RANSOMWARE TASK FORCE

Plan maestro de defensa contra los programas de secuestro (ransomware)

Plan de acción dirigido a las pequeñas y medianas empresas para la mitigación, la respuesta y la recuperación ante programas de secuestro

IST Institute for SECURITY + TECHNOLOGY

Copyright © 2022 - Institute for Security and Technology. ALL RIGHTS RESERVED.

Autores principales

Aaron McIntosh, Director de Comercialización de Productos, ActZero
Valecia Stocchetti, Ingeniera Principal de Ciberseguridad, CIS

Colaboradores

ActZero

Aaron McIntosh, Director de Comercialización de Productos, ActZero

CIS Center for Internet Security®

Curt Dukes, Vicepresidente Ejecutivo, Mejores Prácticas de Seguridad, CIS
Phyllis Lee, Directora Principal de Controles, CIS
Valecia Stocchetti, Ingeniera Principal de Ciberseguridad, CIS
Brian de Vallance, Asesor Principal, CIS

CYBER THREAT ALLIANCE

Michael Daniel, Presidente, Cyber Threat Alliance

GLOBAL CYBER ALLIANCE

Brian Cute, Director del Programa de Capacidad y Resiliencia, Global Cyber Alliance
Leslie Daigle, Directora de Tecnología y del Programa de Integridad de Internet, Global Cyber Alliance
Renee McLaughlin, Responsable de Productos, Programa de Herramientas, Capacidad y Resiliencia

IST Institute for SECURITY + TECHNOLOGY

Megan Stifel, Directora de Estrategias, Institute for Security and Technology

resilience

Davis Hake, Cofundador de Resilience

SecurityScorecard

Sachin Bansal, Director de Operaciones y Asesor Jurídico, SecurityScorecard
Charlie Moskowitz, Vicepresidente de Asuntos Normativos y Gubernamentales, SecurityScorecard

VENABLE LLP

John Banghart, Director Principal de Servicios de Ciberseguridad, Venable LLP

Copyright © 2022 - Institute for Security and Technology. ALL RIGHTS RESERVED.

Agradecimientos

Gracias a la Organización de los Estados Americanos y Amazon Web Services por su patrocinio y apoyo de traducción.

Índice

Resumen ejecutivo 1

Destinatarios 1

Introducción 2

Cómo usar este plan maestro 2

Reconocimiento del riesgo 2

Plan maestro de acción 3

Concordancia con las funciones del Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología 3

Panorama de las salvaguardias 3

Salvaguardias básicas 3

- Identificar 3
- Proteger 4
- Responder 5
- Recuperar 5

Salvaguardias accionables 6

- Identificar 6
- Proteger 6
- Responder 8
- Recuperar 8

Uso del plan maestro para fortalecer el ciberseguro 9

Conclusión 10

Cómo empezar 10

Apéndice A. Plan maestro de defensa contra los programas de secuestro (*ransomware*) 11

Apéndice B. Abreviaturas y siglas 12

Apéndice C. Recursos suplementarios 13

Resumen ejecutivo

Según la Administración para la Pequeña Empresa, en Estados Unidos hay 32.540.953 pequeñas empresas, que representan el 99,9% de todas las firmas[1]. Sin embargo, muchas no están suficientemente preparadas para hacer frente al riesgo de un ciberataque. Por ejemplo, un estudio del costo de los delitos cibernéticos realizado por Accenture en 2019 reveló que 43% de los ciberataques están dirigidos contra pequeñas empresas, de las cuales solo 14% están preparadas para defenderse[2]. A fin de abordar este riesgo, es cada vez más común que las pequeñas y medianas empresas (pymes) obtengan un seguro contra riesgos cibernéticos. Sin embargo, en medida creciente, las aseguradoras están exigiendo que las empresas comprendan mejor los métodos de gestión del ciberriesgo, los apliquen y los demuestren como requisito para contratar seguros de este tipo.

En este contexto, recomendamos que las pymes adopten un marco de ciberseguridad compuesto por las mejores prácticas para defenderse de estos ataques. La aplicación de un marco de este tipo podría ayudar a las empresas a reforzar sus mecanismos de defensa. Lamentablemente, es difícil saber por dónde empezar, de modo que muchas empresas siguen desorientadas y no dan prioridad a las medidas de ciberseguridad. En consecuencia, es necesario presentar ese marco en términos sencillos, con orientación práctica y fácil de entender. Por desgracia, algunas pymes creen que no pueden establecer marcos de ciberseguridad y, por lo tanto, han perdido oportunidades de negocios para las cuales debían demostrar que contaban con estos marcos. Así se perpetúa el ciclo de preparación ineficiente en materia de ciberseguridad.

En respuesta a la acción 3.1.1 del Informe del Grupo de Trabajo sobre Programas de Secuestro, en la cual se exhorta a las organizaciones de ciberseguridad a establecer un marco claro y accionable para la mitigación, la respuesta y la recuperación ante programas de secuestro, el *Grupo de Trabajo encargado de elaborar un plan de defensa contra los programas de secuestro* formuló un plan maestro que abarca un subconjunto de salvaguardias esenciales de ciberhigiene[3] seleccionadas de los controles críticos de seguridad del Centro para la Seguridad de Internet (CIS Controls®) v8. Estas salvaguardias constituyen una norma mínima de seguridad de la información que todas las empresas deben usar para defenderse de los ataques más comunes. El *Plan maestro de defensa contra los programas de secuestro (ransomware)* es un conjunto de salvaguardias básicas y accionables dirigidas a las pymes[4].

Por consiguiente, este plan utiliza los controles CIS, conjunto de medidas prescriptivas prioritarias elaboradas por una comunidad mundial de expertos en ciberseguridad. El plan maestro contiene 40 salvaguardias recomendadas, que han sido seleccionadas cuidadosamente no solo porque son fáciles de aplicar, sino también debido a su eficacia en la defensa contra ataques de secuestro (ataques de *ransomware*). Eso se comprobó en un análisis del Modelo de Defensa Comunitaria CIS v2.0 (CIS CDM v2.0), en el cual se observó que la aplicación de las salvaguardias contenidas en este plan constituye una buena defensa frente a más del 70%[5] de las técnicas de ataque de los programas de secuestro. Cabe destacar que este plan maestro no es una guía para la implementación, sino una recomendación de medidas defensivas para protegerse y responder ante ataques de secuestro y otros ciberataques comunes. En el apéndice C de este documento y en el cuaderno correspondiente se presentan varias herramientas y recursos que pueden usarse para facilitar la aplicación de estas salvaguardias.

Destinatarios

El Grupo de Trabajo formuló el plan maestro específicamente con el fin de eliminar una barrera crucial para las pymes que tienen poca pericia en materia de ciberseguridad para defenderse de los programas de secuestro. El plan está escrito en términos sencillos, con descripciones de la forma en que las salvaguardias recomendadas mitigan los riesgos conexos, y provee información útil para los dirigentes de empresas y el personal técnico, que necesitan trabajar de manera mancomunada para comprender los riesgos y priorizar la acción.

[1] U.S. Small Business Advisory Office of Advocacy. Preguntas frecuentes sobre las pymes, diciembre de 2021, https://cdn.advocacy.sba.gov/wp-content/uploads/2021/12/06095731/Small-Business-FAQ-Revised-December-2021.pdf.
[2] Accenture. *Ninth Annual Cost of Cybersecurity*, marzo de 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.
[3] Las medidas esenciales de ciberhigiene consisten en las salvaguardias del Grupo de Implementación 1 de los Controles CIS.
[4] Las empresas abarcan entidades de los sectores público y privado.
[5] Según el Modelo de Defensa Comunitaria CIS (CDM) v2.

Introducción

El Grupo de Trabajo sobre Programas de Secuestro exhortó a la comunidad de ciberseguridad a establecer un marco claro y accionable para la mitigación, la respuesta y la recuperación. Este plan maestro se basa en los controles CIS, conjunto de prácticas óptimas muy difundidas y de gran aceptación que ayudan a las empresas a concentrar sus recursos en las medidas críticas necesarias para defenderse de los ciberataques más comunes. Incluye las prácticas óptimas o "salvaguardias" más pertinentes para combatir los programas de secuestro[6].

El CIS diseñó las salvaguardias seleccionadas para pymes con equipos pequeños de tecnología de la información, que tienen poca pericia en materia de ciberseguridad y suelen defender a las empresas de ataques generales no focalizados. Estas salvaguardias constituyen medidas esenciales de ciberhigiene, es decir, los controles protectores y la capacidad básica que se necesitan para implementar capacidades más avanzadas. El éxito depende directamente de la planificación y la preparación. Igual que un edificio o un simulacro de incendio, cuanto más sólidos sean los planes y las bases, más probable será que la empresa pueda resistir un ciberataque. Estos ataques pueden ser rápidos e imprevistos y paralizar abruptamente a una empresa que no esté preparada.

Para ayudar a las empresas a priorizar mejor sus actividades, en este plan maestro se presentan salvaguardias de dos tipos: básicas y accionables. Las salvaguardias básicas son aquellas que una empresa debe aplicar para tomar eficazmente cualquier otra medida de ciberseguridad. Las salvaguardias accionables toman como punto de partida las salvaguardias básicas y refuerzan la postura de ciberseguridad de una empresa.

Recomendamos que las pymes apliquen el mayor número posible de estas salvaguardias. Entendemos que no todas las empresas podrán aplicar todas las salvaguardias. Aunque el Grupo de Trabajo recomienda la plena implementación de las salvaguardias del plan maestro, toda aplicación parcial es un paso importante para mejorar la ciberseguridad de una empresa. El objetivo no es la perfección. Si la mayoría de las pymes adoptan estos controles, nuestras empresas serán más resilientes y ciberseguras.

Cómo usar este plan maestro

Los usuarios deben tomar este plan maestro como punto de partida para priorizar sus defensas de ciberseguridad. El apéndice A contiene una lista completa de salvaguardias para la defensa contra los ataques de secuestro. Hay varias herramientas y recursos, que se encuentran en el apéndice C y en el cuaderno correspondiente, para facilitar la aplicación de estas salvaguardias. La inclusión de herramientas en el documento acompañante no constituye ni implica de manera alguna el apoyo del *Grupo de Trabajo encargado de elaborar un plan de defensa contra los programas de secuestro* a una solución en particular, y la inclusión de herramientas y soluciones no constituye una garantía del Grupo de Trabajo con respecto a su eficacia para proporcionar una cobertura de ciberseguridad que mejore la protección contra los programas de secuestro.

Reconocimiento del riesgo

En este plan maestro se hace mucho hincapié en la aplicación de medidas protectoras y en el aumento de la capacidad para implementar capacidades más avanzadas. Aunque los análisis indican que las *medidas esenciales de ciberhigiene* son una defensa contra más del 70%[7] de las técnicas de ataque utilizadas con programas de secuestro, su eficacia dependerá en última instancia de cuán bien se las aplique y del empeño de los adversarios.

Como se verá más adelante, las medidas esenciales de ciberhigiene representan una norma mínima de seguridad de la información para todas las empresas y facilitan la adopción de otros controles CIS. Este plan maestro es lo que toda empresa debería poner en práctica para defenderse de los ataques más comunes. En el caso de las pymes, podría ser necesario adoptar más salvaguardias para defenderse de ataques más avanzados.

[6] Estas prácticas son las indicadas por el Grupo de Implementación 1 de los Controles CIS v8.
[7] De acuerdo con el Modelo de Defensa Comunitaria CIS (CDM) v2.

Plan maestro de acción

Para defenderse de los programas de secuestro, las pymes deben adoptar un enfoque estratificado con el objetivo de proteger sus activos más críticos. Con ese fin es necesario establecer controles en áreas tales como gestión de activos empresariales y del inventario de programas informáticos, gestión de vulnerabilidades, defensa contra programas maliciosos (*malware*), capacitación, recuperación de datos y respuesta a incidentes. A medida que los programas de secuestro evolucionan, los adversarios van creando técnicas nuevas, como extorsión. En estos casos, los atacantes exfiltran datos antes del cifrado y después exigen que les paguen para no divulgarlos al público. Con las salvaguardias descritas en este plan maestro, las pymes están en buenas condiciones para defenderse de los programas de secuestro y de otros tipos de ataques.

A continuación se describen las salvaguardias básicas y las salvaguardias accionables para defenderse de programas de secuestro y se explica su importancia. **Los usuarios de este plan maestro deben concentrarse en la aplicación de las salvaguardias básicas antes de las accionables (que son más técnicas).**

Concordancia con las funciones del Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología

En vista de la amplia aceptación del conjunto de salvaguardias en la administración pública, las empresas y la comunidad de ciberseguridad, el *Grupo de Trabajo encargado de elaborar un plan de defensa contra los programas de secuestro* lo armonizó con las funciones del Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST) —identificar, proteger, detectar, responder y recuperar—, que facilitan la ejecución de un programa de ciberseguridad eficaz. Agrupar las medidas de acuerdo con estas funciones puede ayudar a las pymes a comprender mejor los riesgos, los pasos necesarios para protegerse de esos riesgos, las herramientas que pueden usar para buscar y detectar riesgos, y las soluciones para contener y remediar las amenazas cuanto antes.

Debido a su complejidad y a su índole técnica, en este plan maestro no se presentan las salvaguardias relacionadas con la función de "detectar". No obstante, el Grupo de Trabajo recomienda enfáticamente que las pymes que sigan este plan maestro trabajen con un proveedor de servicios de ciberseguridad si necesitan asistencia para establecer controles de detección o de otros tipos, según corresponda.

Panorama de las salvaguardias

El plan maestro abarca 40 salvaguardias: 14 básicas y 26 accionables. Estas medidas se agrupan primero de acuerdo con las funciones del Marco de Ciberseguridad del NIST. Para cada función, el plan maestro presenta las salvaguardias por orden de prioridad según su utilidad para combatir los programas de secuestro y establecer una postura general de defensa de ciberseguridad[8].

Salvaguardias básicas

Las salvaguardias básicas son los componentes fundamentales de un programa de ciberseguridad de una empresa. Asimismo, permiten la aplicación de salvaguardias accionables. En el plan maestro se presentan 14 salvaguardias básicas prioritarias, que se describen a continuación.

Identificar

Para defender la red, primero hay que saber qué hay en ella, es decir, qué tecnología se usa y qué datos se almacenan y se transmiten. De acuerdo con las salvaguardias básicas que corresponden a la función de *identificar*, se recomienda que las pymes hagan y mantengan inventarios de los activos y los programas informáticos a fin de administrar mejor todos los dispositivos conectados y que establezcan procesos de gestión de datos en los cuales se indiquen claramente los métodos de recopilación, uso y almacenamiento de datos. Asimismo, se debe hacer y mantener un inventario de cuentas, tanto de los usuarios comunes como de aquellos que tengan privilegios.

Estas salvaguardias son indispensables para protegerse y responder a secuestros. Si no se sabe qué activos, programas informáticos y cuentas hay en la red de una empresa, es difícil defenderse de un incidente y responder. Por ejemplo, un atacante podría comprometer y usar dispositivos desconocidos con mayor facilidad

[8] El Grupo de Trabajo basó la priorización en el análisis del marco de Tácticas Adversarias, Técnicas y Conocimiento Común de MITRE (ATT&CK®) realizado por el CIS y presentado en su Modelo de Defensa Comunitaria (CDM) v2.0.

en el entorno de la empresa. Eso podría exacerbar el riesgo para la empresa y prolongar el ataque o posibilitar otros ataques. Conocer el entorno en el cual se opera es la base para aplicar medidas esenciales de ciberhigiene en todos los dispositivos.

Salvaguardias:

- Hacer y mantener un inventario detallado de activos de la empresa
- Hacer y mantener un inventario de programas informáticos
- Establecer y mantener un proceso de gestión de datos
- Hacer y mantener un inventario de cuentas

Aunque estas salvaguardias son muy complejas, ya que constantemente se agregan nuevos activos a la red, son fundamentales para la defensa eficaz y desempeñan un papel crucial en otras actividades defensivas, como las copias de seguridad y la respuesta a incidentes. Además, los datos ya no están contenidos dentro de las cuatro paredes de una empresa: los dispositivos móviles y portátiles se conectan con recursos de la empresa, lo cual dificulta la gestión de datos si no se han establecido salvaguardias apropiadas.

Proteger

Una vez que una pyme sabe qué hay en su red, el paso siguiente consiste en aplicar salvaguardias a los activos, los datos y los usuarios para protegerlos de agentes maliciosos que traten de perjudicarlos.

Configuraciones seguras

Los procesos de gestión de la configuración son importantes para mantener la seguridad con el tiempo. Estas salvaguardias se centran en el diseño de los dispositivos y de la red en general y en las reglas que rigen su funcionamiento, que, en conjunto, constituyen la "configuración". Consisten en el uso de procesos de configuración segura de los activos de la empresa, como computadoras portátiles, computadoras de escritorio, servidores y dispositivos móviles, por nombrar solo algunos. También es importante que haya un proceso para configurar la infraestructura de la red que abarque dispositivos tales como cortafuegos, enrutadores y conmutadores. La adición de activos empresariales, programas informáticos, usuarios, etc., puede aumentar el riesgo si no hay procesos sólidos para aplicar o reaplicar controles de seguridad apropiados. Por ejemplo, la actualización de un programa informático podría cambiar un parámetro de la configuración y volverla menos segura. Una empresa debe contar con un proceso de configuración segura que verifique si los activos se ciñen a las configuraciones y las normas establecidas y que restablezca el cumplimiento de ser necesario, a fin de abordar las desviaciones de la seguridad que puedan producirse con el tiempo.

Gestión de cuentas y del acceso

Las cuentas de usuarios pueden tener tipos de acceso muy variados, que van desde el acceso a funciones básicas, como correo electrónico, hasta cuentas con mayores privilegios desde las cuales se puede tener acceso a casi todo lo que haya en la empresa. Las salvaguardias básicas correspondientes a la función de *proteger* requieren que la empresa establezca un proceso para otorgar y revocar permisos para tener acceso a sistemas de la empresa. También es crucial que la empresa siga el principio del mínimo privilegio, de acuerdo con el cual se otorga a los usuarios solo los privilegios que necesiten para realizar una tarea, incluso cuando cambian las funciones de un empleado, cuando se necesitan permisos nuevos (o temporarios) para un proyecto y cuando un empleado se incorpora a la empresa o se va.

Planificación de la gestión de vulnerabilidades

Los investigadores y otros interesados en el tema de la seguridad encuentran y publican más de 18.000 vulnerabilidades de programas informáticos al año. Aunque siempre hay más vulnerabilidades de las cuales no se tiene conocimiento, los agentes maliciosos por lo general aprovechan primero las vulnerabilidades conocidas. Por lo tanto, la gestión de vulnerabilidades desempeña un papel crucial en la protección de la infraestructura de una empresa. En el plan maestro se recomiendan dos salvaguardias para el establecimiento de procesos de gestión de vulnerabilidades y corrección de riesgos, que consisten en aplicar parches de seguridad al sistema operativo y a las aplicaciones oportunamente. Este proceso se aplica no solo a los activos y los programas informáticos, sino también a los dispositivos de la red que se usan para administrarlos o monitorearlos.

Concientización de seguridad y capacitación

Aunque las inversiones en tecnología son importantes, la gente es un recurso esencial para reforzar las defensas contra programas de secuestro y otros ataques. Según el informe de Verizon sobre las investigaciones de filtraciones de datos de 2021[9], en el 85% de las filtraciones intervino un elemento humano. En este plan maestro se recomienda a las pymes que establezcan y mantengan un programa de concientización de seguridad para todos los empleados, socios y terceros usuarios. Este programa consiste no solo en capacitar al personal para interactuar con las redes y los sistemas de la empresa de manera segura, sino también en lograr que los empleados comprendan la importancia de la seguridad y el papel que desempeñan en la protección de la empresa.

Salvaguardias:

- Establecer y mantener un proceso de configuración segura
- Establecer y mantener un proceso de configuración segura para la infraestructura de la red
- Establecer un proceso para otorgar acceso
- Establecer un proceso para revocar el acceso
- Establecer y mantener un proceso de gestión de vulnerabilidades
- Establecer y mantener un proceso de corrección
- Establecer y mantener un programa de concientización de seguridad

Responder

La preparación es fundamental para responder a incidentes. Al tener un plan antes de que se produzca un incidente, la empresa sabe qué hacer si sufre un ataque. Las salvaguardias relacionadas con la función de *responder* ayudan a acortar la interrupción de las operaciones si los controles fallan y el atacante logra causar daños.

De acuerdo con estas salvaguardias, las empresas establecen procesos para la notificación de incidentes y la gestión de registros de seguridad. Como mínimo, las pymes deben tener un procedimiento para que el personal notifique los incidentes, en el cual se indique el plazo para la notificación, a quién notificar, cómo notificar el incidente y la información necesaria para la notificación. Si las empresas cuentan con medidas de recuperación, pueden reanudar plenamente las operaciones con rapidez a fin de reducir al mínimo la interrupción, la pérdida de ingresos y el daño para la marca. Las empresas deberían hacer periódicamente simulacros improvisados de aplicación del plan de respuesta a incidentes con el propósito de sentar las bases para obtener el mejor resultado posible en caso de ataque real.

Los registros también son cruciales para que una empresa pueda responder a un incidente. El primer paso de la gestión de registros consiste en establecer un proceso a fin de que la empresa sepa qué registros deben recopilarse como mínimo, con qué frecuencia deben examinarse y cuánto tiempo deben conservarse. Si la empresa sufre un ataque, para responder al incidente se necesitarán los registros a fin de determinar la fuente del ataque u obtener pruebas con fines judiciales.

Salvaguardias:

- Establecer y mantener un proceso de notificación de incidentes en la empresa
- Establecer y mantener un proceso de gestión de registros de operaciones

Recuperar

Uno de los daños más grandes que causan los programas de secuestro es la pérdida de datos esenciales para las operaciones de una pyme. El plan maestro incluye una salvaguardia básica de acuerdo con la cual las pymes deben establecer y mantener un proceso de recuperación de datos como parte de la planificación de la respuesta y la recuperación. Las nuevas técnicas de los programas de secuestro (por ejemplo, la extorsión) plantean dificultades para las empresas que tienen buenos controles para recuperar los datos, pero no para protegerlos, razón por la cual se necesitan ambos tipos de controles a fin de recuperarse de un incidente de secuestro.

Salvaguardias:

- Establecer y mantener un proceso de recuperación de datos

[9] *2021 Verizon Data Breach Investigations Report (DBIR)*, https://www.verizon.com/business/resources/reports/dbir/.

Salvaguardias accionables

Además de las salvaguardias básicas, para mantener eficazmente la seguridad a largo plazo se necesitan otras medidas. Con las 26 salvaguardias accionables seleccionadas y priorizadas en el plan maestro, una empresa puede mejorar su seguridad y defenderse de programas de secuestro y otros ciberataques generales no focalizados. Las salvaguardias accionables toman como punto de partida las salvaguardias básicas y consisten en la aplicación de los controles técnicos necesarios para proteger el entorno de una empresa.

Identificar

Como complemento de las salvaguardias básicas relacionadas con la función de *identificar*, de acuerdo con las cuales las pymes deben saber qué dispositivos y datos se usan en su entorno, la salvaguardia accionable del plan maestro correspondiente a esta función requiere que las pymes usen siempre en todos sus activos los programas informáticos autorizados más actualizados que haya. Los adversarios escanean continuamente las redes para explotar versiones vulnerables de programas informáticos. Las vulnerabilidades de estos programas siguen siendo uno de los principales vectores del ataque inicial con fines de secuestro. Por consiguiente, mantener los programas informáticos actualizados y verificar la lista con frecuencia son medidas que ayudan a reducir el riesgo de explotación.

Salvaguardia:

- Verificar que los programas informáticos autorizados sigan vigentes

Proteger

Casi 70% de las salvaguardias accionables del plan maestro corresponden a la función de *proteger*. Esta función es esencial porque su finalidad es limitar o contener el impacto de un posible incidente de ciberseguridad. Las salvaguardias recomendadas están relacionadas con aspectos técnicos y con la capacitación. Las salvaguardias técnicas consisten en instalar y administrar cortafuegos en los servidores de la empresa, administrar la seguridad de los medios extraíbles e instalar y administrar programas antimalware, por nombrar solo algunas. Las salvaguardias relacionadas con la capacitación abordan la necesidad de enseñar al personal a reconocer un ataque y notificarlo.

Configuraciones seguras

Aunque los programas de secuestro usan diversos vectores de infección iniciales, en la mayoría de los intentos de intrusión se usan tres: el protocolo de escritorio remoto (RDP) para el control remoto de dispositivos con Windows; la suplantación de identidad (*phishing*), que generalmente consiste en correos electrónicos maliciosos que parecen provenir de fuentes confiables, pero cuya finalidad es robar credenciales o información confidencial; y la explotación de vulnerabilidades de programas informáticos. La reducción de la vulnerabilidad de activos, programas informáticos y dispositivos de la red los defiende de estos vectores principales de los ataques y cierra las brechas en la seguridad que podrían persistir como consecuencia de configuraciones por defecto poco seguras. Las omisiones tales como no desactivar o cerrar cuentas por defecto, no cambiar las contraseñas por defecto y no modificar otros parámetros vulnerables aumentan el riesgo de explotación por un adversario. Las salvaguardias de esta sección consisten en que las pymes instalen y administren un cortafuegos en los servidores y administren las cuentas por defecto en las redes y los sistemas de la empresa.

Se recomienda también emplear las mejores prácticas (por ejemplo, CIS Benchmarks™ y las guías de implementación técnica de seguridad de la Agencia de Sistemas de Información de Defensa [DISA STIG]) para configurar los sistemas de manera segura.

Gestión de cuentas y del acceso

Cuando un atacante consigue las credenciales para tener acceso a una cuenta, especialmente una con privilegios, puede ocasionar grandes daños. No solo puede entrar en la red de una empresa, sino que también puede desplazarse dentro de la red y comprometer cuentas y sistemas vecinos. En el plan maestro se recomiendan varias actividades para reducir el riesgo de que las cuentas se vean afectadas, entre ellas evaluaciones periódicas de los derechos de acceso privilegiado, el cierre de cuentas inactivas, la gestión apropiada de contraseñas para no caer en la trampa de reutilizarlas, y el uso de la autenticación de múltiples factores en todos los sistemas de la empresa. Esta última medida es especialmente importante porque crea otra capa de seguridad por si una contraseña corre peligro. La gestión de cuentas y del acceso se aplica también a las plataformas en la nube, especialmente los servicios de correo electrónico en la nube, que podrían conectarse a otros recursos de la empresa.

Planificación de la gestión de vulnerabilidades

Los programas de secuestro siguen asediando a las empresas que no instalan oportunamente parches de seguridad para corregir vulnerabilidades conocidas. En varios informes de dominio público se recalca que los atacantes explotan no solo las vulnerabilidades encontradas poco antes, sino también las que existen desde hace mucho tiempo. En el plan maestro se recomiendan varias salvaguardias para la gestión de vulnerabilidades, entre ellas administrar mejor los parches e instalar las actualizaciones más recientes de los sistemas de las redes y los dispositivos. La gestión de vulnerabilidades es especialmente importante en los sistemas de generación anterior, que podrían estar funcionando con programas informáticos obsoletos que el proveedor ya no acepta, lo cual expone el sistema a un ataque. Si un sistema de generación anterior ya no se puede actualizar, hay que adoptar otros controles para que cuente con una protección adecuada o reemplazarlo.

Las empresas deberían considerar la posibilidad de instalar automáticamente parches para sistema operativos tales como Microsoft®, Windows® y Apple® macOS®. Si los parches no se instalan automáticamente, las empresas o sus socios en el ámbito de la seguridad deben prestar especial atención a las vulnerabilidades críticas o de día cero anunciadas en el aviso de seguridad y en las actualizaciones de cada proveedor y poner en práctica de inmediato la orientación proporcionada en el parche.

Defensas contra programas maliciosos

Los programas de secuestro pueden transmitirse de varias maneras; por ejemplo, por correo electrónico (por medio de un enlace o un adjunto), navegadores web y medios extraíbles. Varias de las salvaguardias del plan maestro están relacionadas con defensas contra programas maliciosos, entre ellas la instalación de herramientas antimalware para evitar ataques contra activos de la empresa y la actualización de los programas antimalware y sus definiciones. También es importante mantener actualizados los navegadores y los clientes de correo electrónico para evitar los ataques por medio de estas aplicaciones. Los medios extraíbles (por ejemplo, las memorias USB) también plantean un riesgo. Las funciones tales como el inicio automático y la reproducción automática pueden permitir la ejecución automática de contenido en un sistema cuando se conecta o se enchufa un medio extraíble. Si se enchufa en el sistema un medio extraíble infectado por un programa malicioso, puede infectar al sistema objetivo y a los sistemas vecinos. La desactivación de estas funciones reduce el riesgo.

Otros vectores populares de programas de secuestro son las URL maliciosas, que se pueden transmitir por correo electrónico o directamente por medio de un navegador web. Cualquiera que sea el origen del programa malicioso, con controles tales como filtrado de DNS se puede evitar la descarga de programas maliciosos en el sistema de una víctima o impedir que un usuario vea una página de suplantación de identidad (y así impedir que se envíen credenciales a un atacante o que se descargue un archivo malicioso). Hay muchos servicios gratuitos de filtrado de DNS, que constituyen una manera rápida y fácil de mitigar el riesgo de una empresa.

Concientización de seguridad y capacitación

Es sumamente importante abordar las brechas internas, como la falta de capacitación. En vista del crecimiento incesante de la suplantación de identidad y la captación ilegítima de datos confidenciales por SMS (*smishing*, que consiste en mensajes de texto cuyo fin es engañar a los usuarios para que proporcionen información confidencial o para que descarguen aplicaciones maliciosas), en el plan maestro se recomienda que las pymes enseñen a sus empleados a reconocer y notificar los ataques de ingeniería social y los incidentes de seguridad.

La capacitación del personal a fin de que reconozca un ataque de ingeniería social es crucial para establecer defensas en una red. Aunque se pueden instalar herramientas y tecnología con el objetivo de defender a la empresa de ataques de suplantación de identidad, estas herramientas no son completamente eficaces, de modo que el personal de la empresa es la principal línea de defensa.

Es igualmente importante enseñar al personal a notificar incidentes de seguridad. Cualquiera que sea el tipo de ataque, debe notificarse de inmediato. La pronta notificación, seguida de una acción inmediata, puede interrumpir un ataque y detener o reducir el daño. La capacitación es esencial para que el personal sepa qué hacer y cómo hacerlo.

Salvaguardias:

- Administrar las cuentas por defecto en los activos y los programas informáticos de la empresa
- Usar contraseñas únicas

- Inhabilitar las cuentas inactivas
- Restringir los privilegios de administrador a las cuentas para uso exclusivo del administrador
- Exigir la autenticación de múltiples factores para aplicaciones con acceso externo
- Exigir la autenticación de múltiples factores para el acceso remoto a la red
- Exigir la autenticación de múltiples factores para el acceso administrativo
- Automatizar la gestión de parches del sistema operativo
- Automatizar la gestión de parches de las aplicaciones
- Usar solo navegadores y clientes de correo electrónico que estén plenamente vigentes
- Usar servicios de filtrado de DNS
- Mantener actualizada la infraestructura de la red
- Instalar y mantener programas antimalware
- Configurar la actualización automática de definiciones de antimalware
- Desactivar el inicio automático y la reproducción automática de medios extraíbles
- Enseñar al personal a reconocer ataques de ingeniería social
- Enseñar al personal a reconocer y notificar incidentes de seguridad

Responder

Lamentablemente, en la práctica, los mejores mecanismos de protección a veces no pueden parar a un adversario laborioso que esté dispuesto a dedicar el tiempo y el esfuerzo necesarios para causar perturbaciones en una empresa. Las salvaguardias accionables correspondientes a la función de *responder* consisten en la notificación de incidentes, el establecimiento de contactos importantes, la forma y el momento de interactuar con ellos, y el proceso y las herramientas necesarios para recopilar y almacenar registros de manera adecuada.

Contar por lo menos con una persona que se encargue de manejar los incidentes facilitará la coordinación de la respuesta a incidentes. Estas personas podrían ser empleados de plantilla, terceros proveedores o una combinación de ambos. También es útil hacer una lista de contactos para informarles acerca del incidente, a fin de que la empresa esté preparada de antemano. Los contactos podrían ser empleados de plantilla, las fuerzas del orden, compañías de seguros, organismos públicos, abogados u otros interesados. La comunicación es fundamental durante un incidente, ya que hay muchas piezas en movimiento.

También es importante recopilar registros de operaciones antes de un incidente, que podrían abarcar registros de sistemas operativos, aplicaciones o dispositivos de la red. En un incidente puede ser sumamente útil analizar los registros para determinar qué ocurrió. Lo que es más importante, este análisis puede usarse a fin de aplicar medidas de mitigación para que no se repita el ataque. Es importante también que el almacenamiento de registros sea adecuado, ya que los archivos de registros pueden ocupar espacio con rapidez en un sistema y afectar su desempeño.

Salvaguardias:

- Designar personal que se ocupe del manejo de incidentes
- Obtener y mantener información sobre contactos para la notificación de incidentes de seguridad
- Recopilar registros de operaciones
- Almacenar los registros de operaciones de una manera adecuada

Recuperar

Contar con buenas copias de seguridad de datos esenciales es una de las estrategias más eficaces para recuperarse de un ataque de secuestro. En el plan maestro se prescriben varias salvaguardias accionables para la recuperación de datos, entre ellas hacer y restaurar copias de seguridad de los datos. A fin de recuperarse de un ataque de secuestro, es importante automatizar el proceso de copias de seguridad, proteger los datos y asegurar que no estén conectados regularmente a la red. Esta última medida es importante porque, aunque se adopten todos los controles apropiados para proteger las copias de seguridad de los datos, si las copias están almacenadas directamente en la red o en el sistema secuestrado, los atacantes cifrarán también esos datos.

Salvaguardias:

- Hacer copias de seguridad automáticas
- Proteger los datos de recuperación
- Establecer y mantener una instancia aislada de datos de recuperación

Uso del plan maestro para fortalecer el ciberseguro

El Grupo de Trabajo sobre Programas de Secuestro estima que, en 2021, las víctimas pagaron $602 millones en extorsiones con programas de secuestro, lo cual representa un aumento del 70% en comparación con 2020. Los incidentes de secuestro constituyeron el 79% de los reclamos por interrupción de las operaciones[10] y ocasionaron un aumento interanual de más del 90% en las primas de seguros[11]. Esto es insostenible tanto para los asegurados como para el mercado, y es una de las razones por las cuales muchos proveedores de seguros contra riesgos cibernéticos han estados muy dispuestos a apoyar la labor del Grupo de Trabajo sobre Programas de Secuestro.

El ciberseguro, que comenzó hace veinte años como cobertura nueva para la responsabilidad civil de las empresas por filtración de datos, ha evolucionado notablemente en los últimos diez años y se ha convertido en una herramienta crucial para la gestión del ciberriesgo empresarial. En el plan maestro se examinan salvaguardias básicas y accionables. Las pymes pueden solicitar ayuda y orientación de las aseguradoras de ciberriesgos para poner en práctica muchos de estos controles. La mayoría de las aseguradoras de ciberriesgos ofrecen productos proactivos a precios reducidos que disminuirán considerablemente el costo y la complejidad de la aplicación de muchas de las salvaguardias recomendadas en este plan maestro. Sin embargo, el marcado aumento de la efectividad de los ataques de secuestro y la ampliación de su escala han presentado un gran reto para el mercado utilizado por las aseguradoras y otros con el fin de calcular la responsabilidad civil emanada de grandes incidentes de filtración de datos.

El *Plan maestro de defensa contra los programas de secuestro (ransomware)* aporta dos elementos cruciales para la lucha de las compañías de ciberseguros contra la intensificación de estos ataques delictivos.

- Primero, el plan maestro proporciona una guía práctica basada en los datos, orientada específicamente al mercado de las pequeñas y medianas empresas, que suelen ser las que más dificultades tienen para defender sus sistemas. El Grupo de Trabajo tomó como punto de partida las salvaguardias del Grupo de Implementación 1 de los Controles Críticos de Seguridad CIS y seleccionó las medidas de seguridad más cruciales para la defensa contra programas de secuestro. Estas medidas, que han sido examinadas por profesionales especializados en seguros a fin de comprobar su concordancia con lo que se ve en la práctica en las declaraciones de siniestros, podrían ayudar a reducir la probabilidad de ataques.

- Segundo, el plan maestro ayuda a las compañías de seguros a comprender mejor qué señales deben buscar al asegurar cuentas. En otras líneas de seguros, la tarifación y selección de riesgos, así como las medidas de mitigación de las compañías aseguradoras y reaseguradoras, se fundamentan en datos sobre pérdidas basados en la ingeniería. Debido al elemento de adversarios humanos y a su índole sumamente técnica, en el ciberseguro se han usado con frecuencia datos obtenidos de litigios relacionados con la filtración de datos como base para determinar los precios actuariales y las directrices para la tarifación y selección de riesgos. La proliferación de programas de secuestro ha demostrado sin lugar a dudas la necesidad de prestar más atención a los controles de seguridad para detener los ataques y acelerar la recuperación, a fin de que los asegurados no se vean obligados a pagar una extorsión para recuperar sus sistemas críticos con prontitud.

En consonancia con muchas de las recomendaciones del plan maestro, algunos de los controles de seguridad que la industria de los ciberseguros ha observado que reducen el costo de los incidentes y, por lo tanto, tiene en cuenta en el proceso de aseguramiento son los siguientes:

- buenas copias de seguridad;
- concientización de seguridad y capacitación sobre respuesta a incidentes;
- mecanismos de seguridad del correo electrónico en toda la empresa;
- protección avanzada contra programas maliciosos en el punto final;
- visibilidad y seguridad de la red.

[10] https://netdiligence.com/wp-content/uploads/2021/09/NetD_2021_Claims_Study_1.0_PUBLIC.pdf
[11] https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html

Presentamos varios recursos sobre la respuesta a incidentes en el documento correspondiente para que las empresas que no tienen normas de seguridad bien desarrolladas cuenten con un punto de partida creado por la industria para llevar la ciberseguridad a un nivel más alto.

Conclusión

Las 40 salvaguardias recomendadas en el plan maestro han sido seleccionadas cuidadosamente no solo por la facilidad con la cual pueden aplicarse, sino también por su eficacia en la defensa contra ataques de secuestro. La finalidad de las medidas esenciales de ciberhigiene es dotar a las pymes de medios para responder a un incidente de secuestro, mitigar sus efectos y recuperarse. La aplicación del mayor número posible de salvaguardias debería formar parte de un programa iterativo de gestión de riesgos en toda empresa. Las pymes que apliquen las medidas esenciales de ciberhigiene estarán mejor protegidas y bien posicionadas para defenderse de programas de secuestro. Asimismo, podrán administrar el ciberriesgo más eficazmente y adoptar los controles adicionales que necesiten para abordar amenazas específicas.

Por último, el *Grupo de Trabajo encargado de elaborar un plan de defensa contra los programas de secuestro* se ha propuesto eliminar las barreras a la adopción en la medida de lo posible. Con ese fin, presentamos herramientas y recursos que pueden usarse para aplicar cada una de las salvaguardias. En los casos en que esos recursos no sean suficientes, es aconsejable preguntar y pedir orientación a proveedores de servicios de ciberseguridad. Aunque es imposible mantener una ciberseguridad perfecta, se puede lograr que una empresa sea más resistente y resiliente frente a las ciberamenazas.

Cómo empezar

Como ya se dijo, el establecimiento de un marco de seguridad puede abrumar a muchas pymes. Es importante comenzar en pequeña escala y reforzar las defensas a un ritmo apropiado para la empresa. Para comenzar, las empresas deben descargar el *Plan maestro de defensa contra los programas de secuestro (ransomware)* a fin de determinar qué salvaguardias se recomienda adoptar. En este documento se describen las salvaguardias, así como las funciones conexas del Marco de Ciberseguridad del NIST, y se presentan varias herramientas y recursos que pueden facilitar la implementación.

Además, hay muchas más herramientas y recursos que pueden facilitar la adopción de medidas esenciales de ciberhigiene en las empresas. Por ejemplo, es posible que algunas empresas ya estén usando un marco de seguridad y duden en introducir otro diferente. Afortunadamente, el CIS ha establecido una correlación con otros marcos de seguridad (por ejemplo, el marco del NIST y la Certificación del Modelo de Madurez de Ciberseguridad) y proporciona estas correlaciones libremente a todas las empresas por medio del Navegador de controles CIS y CIS WorkBench. Las empresas que quieran saber más acerca de los controles CIS específicamente y cómo comenzar a aplicar este plan maestro pueden consultar los siguientes recursos:

- Especificación para la evaluación de los controles CIS: explica qué debe medirse para comprobar que las salvaguardias CIS se hayan aplicado correctamente.
- Herramienta de autoevaluación de los controles CIS (CIS CSAT): se usa para evaluar y monitorear la aplicación de los controles CIS.
- Método CIS para la evaluación de riesgos (CIS RAM) v2.1: método para evaluar los riesgos de la seguridad de la información que ayuda a las empresas a implementar y evaluar su postura de seguridad comparándola con los controles CIS.

En el apéndice C de este documento se presentan otros recursos confiables. Como ya se dijo, la meta no es alcanzar la perfección. Todo paso adelante es fundamental para avanzar en la adopción de medidas esenciales de ciberhigiene. Defenderse de programas de secuestro y de las ciberamenazas en general no es tarea fácil, pero es una tarea muy necesaria para reforzar la postura de ciberseguridad de las empresas en todo el mundo. Nuestro Grupo de Trabajo confía en que las salvaguardias seleccionadas facilitarán la defensa contra programas de secuestro y otros ciberataques y ayudarán a sentar una base firme para una ciberdefensa eficaz.

Apéndice A. Plan maestro de defensa contra los programas de secuestro (*ransomware*)

Categoría	Número de salvaguardia CIS	Función de seguridad del NIST	Título de la salvaguardia CIS	Tipo
Identificar				
Conozca su entorno	1.1	Identificar	Hacer y mantener un inventario detallado de activos de la empresa	Básica
	2.1	Identificar	Hacer y mantener un inventario de programas informáticos	Básica
	2.2	Identificar	Verificar que los programas informáticos autorizados sigan vigentes	Accionable
	3.1	Identificar	Establecer y mantener un proceso de gestión de datos	Básica
	5.1	Identificar	Hacer y mantener un inventario de cuentas	Básica
Proteger				
Configuraciones seguras	4.1	Proteger	Establecer y mantener un proceso de configuración segura	Básica
	4.2	Proteger	Establecer y mantener un proceso de configuración segura para la infraestructura de la red	Básica
	4.4	Proteger	Instalar y administrar un cortafuegos en los servidores	Accionable
	4.7	Proteger	Administrar las cuentas por defecto en los activos y los programas informáticos de la empresa	Accionable
Gestión de cuentas y del acceso	5.2	Proteger	Usar contraseñas únicas	Accionable
	5.3	Proteger	Inhabilitar las cuentas inactivas	Accionable
	5.4	Proteger	Restringir los privilegios de administrador a las cuentas para uso exclusivo del administrador	Accionable
	6.1	Proteger	Establecer un proceso para otorgar acceso	Básica
	6.2	Proteger	Establecer un proceso para revocar el acceso	Básica
	6.3	Proteger	Exigir la autenticación de múltiples factores para aplicaciones con acceso externo	Accionable
	6.4	Proteger	Exigir la autenticación de múltiples factores para el acceso remoto a la red	Accionable
	6.5	Proteger	Exigir la autenticación de múltiples factores para el acceso administrativo	Accionable
Planificación de la gestión de vulnerabilidades	7.1	Proteger	Establecer y mantener un proceso de gestión de vulnerabilidades	Básica
	7.2	Proteger	Establecer y mantener un proceso de corrección	Básica
	7.3	Proteger	Automatizar la gestión de parches del sistema operativo	Accionable
	7.4	Proteger	Automatizar la gestión de parches de las aplicaciones	Accionable
	12.1	Proteger	Mantener actualizada la infraestructura de la red	Accionable
Defensa contra programas maliciosos	9.1	Proteger	Usar solo navegadores y clientes de correo electrónico que estén plenamente vigentes	Accionable
	9.2	Proteger	Usar servicios de filtrado de DNS	Accionable
	10.1	Proteger	Instalar y mantener programas antimalware	Accionable
	10.2	Proteger	Configurar la actualización automática de definiciones de antimalware	Accionable
	10.3	Proteger	Desactivar el inicio automático y la reproducción automática de medios extraíbles	Accionable
Concientización de seguridad y capacitación	14.1	Proteger	Establecer y mantener un programa de concientización de seguridad	Básica
	14.2	Proteger	Enseñar al personal a reconocer ataques de ingeniería social	Accionable
	14.6	Proteger	Enseñar al personal a reconocer y notificar incidentes de seguridad	Accionable
Detectar				
Responder				
Recuperación de datos y respuesta a incidentes	17.1	Responder	Designar personal que se ocupe del manejo de incidentes	Accionable
	17.2	Responder	Obtener y mantener información sobre contactos para la notificación de incidentes de seguridad	Accionable
	17.3	Responder	Establecer y mantener un proceso de notificación de incidentes en la empresa	Básica
	8.1	Responder	Establecer y mantener un proceso de gestión de registros de operaciones	Básica
	8.2	Responder	Recopilar registros de operaciones	Accionable
	8.3	Responder	Almacenar los registros de operaciones de una manera adecuada	Accionable
Recuperar				
Recuperación de datos y respuesta a incidentes	11.1	Recuperar	Establecer y mantener un proceso de recuperación de datos	Básica
	11.2	Recuperar	Hacer copias de seguridad automáticas	Accionable
	11.3	Recuperar	Proteger los datos de recuperación	Accionable
	11.4	Recuperar	Establecer y mantener una instancia aislada de datos de recuperación	Accionable

Apéndice B. Abreviaturas y siglas

CIS	*Center for Internet Security* (Centro para la Seguridad de Internet)
CISA	*Cibersecurity and Infrastructure Security Agency* (Agencia de Ciberseguridad y Seguridad de la Infraestructura)
CMMC	*Cibersecurity Maturity Model Certification* (Certificación del Modelo de Madurez de Ciberseguridad)
Controles CIS	Controles críticos de seguridad del Centro para la Seguridad de Internet
DNS	*Domain Name System* (Sistema de Nombres de Dominio)
MITRE ATT&CK	*MITRE Adversarial Tactics, Techniques, and Common Knowledge* (Tácticas Adversarias, Técnicas y Conocimiento Común de MITRE)
MS-ISAC	*Multi-State Information Sharing and Analysis Center* (Centro Multiestatal de Intercambio y Análisis de Información)
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Normas y Tecnología)
pymes	pequeñas y medianas empresas
URL	*uniform resource locator* (localizador uniforme de recursos, es decir, la dirección de un sitio web)
USB	*universal serial bus* (bus universal en serie)

Apéndice C. Recursos suplementarios

Controles críticos de seguridad del Centro para la Seguridad de Internet (CIS Controls) v8: contiene más información sobre los controles CIS; explica cómo empezar y por qué cada control es crítico; presenta los procedimientos y las herramientas que se deben usar para la implementación y una lista completa de salvaguardias para cada control.

Especificación para la evaluación de los controles CIS: explica qué debe medirse para comprobar que las salvaguardias CIS se hayan aplicado correctamente.

Navegador de controles CIS: muestra la correlación de los controles y las salvaguardias con otras normas de seguridad (por ejemplo, CMMC, NIST SP 800-53 Rev. 5, MITRE ATT&CK).

Herramienta de autoevaluación de los controles CIS (CIS CSAT): se usa para evaluar y monitorear la aplicación de los controles CIS.

Modelo de Defensa Comunitaria CIS (CDM) v2.0: guía publicada por el CIS que aprovecha la amplia disponibilidad de resúmenes completos de ataques e incidentes de seguridad y utiliza el marco MITRE ATT&CK, ecosistema refrendado por la industria.

Método CIS para la evaluación de riesgos (CIS RAM) v2.1: método para evaluar los riesgos de la seguridad de la información que ayuda a las empresas a implementar y evaluar su postura de seguridad comparándola con los controles CIS.

Membresía en SecureSuite de CIS: acceso a CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks y más. *Membresía gratuita para gobiernos estatales, locales, tribales y territoriales*.

CIS Benchmarks™: directrices para la configuración segura de más de 100 tecnologías, entre ellas sistemas operativos, aplicaciones y dispositivos de la red.

Guía conjunta de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) y el Centro Multiestatal de Intercambio y Análisis de Información (MS-ISAC®) sobre Programas de Secuestro: mejores prácticas y recomendaciones sobre programas de secuestro basadas en los conocimientos de la CISA y el MS-ISAC®.

CISA | Stop Ransomware: ventanilla única del Gobierno de Estados Unidos para poner fin a los programas de secuestro.

Cyber Readiness Institute | Ransomware Playbook: cómo prepararse para hacer frente un ataque de secuestro, responder y recuperarse.

Guías de implementación técnica de seguridad de la Agencia de Sistemas de Información de Defensa (DISA STIG): normas para la configuración elaboradas por la Agencia de Sistemas de Información de Defensa.

Membresía en el Centro de Intercambio y Análisis de Información sobre la Infraestructura Electoral (EI-ISAC®): gratuita para todas las entidades estatales, locales, tribales y territoriales que trabajan con funcionarios electorales de Estados Unidos y sus asociaciones.

Buró Federal de Investigaciones (FBI) | Hoja informativa sobre programas de secuestro: qué son los programas de secuestro y qué hacer al respecto.

Global Cyber Alliance (GCA) | Herramientas de ciberseguridad para pequeñas empresas: herramientas gratuitas y eficaces que se pueden usar hoy mismo para tomar medidas de inmediato a fin de reducir el ciberriesgo.

Instituto para la Seguridad y la Tecnología (IST) | Informe del Grupo de Trabajo sobre Programas de Secuestro: Marco de acción integral: principales recomendaciones del Grupo de Trabajo sobre Programas de Secuestro.

Membresía en el MS-ISAC: gratuita para los 50 estados, el Distrito de Columbia, los territorios de Estados Unidos, gobiernos locales y tribales, escuelas públicas primarias y secundarias, instituciones públicas de enseñanza superior, autoridades y otras entidades públicas no federales de Estados Unidos.

Marco de Ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST): https://www.nist.gov/cyberframework.

Rincón del NIST para la Ciberseguridad de las Pequeñas Empresas, página sobre programas de secuestro: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/programas de secuestro.