informáticos y de control industrial se realizan de manera consistente con las políticas y los procedimientos.	**PR.MA-2:** el mantenimiento remoto de los activos organizacionales está aprobado, se lleva un registro y se realiza de forma que evita el acceso no autorizado **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 5** MA-4	El mantenimiento remoto brinda un canal de acceso a las redes y la tecnología. Si no se administra apropiadamente, los delincuentes pueden utilizar este acceso para modificar configuraciones para permitir el ingreso de *malware.* El mantenimiento remoto de todos los componentes de los sistemas hecho por la organización o sus proveedores debe validarse para garantizar que este proceso no proporciona un acceso por la puerta trasera a las redes de OT o IT.
Tecnología de protección (PR.PT): las soluciones de seguridad técnicas se administran para garantizar la seguridad y la resiliencia de los sistemas y activos, de acuerdo con las políticas, los procedimientos y los acuerdos relacionados.	**PR.PT-1:** se determinan, implementan y revisan los registros de auditoría/archivos (log) de acuerdo con las políticas **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 5** AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-12, AU-13, AU-14, AU-16	La disponibilidad de registros de archivos (log)/auditoría puede apoyar la detección de comportamientos inesperados y apoyar los procesos de recuperación y respuesta forense.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	PR.PT-3: el principio de la menor funcionalidad es incorporado configurando los sistemas para proporcionar solo capacidades esenciales. **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 5** AC-3, CM-7	Mantener el principio de la menor funcionalidad puede evitar la migración entre potenciales sistemas objetivo (por ejemplo, la migración a un sistema de control de procesos operativo desde una red administrativa).
Detectar		
Eventos y anomalías (DE.AE): se detecta actividad anómala y se comprende el efecto potencial de los eventos.	**DE.AE-3:** se recolectan los datos de los eventos y se correlacionan con múltiples fuentes y sensores **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	Múltiples fuentes y sensores junto con una solución de seguridad de información y gestión de eventos (SIEM) mejora la visibilidad de la red, apoya la detección temprana de *ransomware,* y ayuda en la comprensión de cómo el *ransomware* puede propagarse a través de una red.
	DE.AE-4: se determina el efecto de los eventos **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3, SI-4	Determinar el efecto de los eventos puede suministrar información para las prioridades de respuesta y recuperación de un ataque de *ransomware.*
Monitoreo continuo de la seguridad (DE.CM): se monitorean los sistemas de información y activos para identificar los eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	**DE.CM-1:** se monitorea la red para detectar potenciales eventos de ciberseguridad. **NIST SP 800-53 Rev. 5** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	El monitoreo de la red podría detectar intrusiones e iniciar acciones de protección antes de que el código malicioso pueda introducirse o de que grandes volúmenes de información sean cifrados y exfiltrados.
	DE.CM-3: se monitorea la actividad del personal para detectar potenciales eventos de ciberseguridad **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 5** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	El monitoreo de la actividad del personal podría detectar amenazas internas o prácticas inseguras realizadas por el personal o credenciales comprometidas y frustrar potenciales eventos de *ransomware.*

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	DE.CM-4: se detecta código malicioso **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 5** SI-3, SI-8	La detección puede indicar que un evento de *ransomware* está ocurriendo o está a punto de ocurrir. Frecuentemente el código malicioso no se ejecuta inmediatamente, así que podría haber tiempo desde la introducción del código malicioso y su activación para detectarlo antes de que se lleve a cabo el ataque de *ransomware.*
	DE.CM-7: se realiza monitoreo para la detección de personal, conexiones, dispositivos y software no autorizados. **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	Las personas, las conexiones, los dispositivos y el software no autorizadas son recursos potenciales con los cuales se puede lanzar un ataque de *ransomware.* El monitoreo puede detectar muchos ataques de *ransomware* antes de que sean ejecutados.
	DE.CM-8: se realizan los escaneos de vulnerabilidades **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 5** RA-5	Se pueden aprovechar vulnerabilidades durante un ataque de *ransomware.* Los escaneos regulares pueden permitir que una organización detecte y mitigue la mayoría de las vulnerabilidades antes de que sean utilizadas para ejecutar *ransomware.*
Procesos de detección (DE.DP): se hace mantenimiento a los procedimientos y procesos de detección y se prueban para garantizar estar al tanto de eventos anómalos.	**DE.DP-1:** los roles y responsabilidades para la detección son bien definidos para garantizar la responsabilidad **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-14	La comprensión clara de los roles y las responsabilidades es clave para adjudicar la responsabilidad y alienta el cumplimiento de las políticas y los procedimientos para ayudar a detectar los ataques de *ransomware.*
	DE.DP-2: las actividades de detección cumplen todos los requerimientos aplicables **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 5** AC-25, CA-2, CA-7, PM-14, SI-4, SR-9	Las actividades de detección deben conducirse cumpliendo con las políticas y los procedimientos de la organización.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	DE.DP-3: se prueban los procesos de detección **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 5** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	Las pruebas brindan una garantía de procesos de detección correctos para ataques basados en *ransomware,* reconociendo que no se detectarán todos los intentos de intrusiones. Las pruebas sirven de capacitación para las personas que deberán ejecutar el plan.
	DE.DP-4: se comunica la información de detección de eventos **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA-5, SI-4	La comunicación oportuna de eventos anómalos en necesaria para poder llevar a cabo acciones de remediación antes de que un ataque de *ransomware* sea llevado a cabo completamente.
	DE.DP-5: se mejoran continuamente los procesos de detección **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 5** CA-2, CA-7, PL-2, PM-14, RA-5, SI-4	Se afinan constantemente las tácticas utilizadas en los ataques de *ransomware,* para que los procesos de detección evolucionen continuamente para mantenerse vigentes ante las nuevas amenazas.
Responder		
Planificación de respuesta (RS.RP): se ejecutan los procesos y procedimientos de respuestas y se les hace mantenimiento para garantizar la respuesta a incidentes de ciberseguridad detectados.	**RS.RP-1:** se ejecuta el plan de respuesta durante o después de un incidente **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8	La ejecución inmediata de los componentes de comunicación y relaciones públicas del plan de respuesta es necesaria para parar cualquier corrupción o continuación de exfiltración de datos, restringir la propagación de una infección a otros sistemas y redes e iniciar mensajes preventivos para minimizar daños adicionales, incluyendo daños legales o de reputación.
Comunicaciones (RS.CO): las actividades de respuesta son coordinadas con partes interesadas internas y externas (por ejemplo, apoyo de agencias de las fuerzas del orden).	**RS.CO-1:** el personal conoce sus roles y el orden de operaciones cuando es necesaria una respuesta **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 5** CP-2, CP-3, IR-3, IR-8	La respuesta a eventos de *ransomware* incluye tanto respuestas técnicas como empresariales. Una respuesta efectiva y eficiente requiere que todas las partes comprendan sus roles y responsabilidades. Los roles de respuesta de comunicaciones deben documentarse formalmente en los planes de recuperación y de respuesta a incidentes y deben reforzarse practicando los planes.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	RS.CO-2: los incidentes son reportados uniformemente con criterios establecidos **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8	La respuesta a eventos de *ransomware* incluye tanto respuestas técnicas como empresariales. Una respuesta efectiva y eficiente requiere criterios preestablecidos para el reporte y el cumplimiento de esos criterios durante un evento.
	RS.CO-3: la información se comparte de acuerdo con los planes de respuesta **ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4, Cláusula 16.1.2 **NIST SP 800-53 Rev. 5** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	Las prioridades de intercambio de información incluyen frustrar la propagación de una infección a otros sistemas y redes así como el envío de mensajes preventivos.
	RS.CO-4: la coordinación con partes interesadas ocurre de acuerdo con los planes de respuesta **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	La coordinación con las partes interesadas internas y externas es importante para las prioridades como frustrar la propagación de desinformación y establecer mensajes preventivos.
	RS.CO-5: el intercambio de información voluntario ocurre con las partes interesadas externas para lograr una concientización situacional de ciberseguridad más amplia **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 5** PM-15, SI-5	El intercambio de información puede producir beneficios forenses y reducir el efecto y la rentabilidad de los ataques de *ransomware.* El intercambio voluntario debe complementar cualesquiera requerimientos regulatorios u otros requerimientos de cumplimiento para el reporte y el intercambio.
Análisis (RS.AN): el análisis se lleva a cabo para garantizar una respuesta efectiva y apoyar las actividades de recuperación.	**RS.AN-1:** se investigan las notificaciones generadas por los sistemas de detección **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	Las notificaciones generadas por los sistemas de detección deben investigarse rápida y completamente, dado que estas pueden indicar frecuentemente un ataque de *ransomware* en sus fases tempranas para que pueda evitarse o para que el efecto pueda mitigarse.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	RS.AN-2: se comprende el efecto del incidente **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 5** CP-2, IR-4	Comprender el efecto dará forma a la implementación del plan de recuperación. Las organizaciones deben intentar comprender el efecto técnico de un ataque de *ransomware* (por ejemplo, qué sistemas no están disponibles) y luego comprender el efecto generado sobre el negocio (por ejemplo, cuáles procesos empresariales no están funcionando). Esto ayudará a garantizar que los esfuerzos de respuesta y recuperación sean debidamente priorizados y que se les asignen los recursos debidos y que puedan implementarse los planes de continuidad del negocio en el ínterin.
	RS.AN-3: se realizan las actividades forenses **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 5** AU-7, IR-4	Las actividades forenses ayudan a identificar la causa raíz para contener y erradicar el ataque, incluyendo cosas como el restablecimiento de contraseñas de credenciales robadas por el atacante, la eliminación del *malware* utilizado por el atacante y la eliminación de mecanismos persistentes utilizados por el atacante. Las actividades forenses también pueden suministrar información para los procesos de recuperación y apoyar las acciones de reporte e intercambio de información.
	RS.AN-5: se establecen los procesos para recibir, analizar y responder a vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad) **NIST SP 800-53 Rev. 5** PM-15, SI-5	Los procesos de análisis pueden evitar futuros ataques exitosos y la propagación de *ransomware* a otros sistemas y redes. También pueden ayudar a restablecer la confianza entre las partes interesadas.
Mitigación (RS.MI): se realizan las actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-1:** se contienen los incidentes **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 5** IR-4	Deben tomarse acciones inmediatas para evitar la propagación del *ransomware* a otros sistemas y redes, mitigar sus efectos y resolver el incidente. Contener el *ransomware* incluye cualquier ICS asociado.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
	RS.MI-2: se mitigan los incidentes **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 5** IR-4	Deben tomarse acciones inmediatas para aislar el *ransomware* con el fin de minimizar daños a otros datos, evitar que la infección se propague dentro de la red y a otros sistemas y redes y minimizar el efecto sobre la misión o las actividades empresariales.
	RS.MI-3: se mitigan o documentan las vulnerabilidades recientemente detectadas como riesgos aceptados **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 5** IR-4	La gestión de vulnerabilidades minimiza la probabilidad de ataques de *ransomware* exitosos. Si no se le puede aplicar un parche a una vulnerabilidad o no puede ser mitigada, documentar este riesgo al menos permite que se incluya en la toma de decisiones futuras y proporciona transparencia para las partes interesadas que puedan verse afectadas por eventos de *ransomware.*
Mejoras (RS.IM): las actividades de respuesta organizacionales son mejoradas incorporando las lecciones aprendidas de las actividades de detección/respuesta actuales y anteriores.	**RS.IM-1:** se incorporan las lecciones aprendidas en los planes de respuesta **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	Esto minimiza la probabilidad de futuros ataques de *ransomware* exitosos y puede ayudar a restablecer la confianza entre las partes interesadas.
	RS.IM-2: se actualizan las estrategias de respuesta **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	Esto minimiza la probabilidad de futuros ataques de *ransomware* exitosos y puede ayudar a restablecer la confianza entre las partes interesadas.
Recuperar		
Planificación de recuperación (RC.RP): Se ejecutan los procesos y procedimientos de recuperación y se les hace mantenimiento para garantizar la restauración de sistemas o activos afectados por incidentes de ciberseguridad.	**RC.RP-1:** se ejecuta el plan de recuperación durante o después de un incidente de ciberseguridad **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8	Se pueden reducir pérdidas iniciando el plan de recuperación inmediatamente después de que haya identificado la causa raíz.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Mejoras (RC.IM): se mejoran los procesos y la planificación de recuperación incorporando las lecciones aprendidas en las actividades futuras.	**RC.IM-1:** los planes de recuperación incorporan las lecciones aprendidas **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	Esto minimiza la probabilidad de futuros ataques de *ransomware* exitosos y puede ayudar a restablecer la confianza entre las partes interesadas.
	RC.IM-2: se actualizan las estrategias de recuperación **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	Esto es necesario para mantener la efectividad de la planificación de contingencias para futuros ataques de *ransomware.*
Comunicaciones (RC.CO): se coordinan las actividades de restauración con las partes internas y externas (por ejemplo, centros de coordinación, proveedores del servicio de internet, dueños de los sistemas atacantes, víctimas, otros CSIRT y proveedores).	**RC.CO-1:** se gestionan las relaciones públicas **ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4	Esto minimiza el efecto sobre la empresa al ser abiertos y transparentes y restablece la confianza entre las partes interesadas.
	RC.CO-2: se repara la reputación después de un incidente **ISO/IEC 27001:2013** Cláusula 7.4	La reparación de la reputación minimiza el efecto sobre la empresa y restaura la confianza entre partes interesadas.
	RC.CO-3: se comunican las actividades de recuperación a las partes interesadas internas y externas así como a los equipos ejecutivos y gerenciales **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 5** CP-2, IR-4	La comunicación sobre las actividades de recuperación ayuda a minimizar el efecto sobre el negocio y restaura la confianza entre las partes interesadas.

Referencias

[1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. [Marco para la mejora de la infraestructura crítica de ciberseguridad, versión 1.1 del Instituto Nacional de Normas y Tecnología] (National Institute of Standards and Technology, Gaithersburg, MD) [Instituto Nacional de Normas y Tecnología]. https://doi.org/10.6028/NIST.CSWP.04162018

[2] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) (2013) *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements* (ISO, Geneva, Switzerland). [Organización Internacional para la Normalización/Comisión Electrotécnica Internacional (ISO/IEC) (2013) *ISO/IEC 27001:2013, – Tecnología informática — técnicas de seguridad — sistemas de gestión de seguridad informática — requerimientos* (ISO, Ginebra, Suiza).] Disponible en https://www.iso.org/isoiec-27001-information-security.html

[3] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. [Controles de seguridad y privacidad de fuerzas de trabajo conjunto (2020) para sistemas informáticos y organizaciones] (Instituto Nacional de Normas y Tecnología, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. *[Publicación especial (SP) de NIST, revisión 5]* Incluye las actualizaciones a 10 de diciembre de 2020. https://doi.org/10.6028/NIST.SP.800-53r5

Appendix A—Recursos adicionales de ransomware de NIST

Además de otros recursos mencionados en este documento, El Centro Nacional de Excelencia de Ciberseguridad (NCCoE) de NIST ha producido orientación adicional para apoyar la mitigación de amenazas de *ransomware*. Estos incluyen:

- NIST Special Publication (SP) 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events* [Publicación especial de NIST (SP) 1800-26, *Integridad de datos: detección y respuesta a ransomware y otros eventos destructivos*] aborda cómo una organización puede gestionar un ataque cuando ocurre y qué capacidades necesita tener implementadas para detectar y responder a eventos destructivos.
- NIST SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events* [NIST SP 1800-25, *Integridad de datos: identificación y protección de activos en contra de ransomware y otros eventos destructivos*] aborda cómo una organización puede trabajar antes de un ataque para identificar sus activos y vulnerabilidades potenciales y remediar las vulnerabilidades descubiertas para proteger estos activos.
- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events* [NIST SP 1800-11, *Integridad de datos: recuperación de ransomware y otros eventos destructivos*] aborda esquemas de recuperación en caso de que un ataque de integridad de datos sea exitoso.
- *Protecting Data from Ransomware and Other Data Loss Events [Protección de datos en contra de ransomware y otros eventos de pérdida de datos]* es una guía para proveedores de servicios administrados para hacer, mantener y probar respaldos de archivos que son críticos en la recuperación de ataques de *ransomware*.

NIST tiene muchos otros recursos que, aunque no sean específicos para *ransomware,* contienen información valiosa sobre la identificación, la protección, la detección, la respuesta y la recuperación de eventos de *ransomware.* Se destacan varios a continuación. Para obtener una lista de recursos más completa, visite el sitio web de Protección y respuesta de NIST en https://csrc.nist.gov/ransomware.

- Mejorar la seguridad de las tecnologías de **teletrabajo, acceso remoto** y **traiga su propio equipo (BYOD):**
  - Telework: Working Anytime, Anywhere project [Teletrabajo: proyecto de trabajo en cualquier momento, desde cualquier sitio]
  - NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* [NIST SP 800-46 revisión 2, *Guía de seguridad para el teletrabajo corporativo, acceso remoto y uso de dispositivos personales (BYOD)*]
- **Instalar parches de software** para eliminar vulnerabilidades:

  - NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies* [NIST SP 800-40 revisión 3, *Guía para las tecnologías corporativas de gestión de parches*]
  - Higiene de ciberseguridad crítica: Instalación de parches en proyectos corporativos
- **Usar tecnología de control de aplicaciones** para evitar la ejecución de *ransomware*:
  - NIST SP 800-167, *Guide to Application Whitelisting* [NIST SP 800-167, *Guía para marcar una aplicación en la lista blanca*]
- Encontrar orientación básica sobre la **configuración segura de software** para eliminar vulnerabilidades:
  - Programa Nacional Lista de Verificación
- Obtener la última **información sobre vulnerabilidades conocidas:**
  - Base de datos de vulnerabilidades nacional
- **Planificación para la recuperación** de un evento de ciberseguridad:
  - NIST SP 800-184, *Guide for Cybersecurity Event Recovery [*NIST SP 800-184, *Guía para la recuperación de un evento de ciberseguridad*]
- **Planificación de contingencias para la restauración de operaciones** después de una interrupción causada por *ransomware*:
  - NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems* [NIST SP 800-34 revisión 1, *Guía de planificación de contingencias para sistemas informáticos federales*]
- **Gestión de ransomware** y otros **incidentes** de *malware*:
  - NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [NIST SP 800-83 revisión 1, *Guía para la prevención de incidentes de malware y la gestión para computadoras personales y laptops*]
- **Gestión de incidentes** de ciberseguridad en general:
  - NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* [NIST SP 800-61 revisión 2, *Guía de gestión de incidentes de seguridad informática*]
- Primeros pasos de la **gestión de riesgo de ciberseguridad:**
  - Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide [Primeros pasos del Marco de Ciberseguridad de NIST: Guía de inicio rápido]