Reducción de los riesgos de ciberseguridad en los puntos finales de la organización

Mejores Prácticas en Ciberseguridad

B.05

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título *Recomendaciones de defensa: Reducción de riesgos cibernéticos en los puntos finales de la organización.* © (2018) Dirección Nacional de Ciberseguridad de Israel.

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad en idioma hebreo. Su traducción al idioma español fue realizada por el equipo de ciberseguridad de la división de Innovación para Servir al Ciudadano (IFD/ICS) del Banco Interamericano de Desarrollo (BID), y se incluye como capítulo de la colección "Mejores Prácticas en Ciberseguridad".

El lector debe tener presente que la ciberseguridad es un campo que evoluciona rápidamente. Aunque estos documentos reflejan principios establecidos, podrían actualizarse periódicamente según sea necesario para reflejar los avances en este campo. Adicionalmente, aunque se ha hecho lo posible para presentar las recomendaciones y recursos de manera que sean universalmente aplicables a las organizaciones de todo el mundo, el lector puede encontrar referencias que son específicas al ecosistema cibernético y contexto de Israel (tales como las sumas indicadas en Nuevos Shekels Israelíes [NIS], o las referencias a la normativa israelí o a sus organismos gubernamentales).

El documento original se encuentra disponible en el siguiente link: **https://www.gov.il/he/pages/endstation**. Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

"El presente documento ha sido redactado por el Plan Cibernético Nacional para beneficio del público. Constituye una recomendación para todas las organizaciones de la economía israelí. Puede utilizarse libremente para incrementar la ciberresiliencia en la economía. Ha sido redactado para ejecutivos de corporaciones, gerentes, directores de ciberprotección y profesionales informáticos, entre otros. El documento presenta las exigencias mínimas de defensa requeridas de acuerdo al potencial de daños. Las organizaciones deben llevar a cabo un proceso de evaluación de riesgos; a continuación, podrán elaborar un estricto plan de protección a partir de los requisitos expuestos en este documento. El documento ha sido concebido para todas las actividades económicas. Ha sido redactado utilizando el género masculino únicamente por una cuestión de comodidad. Debido a la naturaleza técnica de algunas recomendaciones, se requiere que sean implementadas por profesionales especializados y con experiencia. Puede enviar sus observaciones y comentarios relacionados con el documento por correo electrónico a tora@cyber.gov.il."

Índice

Prólogo

La transformación digital y el reto de la ciberseguridad

A medida que la transformación digital continúa expandiéndose por todo el mundo, los gobiernos, las organizaciones, los individuos e incluso los objetos están cada vez más conectados a Internet. Aunque la digitalización ha demostrado ofrecer beneficios innegables, como la prestación eficiente de servicios públicos, el crecimiento económico y la conectividad esencial para el desarrollo de innumerables actividades, también contribuye a una creciente exposición colectiva a los riesgos de ciberseguridad. Un importante motor de este fenómeno en los últimos tiempos ha sido la pandemia mundial de la COVID-19. Como resultado de las generalizadas políticas de distanciamiento social, el número de transacciones de comercio electrónico y las comunicaciones personales en línea experimentaron un crecimiento repentino y pronunciado en un corto período de tiempo, junto con el número de empleados que comenzaron a teletrabajar por primera vez. En esta situación sin precedentes, muchos usuarios de Internet se enfrentaron a nuevas interacciones en línea sin ser suficientemente conscientes de los riesgos de seguridad que estas conllevan. Las organizaciones también tuvieron que adaptarse rápidamente a los desafíos, estableciendo flujos de trabajo totalmente remotos, a menudo sin contar con todas las medidas de seguridad necesarias ni con la orientación adecuada para los empleados.

Sin duda, los ciberdelincuentes no tardaron en explotar la incertidumbre y vulnerabilidad de los usuarios desprevenidos. Proliferaron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se detectaron casi un millón de intentos de ataque diarios contra las conexiones del protocolo de escritorio remoto (RDP), ampliamente utilizado entre las organizaciones para las conexiones remotas de los empleados. De hecho, los ataques al RDP fueron la forma más popular de ciberataque, superando incluso a los correos electrónicos de *phishing*. Durante la segunda mitad del año, a medida que más organizaciones reforzaban la seguridad de sus plataformas remotas, los *hackers* centraron sus esfuerzos en explotar las vulnerabilidades de los activos privados de los empleados y los dispositivos de acceso remoto para penetrar en sus organizaciones. Aunque estas amenazas se vieron maximizadas por este contexto global, no son novedosas ni desaparecerán; las personas siguen viviendo en un entorno de riesgo elevado, que es especialmente grave en regiones del mundo donde las políticas y tecnología de ciberseguridad están menos desarrolladas, y donde falta educación y concienciación ciudadana en torno a este tema. En otras palabras, aunque los cambios debidos a la pandemia de la COVID-19 acabarán por asentarse, estos han evidenciado la urgente necesidad de reforzar las protecciones individuales y colectivas contra los riesgos cibernéticos.

Reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, promover la confianza de las personas en las tecnologías digitales y apoyar el crecimiento económico mediante una transformación digital segura. En particular, los ciudadanos deben tener la seguridad de que los sistemas digitales que utilizan para sus actividades personales o profesionales, y también los que involucran sus datos personales, cuentan con las medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de su información y de los servicios de los que dependen. Además, los fallos de ciberseguridad tienen un impacto económico importante. Un reciente informe de McAfee estimó que la ciberdelincuencia cuesta a la economía mundial unos US$600.000 millones anuales, es decir, el 0,8% del producto interno bruto (PIB) global.

Israel, líder en ciberseguridad a nivel mundial

El ecosistema de innovación y emprendimiento de Israel es reconocido globalmente como uno de los más vibrantes del mundo, lo cual le ha ganado el nombre de *Startup Nation*. Según los indicadores de ciencia y tecnología de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de marzo de 2021, Israel es el país de la OCDE que invierte un mayor porcentaje de su PIB (4,9%) en investigación y desarrollo (I+D). Cuenta con un total de más de 300 centros de innovación, investigación y desarrollo de compañías multinacionales; de ellos, docenas están dedicadas a la ciberseguridad.

No es sorpresa entonces que el 40% de la inversión privada a nivel mundial en ciberseguridad tenga lugar en Israel, que posee también el segundo ecosistema privado más grande del mundo en esta área después de Estados Unidos. Según datos de 2021, durante ese año se invirtieron US$8,8 billones en alrededor de 131 compañías israelíes del sector, y más de 40 fueron adquiridas por un total de US$3,5 billones. El país cuenta con más de 500 *start-ups* de ciberseguridad y, en 2021, el 33% de la población de "unicornios" del mundo eran israelíes. En total, se estimó su exportación de productos de ciberseguridad para 2020 en US$6,85 billones.

La Dirección Nacional de Ciberseguridad de Israel (INCD) es responsable de asegurar el ciberespacio nacional y de establecer y promover la resiliencia cibernética en el país. La INCD opera a nivel nacional para elevar constantemente el nivel de seguridad de las organizaciones y ciudadanos, prevenir y gestionar los ciberataques, y reforzar las capacidades de respuesta en caso de una emergencia cibernética. Su posición como parte de la oficina del Primer Ministro demuestra claramente la centralidad e importancia de sus competencias para el país. Sus objetivos también incluyen la preparación y capacitación del sector privado israelí y del público en general para protegerse de las ciberamenazas mediante la adopción de tecnologías ciberseguras, la publicación de mejores prácticas, la formación del personal y el aumento de la concienciación. Se encarga además de establecer y reforzar la base científica y tecnológica de ciberseguridad mediante el desarrollo de un capital humano altamente cualificado, el apoyo a la investigación académica de vanguardia, la participación en una avanzada I+D tecnológica y el fomento de la ciberindustria. La INCD dedica sus esfuerzos a mantener un ciberespacio protegido, seguro y abierto para todos los habitantes y empresas del Estado de Israel y a facilitar su crecimiento y su base científica e industrial.

¿Cuál es el estado de la ciberseguridad en la región de América Latina y el Caribe?

El Banco Interamericano de Desarrollo (BID) realiza periódicamente estudios sobre la evolución de las capacidades de sus Estados miembros para defenderse de las crecientes amenazas en el ciberespacio. El *Reporte regional de madurez en ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe,* elaborado en colaboración con la Organización de los Estados Americanos (OEA), mostró que los países se encontraban en diferentes etapas de desarrollo en su preparación para enfrentar los desafíos de la ciberseguridad, pero en general aún tenían un amplio margen de mejora.

Mientras que, en 2016, año de la primera edición del informe, el 80% de los países de la región no contaba con una estrategia nacional de ciberseguridad, esta cifra se redujo al 60% en 2020. Además, solo unos pocos países gestionan la exposición de sus infraestructuras críticas —como energía, sanidad, telecomunicaciones, transporte, suministro de agua y finanzas— a ciberataques. Como revela el Reporte de 2020, solo siete de los 32 países evaluados contaban con un plan de protección cibernética de infraestructuras críticas. Esta es una de las conclusiones más preocupantes, si se tiene en cuenta el impacto catastrófico que los ataques a estos sectores podrían tener no solo en las economías nacionales, sino en la vida de todos sus ciudadanos.

En cuanto a la capacidad de los países para gestionar y responder a los incidentes de ciberseguridad, el mismo estudio relevó que el 63% de los países contaba con equipos de respuesta a incidentes de seguridad, como Equipos de Respuesta a Emergencias Informáticas (CERT) o Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Sin embargo, de los 20 países que sí los tenían, solo tres habían alcanzado una madurez avanzada en su capacidad de coordinar dichas respuestas. De hecho, 23 de los 32 países se encontraban todavía en una fase inicial de madurez en este tema. Este hallazgo llamó la atención sobre la necesidad de que los países refuercen la capacidad de sus equipos para coordinar eficazmente sus respuestas a los ciberincidentes. Además, el informe examinó la disponibilidad de oportunidades educativas y de formación en ciberseguridad y descubrió que menos de la mitad de los países de la región ofrecían educación formal en ciberseguridad, como posgrados, maestrías o títulos técnicos. No hace falta decir que contar con suficientes profesionales formados es esencial para diseñar e implementar las políticas y medidas de ciberseguridad necesarias para garantizar la resiliencia de un país frente a ciberataques cada vez más sofisticados y complejos.

¿Qué hace el BID para apoyar a la región?

Durante los últimos años, el BID ha apoyado activamente a la región en el desarrollo de la capacidad en ciberseguridad, el diseño e implementación de una política pública de ciberseguridad a nivel nacional y el fortalecimiento de las capacidades sectoriales en ciberseguridad. Este apoyo adopta diversas formas. El BID ha puesto a disposición de los países de América Latina y el Caribe (ALC) asistencia financiera por valor de decenas de millones de dólares para desarrollar capacidades nacionales de ciberseguridad a través de más de 15 operaciones de inversión en el sector público, así como una importante financiación adicional para garantizar la ciberseguridad en los proyectos de inversión en transformación digital.

También proporciona orientación técnica y lleva a cabo proyectos de ciberseguridad en toda la región en forma de consultorías, diagnósticos y proyectos de fortalecimiento de la ciberseguridad hechos a medida, en temas que incluyen la protección cibernética de infraestructuras críticas, cibercrimen y análisis forense, diseño y fortalecimiento de los CSIRT y de los Centros de Operaciones de Seguridad (SOC), y estrategias nacionales y sectoriales de ciberseguridad. Además, el BID ha realizado importantes esfuerzos para proporcionar oportunidades a los profesionales de ALC, a fin de reforzar y actualizar sus habilidades en este campo, ofreciendo regularmente talleres y actividades de formación. Estos han incluido cursos ejecutivos de ciberseguridad de dos semanas de duración, ofrecidos conjuntamente con la Universidad Hebrea de Jerusalén en Israel, así como cursos a medida sobre protección de infraestructuras críticas y otros dirigidos a sectores específicos. Por último, el BID ha elaborado varias publicaciones de gran impacto sobre cuestiones de ciberseguridad a nivel nacional y sectorial, y sigue actualizando y ampliando periódicamente este cuerpo de conocimientos.[1]

1. Véase el sitio del Clúster de Datos y Gobierno Digital (DDG) de la división Innovación para Servir al Ciudadano (ICS) de BID, disponible en: **https://www.iadb.org/es/reforma-modernizacion-del-estado/cluster-de-datos-y-gobierno-digital**.

El BID y la INCD: uniendo esfuerzos

Los retos de la ciberseguridad, como los de la propia Internet, son de naturaleza global, por lo que compartir el conocimiento y herramientas para afrontarlos beneficia a la población en su conjunto. Reconociendo esta realidad, la INCD y el BID se han asociado para poner la experticia israelí a disposición de los países de ALC. La colaboración entre ambas instituciones ha proporcionado un fuerte apoyo a la región, en forma de capacitaciones ejecutivas y técnicas sobre temas avanzados de ciberseguridad, conferencias de vanguardia para funcionarios públicos de ALC y profesionales en el campo, y proyectos innovadores de asistencia técnica. La presente publicación es un producto más de esta colaboración. Consiste de una serie de guías metodológicas de ciberseguridad para organizaciones desarrollada por la INCD a la luz de su análisis sobre riesgos, métodos de ataque, incidentes cibernéticos y estándares globalmente aceptados. Estas guías han sido traducidas al español y al inglés, en una actividad conjunta de ambas organizaciones, con el objetivo de permitir el acceso a este cuerpo de conocimiento por parte de audiencias de toda la región de ALC, y así contribuir a aumentar su resiliencia cibernética.

Esta colección ofrece una orientación práctica sobre una serie de cuestiones metodológicas y técnicas relevantes para el fortalecimiento de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

El reto de proteger el espacio digital seguirá creciendo, junto con la necesidad de contar con experiencia probada para afrontarlo. Las reflexiones aquí contenidas pretenden servir como recurso para potenciar la tan necesaria formación profesional en ciberseguridad que se observa actualmente en ALC. Estas guías contribuirán a elevar los estándares organizacionales, a promover mayor conciencia y cultura de ciberseguridad dentro de las organizaciones y en el público en general, y a informar a los tomadores de decisiones, gerentes y líderes en sus iniciativas de ciberseguridad. Confiamos en que estas guías servirán de hoja de ruta para los profesionales y líderes de ALC, trabajando juntos para construir un futuro más seguro y próspero.

Finalidad de la publicación

La finalidad de la presente publicación es recomendar medidas que permitan proteger los puntos finales (*endpoints*), mediante la creación de los siguientes circuitos de seguridad: seguridad física y denegación de acceso, privilegios, protección de la información y *software* de seguridad.

Las recomendaciones de la publicación pueden implementarse en computadoras fijas de la organización, en computadoras portátiles y también cuando se conecten a la red empresarial puntos finales que no sean propiedad de la organización (como cuando en la empresa existe una política de "traiga su propio dispositivo" [BYOD, por sus siglas en inglés]).

La publicación hace referencia de forma general a puntos finales dondequiera que estos estén, independientemente del sistema operativo. Sin embargo, la mayoría de las muestras y capturas de pantalla se han tomado del sistema Windows, que es el sistema operativo más común para puntos finales.[2]

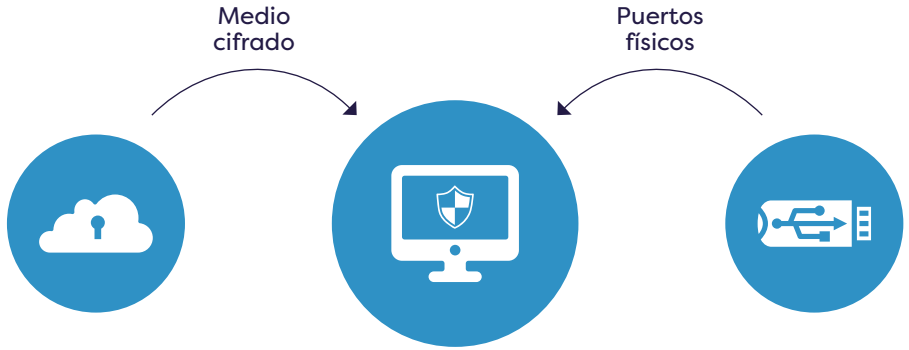
2. Puede accederse a las reglas de securización del sistema Windows en: **https://learn.microsoft.com/es-mx/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines**. Pueden encontrarse las reglas de securización del punto final con Linux en: **https://www.networkworld.com/article/957793/linux-hardening-a-15-step-checklist-for-a-secure-linux-server.html**.

Grupo destinatario

La publicación está dirigida a ejecutivos de empresas, gerentes informáticos y gerentes de seguridad de la información que deseen mejorar el nivel de seguridad de la información en su organización, mediante la mejora de la seguridad en los puntos finales. Debido a la naturaleza técnica de algunas recomendaciones, se requiere que sean implementadas por profesionales especializados y con experiencia.

Amenazas

Gráfico 1. Mapeo de acceso y oportunidades de ataque



El punto final es un objetivo atractivo para los atacantes y puede servir como "punto débil" para los ataques contra la organización. Aquí se hará referencia a las computadoras personales como puntos finales del empleado de la organización.

Los puntos finales de la organización pueden ser atacados de diversas formas (vectores de ataque) y con diferentes propósitos:

- Insertando un dispositivo de memoria física; por ejemplo, una unidad externa que contenga un *software* malicioso (*malware*).
- Vinculando el punto final a una red externa (por ejemplo, Internet).
- Mediante el robo del punto final (especialmente si es portátil).
- A través de un acceso no autorizado al punto final, pirateo físico o una combinación de *hardware* o *software*. Por ejemplo, al insertar un espía *keylogger* o introducir un troyano en el punto final con el propósito de robar su información o de saltar a otras computadoras en la organización, etcétera.

/01. Seguridad física y denegación de acceso

Principio de securización

La denegación de acceso no autorizado y la seguridad física son medidas básicas que deben implementarse a fin de proteger el punto final. Su propósito es evitar la pérdida o el robo de *hardware*, lo que puede causar un daño inmenso a la organización. Por lo tanto, deben aplicarse mecanismos de seguridad física a los puntos finales.

Proceso de securización

La protección física del punto final debe llevarse a cabo a diferentes niveles:

01

A nivel de recinto: el recinto de trabajo debe estar protegido y el acceso a este debe ser solo para personas autorizadas; por ejemplo, puede implementarse un sistema de control de acceso basado en etiquetas de proximidad.

Imagen 1. Sistema de control de acceso basado en etiquetas de proximidad

02

A nivel del punto final: uso de una jaula de seguridad o de un cable de seguridad como medio masivo y permanente en las estaciones de trabajo. Ello evita la desconexión y el robo del punto final de su lugar.

Imagen 2. Cable de seguridad para el punto final

03

Implementación de un mecanismo automático para bloquear el punto final, después de un período determinado de inactividad.

04

Debe asegurarse de que los empleados firmen y se comprometan con los procedimientos apropiados para proteger y vigilar el punto final (por ejemplo, bloquear el equipo con una contraseña, impedir el acceso al área de trabajo, etc.).

¡Atención! Asegúrese de que haya una política de mantenimiento de la seguridad física en la organización.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Protección física y ambiental** > 18.1

/02. Acceso y privilegios

Arranque seguro

01

Principio de securización: el arranque seguro (*Secure Boot*) es una función implementada en las computadoras (PC) que carga el sistema operativo una vez firmado y aprobado. Ello evita que *malwares* del tipo *rootkit* se activen y controlen el punto final. Debe asegurarse de que la organización solo utilice sistemas operativos que sean compatibles con *Secure Boot*.

02

Proceso de securización: por lo general, cuando se instalan sistemas operativos, la función de arranque seguro está habilitada de forma predeterminada. Para evitar que un *malware* de tipo *rootkit* tome el control del punto final, se recomienda no cambiar esta configuración.[3]

¡Atención! Se recomienda no desactivar la configuración predeterminada del sistema operativo relacionada con la protección de este. Este cambio en la configuración tiene consecuencias a nivel de seguridad de los puntos finales.

Cifrado del disco duro

01

Principio de securización: los puntos finales en general, y las computadoras portátiles en particular, corren riesgo de robo, pérdida u olvido, lo que podría facilitar el acceso a la información almacenada en ellas a una persona no autorizada. El cifrado del disco hace que la información que contiene sea ilegible para quienes no tengan la clave de cifrado y reduce significativamente el riesgo de fugas de información.

02

Proceso de securización: para los propietarios de puntos finales que utilizan el sistema operativo Microsoft Windows, el fabricante proporciona un *software* de cifrado de disco llamado **BitLocker**. Además, existen soluciones de otros fabricantes.

Para los propietarios de puntos finales con Linux, existe una herramienta de código abierto para el cifrado del disco.

De manera similar, la compañía Apple ofrece una solución llamada **FileVault** para el cifrado del disco en computadoras basadas en su sistema operativo.

¡Atención! Debe asegurarse de que la solución cifre todo el disco para que no se filtre información del punto final en caso de robo o pérdida.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Cifrado >** 8.7

Limitación de privilegios

01

Principio de securización: las cuentas con privilegios amplios (cuentas privilegiadas o de administrador) son unos de los principales objetivos de los ciberatacantes, ya que permiten que quienes acceden a ellas tomen control del punto final y, desde allí, de toda la red. Una de las primeras medidas para reducir la superficie de ataque es crear una cuenta de usuario "común" con privilegios limitados, que sea utilizada para el trabajo diario.[4]

Una cuenta con privilegios de administrador solo debe utilizarse cuando sea necesario, por ejemplo, al instalar un *software*. Esto se debe a que, si el *malware* o un atacante llegan al punto final, el usuario con privilegios limitados dificulta que el atacante obtenga privilegios de administrador para realizar cambios extensos en el sistema y obtener una base en el punto final.

3. **https://learn.microsoft.com/es-mx/windows-hardware/manufacture/desktop/disabling-secure-boot**.

4. Más información en CIS Control 6, disponible en: **https://www.cisecurity.org/controls/access-control-management**.

02

Proceso de securización

- Debe limitarse al mínimo el número de cuentas de administrador en el punto final (consulte el apartado **Protección del administrador local (*Local Admin*) en los puntos finales** sobre cómo configurar adecuadamente una cuenta de administrador).
- El titular del punto final no debe definirse como un administrador local, sino como un usuario "común".
- Las operaciones en el punto final debe realizarlas un usuario con los niveles de privilegios más bajos posible para llevar a cabo dicha operación. En el caso de acciones que requieran el uso de un usuario con privilegios altos, se hará únicamente para esta acción específica. Es posible utilizar sistemas para elevar el nivel de privilegios, según sea necesario.
- Se recomienda monitorear y emitir alertas sobre cualquier cambio o adición de cuentas con privilegios altos.

¡Atención! Los privilegios en la organización deben ajustarse a las necesidades de las distintas funciones (y se debe otorgar un mínimo de privilegios a cada una de dichas funciones).

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Control de acceso >** 4.9 y 4.10

Política de contraseñas

01

Principio de securización: una de las primeras y más comunes técnicas de piratería por parte de una entidad maliciosa contra una organización consiste en intentar un ataque contra el mecanismo de contraseñas de la red empresarial.

Eludir el mecanismo de contraseña reducirá la necesidad de invertir recursos y tiempo para piratear otros mecanismos, tales como privilegios, sistemas o cifrado. Por lo tanto, el objetivo es hacer que al atacante le resulte más difícil atacar el mecanismo de contraseña.

Una contraseña difícil de descifrar hará que un atacante no pueda adivinarla en un período de tiempo razonable. Elegir una buena contraseña no dejará al pirata informático otra opción que probar todas las contraseñas posibles mediante la búsqueda por fuerza bruta, lo que aumenta el tiempo requerido para descifrarla o lo hará fallar por completo.

¿Lo sabía?

El término fuerza bruta (*brute force*) hace referencia a un proceso o algoritmo, que opera por medio de la prueba y error de todas las posibilidades para resolver un problema dado hasta encontrar la solución correcta.

Ataque de diccionario (*dictionary attack*) es otro nombre que recibe el uso de *software* para adivinar la contraseña de un usuario. Se trata de un intento de adivinar por medio de fuerza bruta la contraseña del usuario, es decir, se experimenta y se prueba con todas las contraseñas posibles, las más probables o las más comunes, para lo que se utilizan por lo general archivos que contienen largas lista de contraseñas de este tipo. Un atacante también puede encontrar estas listas en Internet.

02

Proceso de securización: reglas básicas para elegir una contraseña.

- Como regla general, no confíe únicamente en la contraseña. Es recomendable incorporar un mecanismo de verificación adicional, como la verificación en dos pasos.[5]
- No utilice los datos del usuario en la contraseña, como el nombre, el apellido, la fecha de nacimiento, el número del documento de identidad, el número de teléfono, etc.
- La contraseña debe tener al menos ocho caracteres.
- Debe establecerse una contraseña que contenga letras, caracteres especiales y números.
- Deben evitarse las palabras estándar.
- Debe establecerse claramente en los procedimientos de la organización que la contraseña es personal y que no debe compartirse ni transferirse a nadie.

Nota: Existen varios enfoques y recomendaciones; por ejemplo, las recomendaciones del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés) para frases de contraseñas (*passphrases*).[6]

Política para hacer cumplir el cambio de contraseña:

- Debe cambiarse la contraseña cada 90 días.
- No deben usarse nuevamente las contraseñas utilizadas con anterioridad.
- Debe establecerse el bloqueo de usuario después de cinco errores.

Es importante asegurarse de que el administrador de la red aplique la política de contraseñas establecida por la organización a nivel de red (dominio) y que haga uso de objetos de directiva de grupo (GPO, por sus siglas en inglés), a fin de hacer cumplir dicha política en toda la red empresaria.

Verificaciones trimestrales, que puede realizarlas el Director de Seguridad de la Información (CISO, por sus siglas en inglés) o el Help Desk para la política de Active Directory (AD), a fin de verificar que el usuario cumple con la política establecida:

- Campo **"Contraseña requerida"**: asegúrese de que todos los usuarios deban identificarse con una contraseña.
- Campo **"Último cambio de la contraseña"**: verifique que no haya registros de contraseñas en los cuales la fecha sea de más de 90 días en el pasado.
- Campo **"La contraseña vencerá en"**: compruebe si existen usuarios con una configuración que no requiera un cambio de contraseña.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Control de acceso >** 4.35

¡Atención! Es importante asegurarse de que el proceso de gestión de contraseñas en la organización cumpla con la política de contraseñas establecida para dificultar el hackeo y evitar el uso indebido de esos datos.

5. Para obtener más información, consulte el documento ***Autenticación multifactor avanzada ante amenazas de ciberseguridad***, de próxima publicación dentro de esta serie de guías de buenas prácticas en ciberseguridad.
6. **https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd**.

Protección del administrador local (*Local Admin*) en los puntos finales

01

Principio de securización: los privilegios del tipo administrador local (*Local Admin*) en los puntos finales permiten un control casi completo sobre dichos puntos, lo que expone la red empresarial a un mayor riesgo.

El administrador local obtiene acceso a todos los archivos y aplicaciones de la red. Cuando se encuentra con algún problema de privilegios, puede otorgarse a sí mismo el privilegio solicitado sin ningún control por parte del administrador de la red. Esto conlleva el riesgo de que el punto final quede expuesto a cualquier acción que el atacante elija realizar.

Por lo general, los sistemas operativos crean automáticamente una cuenta de administrador, por lo que esta cuenta es conocida entre los atacantes y constituye un punto débil en la organización.

¡Importante! Antes de deshabilitar o renombrar una cuenta de administrador, asegúrese de tener otro nombre de usuario con privilegios sólidos por si fuese necesario.

02

Proceso de securización: la cuenta de administrador puede protegerse de varias formas:

- Manualmente: en organizaciones pequeñas, es posible establecer para cada punto final un nombre de usuario alternativo para un administrador local.
- Ejecutando un *script* después de la instalación.[7]
- Por medio de GPO.

Usuario señuelo o tarro de miel (*honeypot*)

01

Principio de securización: el usuario señuelo es un usuario ficticio, localizado en la red de la organización con detalles también ficticios. Su función es atraer al atacante potencial a que entre en el tarro de miel (*honeypot*).[8]

7. Para hacerlo, pueden seguirse los pasos descritos en: **https://learn.microsoft.com/es-mx/powershell/module/microsoft.powershell.localaccounts/rename-localuser?view=powershell-5.1&viewFallbackFrom=powershell-5.1localuser%3Fview%3Dpowershell-5.1**.
8. **https://www.linkedin.com/pulse/honeypots-security-managers-guide-ismail-orhan-ceh**.

Un atacante que trate de piratear una organización, normalmente intentará localizar tantos nombres de usuario como sea posible para obtener una selección de privilegios de conexión a la organización, a fin de llegar a un nombre de usuario con privilegios altos. El usuario señuelo está diseñado para tender una trampa al atacante. Al caer en ella, se activará una alerta. Para que este usuario sea efectivo, no debe posibilitarse la conexión/identificación con el nombre de usuario anteriormente mencionado y, por lo tanto, cuando se haga un intento de identificación, se recibirá una alerta de inmediato y será posible saber casi con total certeza que se ha producido un intento de infiltrarse en la organización.

02

Proceso de securización: a continuación, figuran los pasos a seguir para crear un usuario señuelo:

- En primer lugar, debe crearse un nombre de usuario señuelo creíble, mas no debe permitirse la conexión con el nombre de usuario anterior (de manera completa).[9]
- Deben crearse usuarios locales señuelos y usuarios de red (usuarios de dominio).
- El usuario señuelo debe contar con todos los privilegios legítimos en la organización, para que el nombre de usuario no despierte las sospechas del atacante.
- El nombre del usuario señuelo debe configurarse en el *software* diseñado para detectar nombres de usuario de tipo señuelo, de modo que el *software* advierta cuando se produce la conexión.

¡Atención!

El uso de un usuario señuelo puede ayudar a la organización a reducir el tiempo necesario para detectar un ataque. La condición para ello es que se planifique correctamente y que haya un proceso de seguimiento y mantenimiento del entorno de "trampa".

Cuantos más nombres de usuario del tipo señuelo utilice la organización, más probable será detectar que se trata de un ataque.

9. **https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey.pdf**.

/03. Protección de la información

Copia de seguridad de la información

01

Principio de securización: como ya se ha mencionado, los puntos finales en las organizaciones pueden contener mucha información sensible, por lo que pueden verse perjudicadas por errores humanos (eliminación accidental de información) o por un ciberataque. Por ejemplo, uno de los ataques más comunes son los llamados *ransomware*: un *software* malicioso que inhabilita la información existente en el punto final por medio de un cifrado, tras lo cual los atacantes no permiten el acceso a la información sin pagar un rescate. A veces, incluso después de realizar el pago, no es posible acceder a la información y esta se pierde.

Además de utilizar antivirus, la forma más eficaz de hacer frente a este tipo de ataque es hacer una copia de seguridad de la información. Toda la información esencial para la organización debe estar respaldada por medios que permitan su recuperación en caso de producirse daños en el punto final.[10]

02

Proceso de securización: la forma de hacer frente a los ataques del tipo *ransomware* es hacer una copia de seguridad de la información por medios externos: en una unidad de red, una unidad externa o una copia de seguridad en la nube. El dispositivo debe estar conectado al punto final solo durante el tiempo de respaldo. El resto del tiempo, este dispositivo debe estar permanentemente desconectado del punto final para no sufrir daños en caso de intrusión.

03

Aspectos importantes

- Deben asignarse medios físicos dedicados especialmente a generar una copia de seguridad, por ejemplo, servidor, nube de respaldo, unidad de red.
- Debe establecerse una instancia, equipo o individuo responsable del respaldo de la información en la organización.
- Debe definirse una política de respaldo periódico de la información en la organización (diaria, semanal, mensual).
- Debe realizarse una prueba de recuperación para verificar que la copia de seguridad sea efectiva.

¡Atención! Hacer una copia de seguridad de la información ayudará a recuperarse en caso de que se pierda información de la organización y contribuirá a la continuidad comercial.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Continuidad del negocio**

Prevención de fugas de datos (DLP, por sus siglas en inglés)

01

Principio de securización: los empleados de la organización pueden extraer información confidencial de la organización por medios como el correo electrónico y la copia a un dispositivo USB, entre otros.

La divulgación de información confidencial puede ocurrir intencionalmente o como resultado de un error humano. Por lo tanto, es muy importante que exista una capa de seguridad contra la fuga de datos de la organización. Las soluciones DLP ayudan a la organización a monitorear datos y, de acuerdo con políticas predeterminadas, bloquean la transferencia de información a partes no autorizadas, de manera de minimizar los incidentes de pérdida y fuga de datos confidenciales.[11]

Además, el sistema DLP puede documentar las acciones del usuario en el punto final y examinar las actividades sospechosas que pudiesen dañar a la organización, como vender información, cometer estafas y otras acciones maliciosas.

02

Proceso de securización: las siguientes son las acciones principales que deben considerarse.

- Establecer políticas de seguimiento y reglas pertinentes.
- Monitorear el acceso a información sensible y confidencial de la organización.

10. Más información en CIS Control 11, disponible en: **https://www.cisecurity.org/controls/data-recovery**.

11. Más información en CIS Control 3, disponible en: **https://www.cisecurity.org/controls/data-protection**.

- Supervisar la transferencia de información desde el punto final a algún dispositivo externo o a un correo electrónico externo.
- Instalar sistemas DLP.

Bloqueo de dispositivos

01

Principio de securización: el uso de dispositivos de memoria basados en USB es común en la actualidad. Estos dispositivos permiten copiar rápidamente la información de la PC a unidades externas, así como utilizar otros dispositivos extraíbles.

Por medio de estos dispositivos es posible infiltrar *malware* o virus en cualquier computadora que permita una conexión por USB. Para proteger la información confidencial de la organización, el acceso para conectar dichos dispositivos debe estar restringido en el punto final.

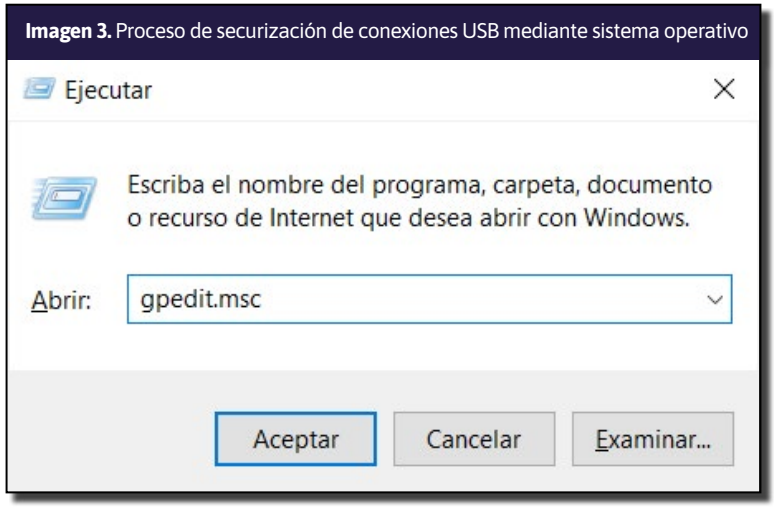
Existen dos puntos débiles para proteger el punto final: la computadora y los dispositivos externos o extraíbles que se utilicen.

02

Proceso de securización: existe una serie de procesos disponibles. El primero es la securización de las conexiones USB con la ayuda del sistema operativo de su computadora:

- Para comenzar, presione la tecla **`Inicio`** y luego, en la barra de búsqueda, introduzca: **`ejecutar`**.

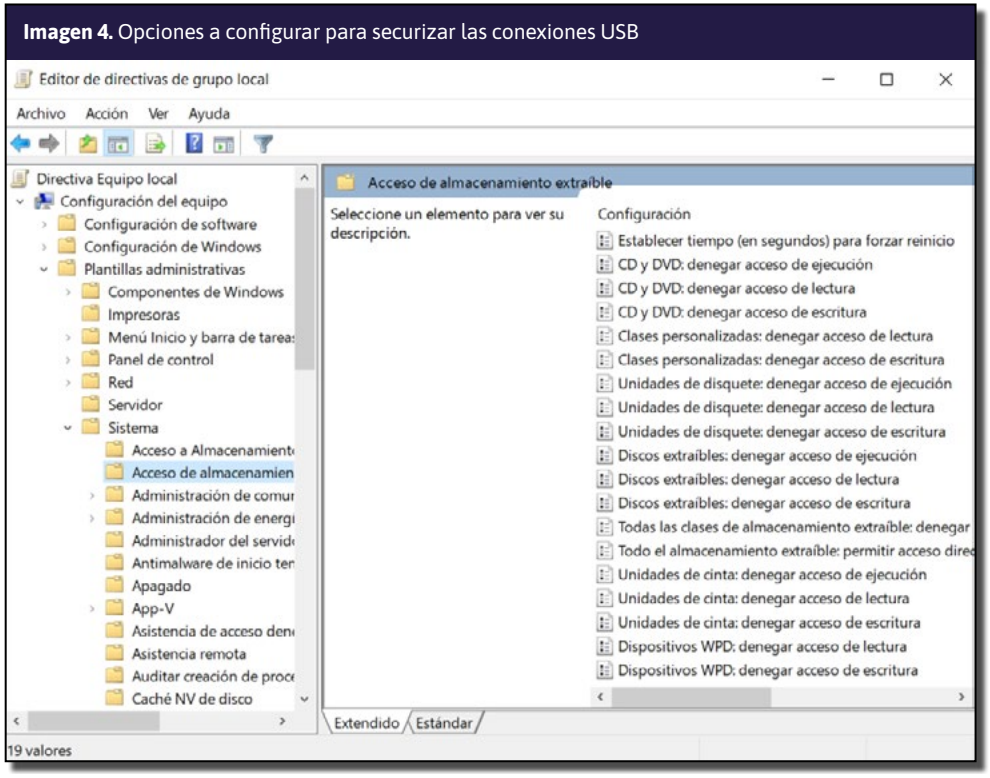
Imagen 3. Proceso de securización de conexiones USB mediante sistema operativo



- En la ventana que se abre, introduzca el comando **`gpedit.msc`** y a continuación haga clic en **`Aceptar`**.
- En la ventana que se abre, navegue hasta **`Configuración del equipo`** > **`Plantillas administrativas`**.
- Dentro de la carpeta **`Plantillas administrativas`**, primero seleccione la carpeta **`Sistema`**; luego seleccione la opción **`Acceso de almacenamiento extraíble`**.
- Ahora aparecerá un conjunto de opciones en el lado derecho de la ventana. De a uno por vez, haga doble clic y luego configure cada uno de los siguientes elementos:

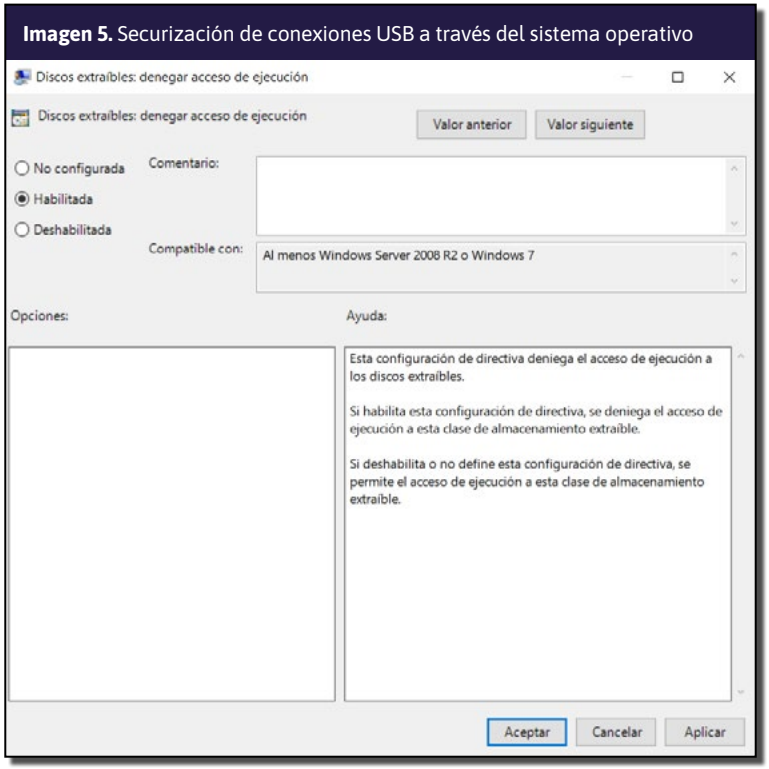
`Discos extraíbles: denegar acceso de ejecución`
`Discos extraíbles: denegar acceso de lectura`
`Discos extraíbles: denegar acceso de escritura`

Imagen 4. Opciones a configurar para securizar las conexiones USB



- Después de seleccionar un elemento, en la siguiente ventana seleccione la opción **Habilitada** y después haga clic en **Aceptar**.

Imagen 5. Securización de conexiones USB a través del sistema operativo



- Una vez hecho esto para los tres elementos listados anteriormente, reinicie la computadora.

El segundo es la remoción física:[12]

- Otra opción es remover o bloquear físicamente las unidades de disco y los puertos USB.

El tercero es la protección de dispositivos extraíbles:

- **AutoRun**: esta configuración activa automáticamente archivos desde dispositivos externos o extraíbles o abre un menú de opciones. En la práctica, el dispositivo contiene un archivo llamado **autorun.inf**, en el cual los atacantes pueden plantar un virus, que se activará mediante la ejecución automática de todos los archivos enumerados en el archivo **AutoRun**.

Por lo tanto, es importante securizar **AutoRun** de la siguiente manera:

- En las redes basadas en dominios de Microsoft, es posible configurar en GPO el bloqueo de dispositivos.

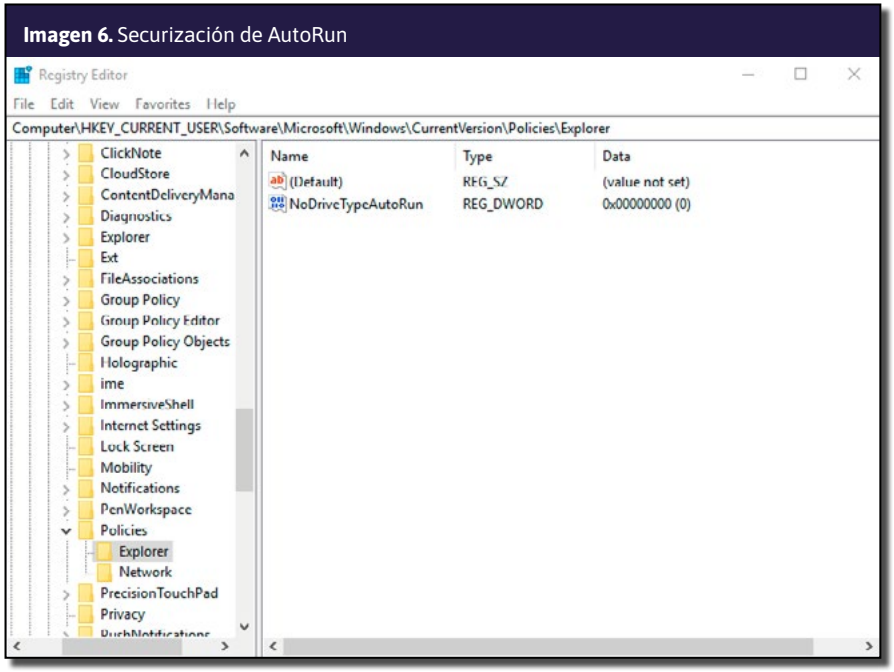
Además, el punto final puede securizarse localmente de la siguiente manera:

- Haga clic en la tecla **Inicio** y luego en la barra de búsqueda escriba: **ejecutar**.
- En la ventana que se abre, introduzca **regedit** y a continuación **Aceptar**.
- Acceda a la siguiente ruta:

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

- Haga clic con el botón derecho en la opción **NoDriveTypeAutoRun** y a continuación seleccione **Modify**.
- En la hilera **Value data**, cambie el valor a **0xFF**, y después **Aceptar**.
- Reinicie la computadora.

Imagen 6. Securización de AutoRun



12. De hecho, puede bloquear físicamente cualquier interfaz innecesaria en su computadora.

Tenga en cuenta que también es posible bloquear solo ciertos archivos según su origen utilizando los valores proporcionados en el cuadro 1:

Cuadro 1. Valores para el bloqueo de archivos AutoRun

Valor	Significado
0x1 o 0x80	Desactiva «AutoRun» en unidades de tipo desconocido
0x4	Desactiva «AutoRun» en unidades extraíbles
0x8	Desactiva «AutoRun» en unidades fijas
0x10	Desactiva «AutoRun» en unidades de red
0x20	Desactiva «AutoRun» en unidades CD-ROM
0x40	Desactiva «AutoRun» en discos RAM
0xFF	Desactiva «AutoRun» en todo tipo de unidades

03

Escaneo de dispositivos extraíbles: se aconseja escanear siempre los dispositivos extraíbles antes de copiar archivos hacia o desde ellos, y especialmente antes de activar archivos desde los mismos. Si el *software* antivirus instalado en la organización lo permite, se recomienda configurar un escaneo automático de cualquier dispositivo externo que se inserte en la computadora.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Seguridad de los soportes físicos** > 15.5

/04. *Software* de seguridad

Antivirus[13]

01

Principio de securización: el propósito del *software* antivirus es detectar virus y otros atacantes en el punto final y protegerlo de esas actividades.

En condiciones óptimas, el *software* podrá detectar un intento de ataque en el punto final antes de que la entidad maliciosa pueda alojarse en la computadora.

13. Más información en CIS Control 10, disponible en: **https://www.cisecurity.org/controls/malware-defenses**.

En el caso de que el equipo ya esté infectado con un archivo malicioso, el antivirus puede detectar el archivo existente mientras está activo en la computadora con la ayuda de varias firmas y en algunos casos incluso eliminarlo. Por este motivo, es muy importante actualizar periódicamente el *software* antivirus.

02

Proceso de securización

- Debe instalarse en el punto final un *software* antivirus de proveedores de confianza.
- El *software* antivirus debe actualizarse de forma automática o manual (al menos una vez al día o según las recomendaciones del fabricante).

¿Lo sabía?

Caja de arena (*sandbox*): es una herramienta de emulación mediante la cual el antivirus analiza un archivo o proceso en una computadora, dentro de un área de cuarentena de la memoria. Cuando el virus se encuentra en la zona de cuarentena, no puede causar daños; es posible comprobar cuáles serán los resultados de su activación de forma aislada. Si se detecta que el archivo es un virus, el antivirus lo bloquea y notifica al usuario.

Firma del archivo: puede ser una firma estática, que es un valor *hash* de un fragmento de código único para el virus, o una firma basada en el comportamiento. Es decir, si un *software* intenta realizar alguna de las acciones definidas por el antivirus como sospechosas, este debe detener su acción y notificar al usuario.

Detección genérica: el antivirus analiza el comportamiento de los procesos que se están ejecutando en la computadora. Ello incluye monitorear su actividad, examinar los intentos de acceder a otros procesos, recursos, etc. Cuando un proceso en particular comienza a modificar un archivo del sistema, el antivirus monitorea cuidadosamente su comportamiento.

Sistema EDR

01

Principio de securización: *Endpoint Detection and Response* (EDR) define una categoría de herramientas y soluciones que se centran en localizar y monitorear información en los puntos finales de la organización. El sistema funciona con la ayuda de un agente instalado en los puntos finales. Este examina la posibilidad de ataques externos y amenazas internas, por medio del monitoreo del tráfico de la red, la actividad del punto final, servicios y procesos en marcha, etc. El agente recopila la información relevante y la almacena en una base de datos predefinida.

Un empleado de seguridad de la información que trabaja con el sistema puede utilizar la información recopilada con el fin de identificar anomalías, investigar, informar y dar alarma sobre eventos de seguridad de la información en la organización. La singularidad de la solución es que se trata de una plataforma unificada, que protege las computadoras portátiles, computadoras de escritorio, servidores y entornos virtuales.

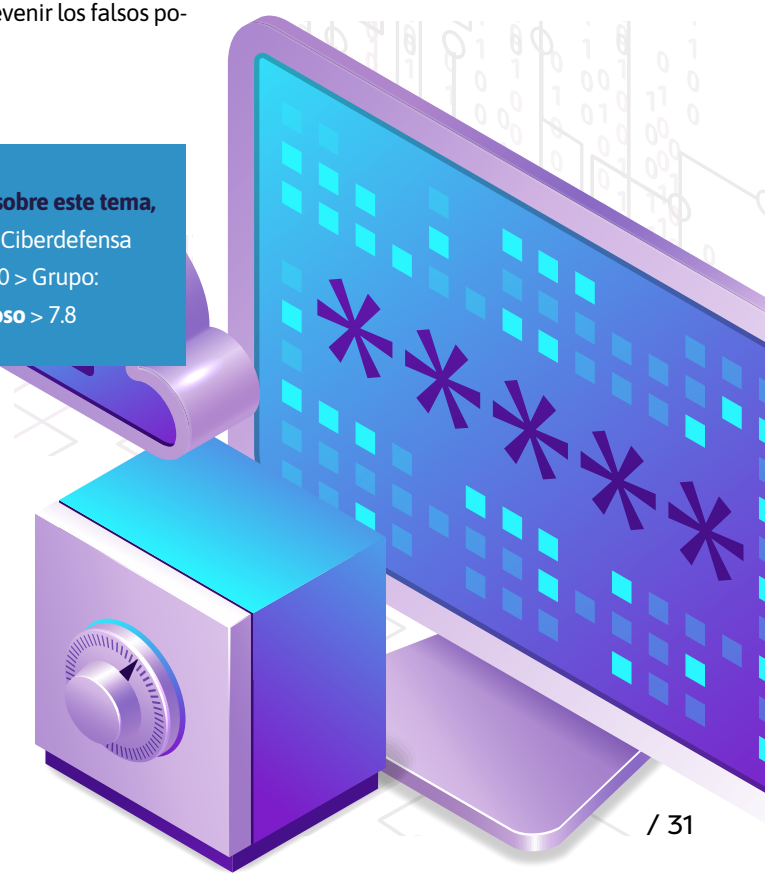
Monitorear los puntos finales y responder rápidamente a un ataque es clave para preservar la seguridad de un punto final. Las soluciones EDR son capaces de detectar un incidente o amenaza cibernética en una red de múltiples estaciones de trabajo.

¡Atención! La solución EDR monitoreará actividades en los puntos finales y hará posible examinar incidentes que comprometan la seguridad de la información.

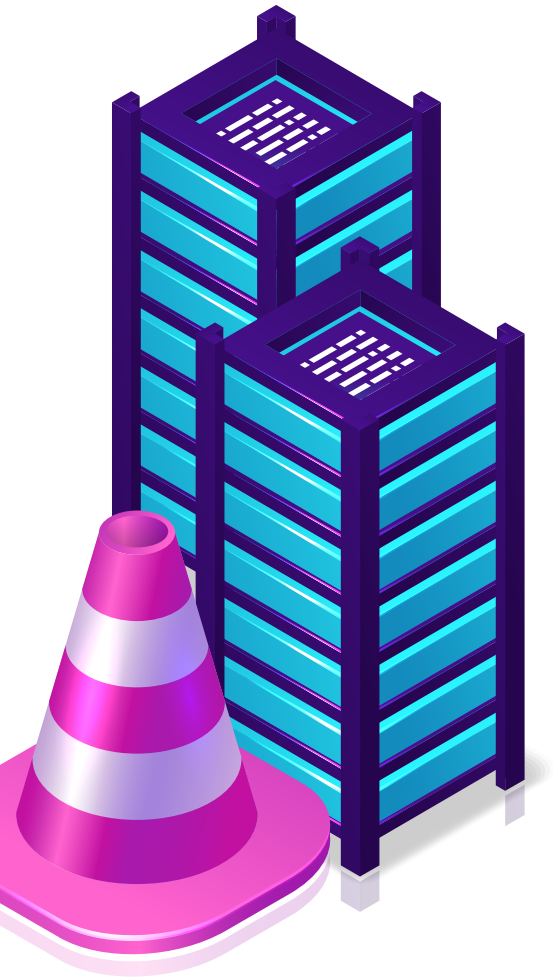
02

Proceso de securización: debe programarse el sistema EDR para localizar la cadena de eventos y almacenarlos para futuras investigaciones y comparaciones con eventos en línea, por ejemplo, de análisis de comportamiento. Ello se hace poniendo énfasis en configuraciones que permitan localizar y prevenir los falsos positivos y evitarlos.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Evitar el código malicioso** > 7.8



/05. Cortafuegos local



01

Principio de securización: los sistemas operativos de los puntos finales suelen proporcionar un cortafuegos, lo que permite bloquear el tráfico ilegal hacia y desde el punto final.[14]

El cortafuegos está diseñado para proteger la red al detectar y bloquear el tráfico no autorizado, con lo que ayuda a bloquear programas de *malware*, como virus y *software* malicioso.

14. Más información en CIS Control 13, disponible en: **https://www.cisecurity.org/controls/network-monitoring-and-defense**.

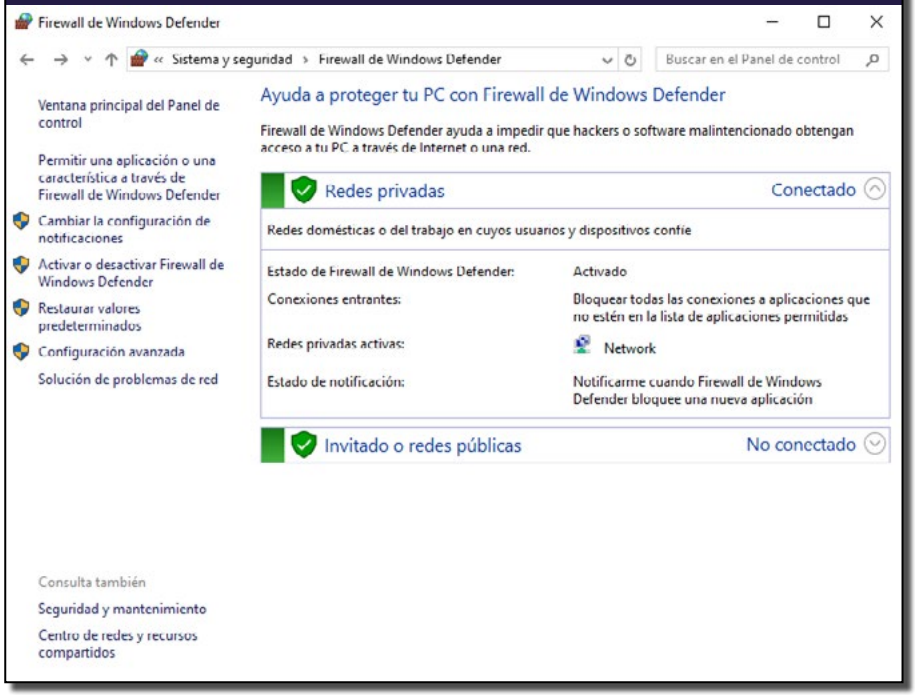
¡Atención! Es importante mantener activo el cortafuegos en los puntos finales, incluso si su red empresarial ya tiene instalado un cortafuegos empresarial, ya que se trata de una capa adicional de seguridad.

02

Proceso de securización: para verificar que el cortafuegos se esté ejecutando en segundo plano, siga los siguientes pasos.

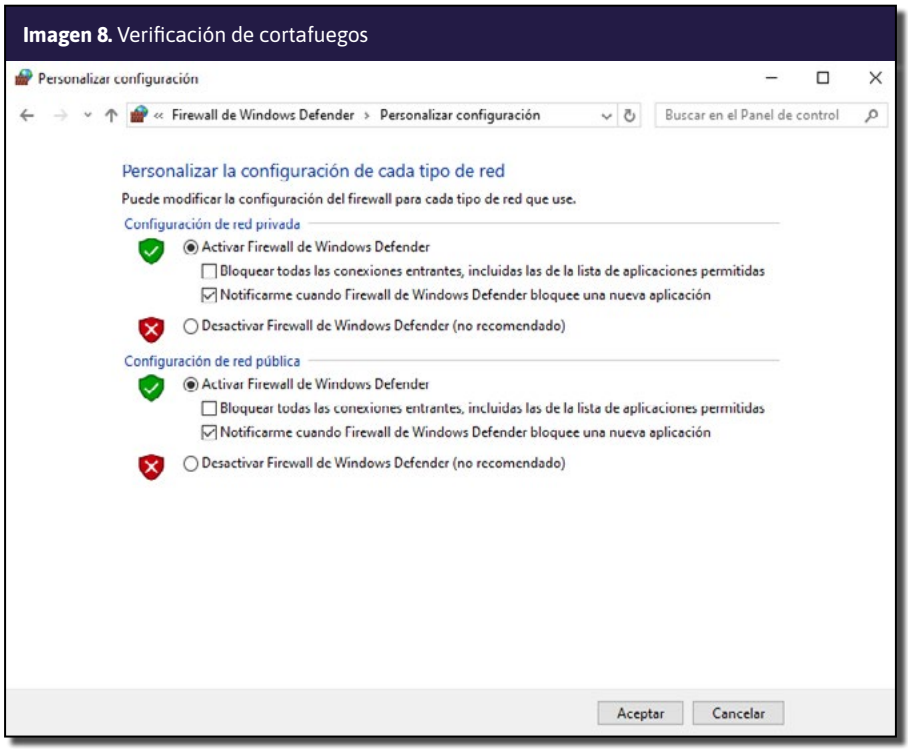
- Haga clic en **`Inicio`** y luego en la barra de búsqueda escriba: **`Panel de control`**. A continuación, acceda al cortafuegos seleccionando **`Sistema y seguridad`** > **`Firewall de Windows Defender`**.

Imagen 7. Cortafuegos local de Windows



- Seleccione la opción **`Activar o desactivar Firewall de Windows Defender`**, en el lado izquierdo de la pantalla (imagen 7).
- Asegúrese de que el cortafuegos esté activado tanto para la configuración de red privada como para la de red pública, como en la imagen 8.

Imagen 8. Verificación de cortafuegos



- En caso de necesitarlo, dentro del cortafuegos de Windows existen tres perfiles para diferentes entornos: **`PÚBLICO`**, **`PRIVADO`**, y **`DOMINIO`**.[15]

15. Puede encontrarse información adicional en: **https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-profiles**.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Protección de estaciones de trabajo y servidores** > 6.1

/06. Actualizaciones de seguridad

01

Principio de securización: en todo *software*, a veces se descubren problemas técnicos, que los intrusos pueden aprovechar para atacar el punto final. La mayoría de los fabricantes de *software* proveen actualizaciones de *seguridad* para sus productos, con el propósito de ayudar a sus clientes a preservar la seguridad de los puntos finales. En particular, los fabricantes de sistemas operativos, que son el componente de *software* clave en todo punto final, proporcionan regularmente actualizaciones de seguridad (por lo general, una vez al mes) y en ocasiones distribuyen actualizaciones críticas con mayor frecuencia. Las actualizaciones periódicas minimizan la posibilidad de que un atacante se aproveche de estas vulnerabilidades.[16]

02

Proceso de securización: como regla general, las actualizaciones deben instalarse automáticamente sin la intervención del usuario. Sin embargo, durante las actualizaciones existe el riesgo de que se desactive el punto final por varias razones. En aquellas organizaciones en las que este riesgo pueda ser crítico, las actualizaciones deben realizarse manualmente y solo después de que se haya verificado que no se están desactivando los puntos finales.

16. Más información en CIS Control 7, disponible en: **https://www.cisecurity.org/controls/continuous-vulnerability-management**.

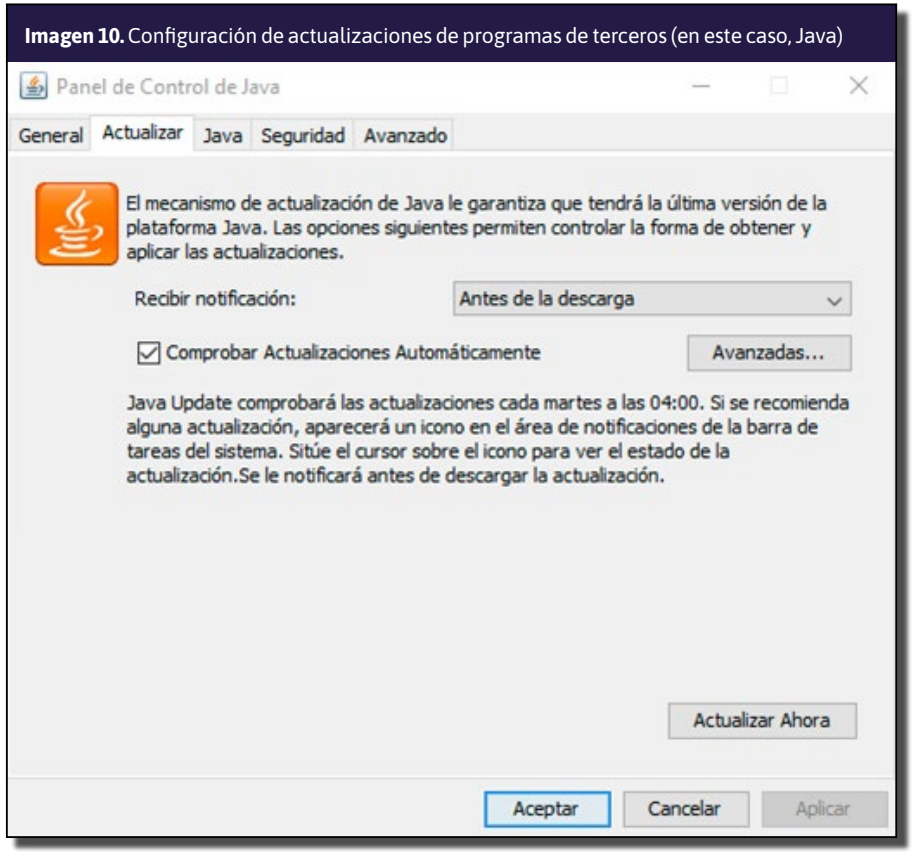
Deben realizarse las siguientes acciones para ejecutar actualizaciones de seguridad en el sistema operativo:

- Haga clic en **`Inicio`**, luego seleccione **`Configuración`** > **`Actualización y seguridad`** > **`Windows Update`**.
- Seleccione **`Buscar actualizaciones`**.

Imagen 9. Configuración de actualizaciones de Windows

Para programas desarrollados por terceros, puede leer la documentación incluida con el *software* o simplemente explorar los menús de configuración del programa para aprender cómo ejecutar el proceso de actualización manual o para habilitar las actualizaciones automáticas de ser posible. La imagen 10 presenta un ejemplo de configuración en Java.

Imagen 10. Configuración de actualizaciones de programas de terceros (en este caso, Java)



¡Atención! Las actualizaciones de los puntos finales deben realizarse de manera continua para evitar que los atacantes aprovechen vulnerabilidades.

Para más información sobre este tema, véase Metodología de Ciberdefensa para Organizaciones 1.0 > Grupo: **Evitar el código malicioso** > 7.9

Anexo

Cuadro A1.1. Lista de verificación recomendada

Tarea	Realizado	Parcialmente	No realizado
Seguridad física de los puntos finales	☐	☐	☐
Securización del BIOS (sistema básico de entrada/salida, siglas en inglés)	☐	☐	☐
Cifrado del disco duro	☐	☐	☐
Reducción de las cuentas de administrador	☐	☐	☐
Política de contraseñas	☐	☐	☐
Protección del administrador local	☐	☐	☐
Instalación de señuelos	☐	☐	☐
Copia de seguridad de la información	☐	☐	☐
Prevención de fugas de información	☐	☐	☐
Bloqueo de dispositivos	☐	☐	☐
Instalación de antivirus	☐	☐	☐
Instalación de sistema EDR	☐	☐	☐
Activación del cortafuegos	☐	☐	☐
Activación de actualizaciones de seguridad	☐	☐	☐

El punto final (*endpoint*) es el medio informático con el que trabaja el usuario en la organización. A través de este se accede a programas, aplicaciones, recursos informáticos de la organización y a la implementación de procesos. Como tal, un punto final está expuesto a un gran número de amenazas cibernéticas derivadas del uso de una computadora por parte del empleado, su configuración y su conexión a la red empresarial. El presente documento se basa en la **Metodología de Ciberdefensa para Organizaciones 1.0**[17], publicada por la Dirección Nacional de Ciberseguridad de Israel, en la que se detallan las recomendaciones para la protección de los puntos finales.

17. El documento se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad. Véase **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad**.

El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que una organización esté preparada para defenderse de las amenazas cibernéticas, debe dominar una gran cantidad de especializaciones: tecnológicas, organizativas y de procesos. La lista de capítulos presentada a continuación refleja el estado de la colección al momento de la publicación de este documento.

Volumen A: Un enfoque metodológico

Volumen B: Un enfoque técnico

- **B.01** Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)
- **B.02** Seguridad de infraestructuras Access Point Name (APN)
- **B.03** Endurecimiento de sistemas informáticos
- **B.04** Reducción de riesgos de ciberseguridad en cámaras de videovigilancia
- **B.05** Reducción de los riesgos de ciberseguridad en los puntos finales de la organización
- **B.06** Seguridad de sistemas de planificación de recursos empresariales (ERP)
- **B.07** Preparación y respuesta ante un ataque de *ransomware* en la organización
- **B.08** Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.09** Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.10** Seguridad de infraestructuras de voz sobre protocolo de internet (VoIP)
- **B.11** Autenticación multifactor avanzada ante amenazas de ciberseguridad
- **B.12** Principales amenazas de ciberseguridad de las plataformas de asistencia remota a usuarios
- **B.13** Prevención y respuesta ante un secuestro de Border Gateway Protocol (BGP Hijacking)
- **B.14** Preparación ante ataques distribuidos de denegación de servicio (DDoS)
- **B.15** Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)
- **B.16** Ciberseguridad por medio de sistemas de gestión de dispositivos móviles (MDM/EMM)
- **B.17** Seguridad en la transferencia gestionada de archivos (MFT)
- **B.18** Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)
- **B.19** Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí
- **B.20** Seguridad de los sistemas multimedia

Volumen C: Desarrollo seguro de *software*