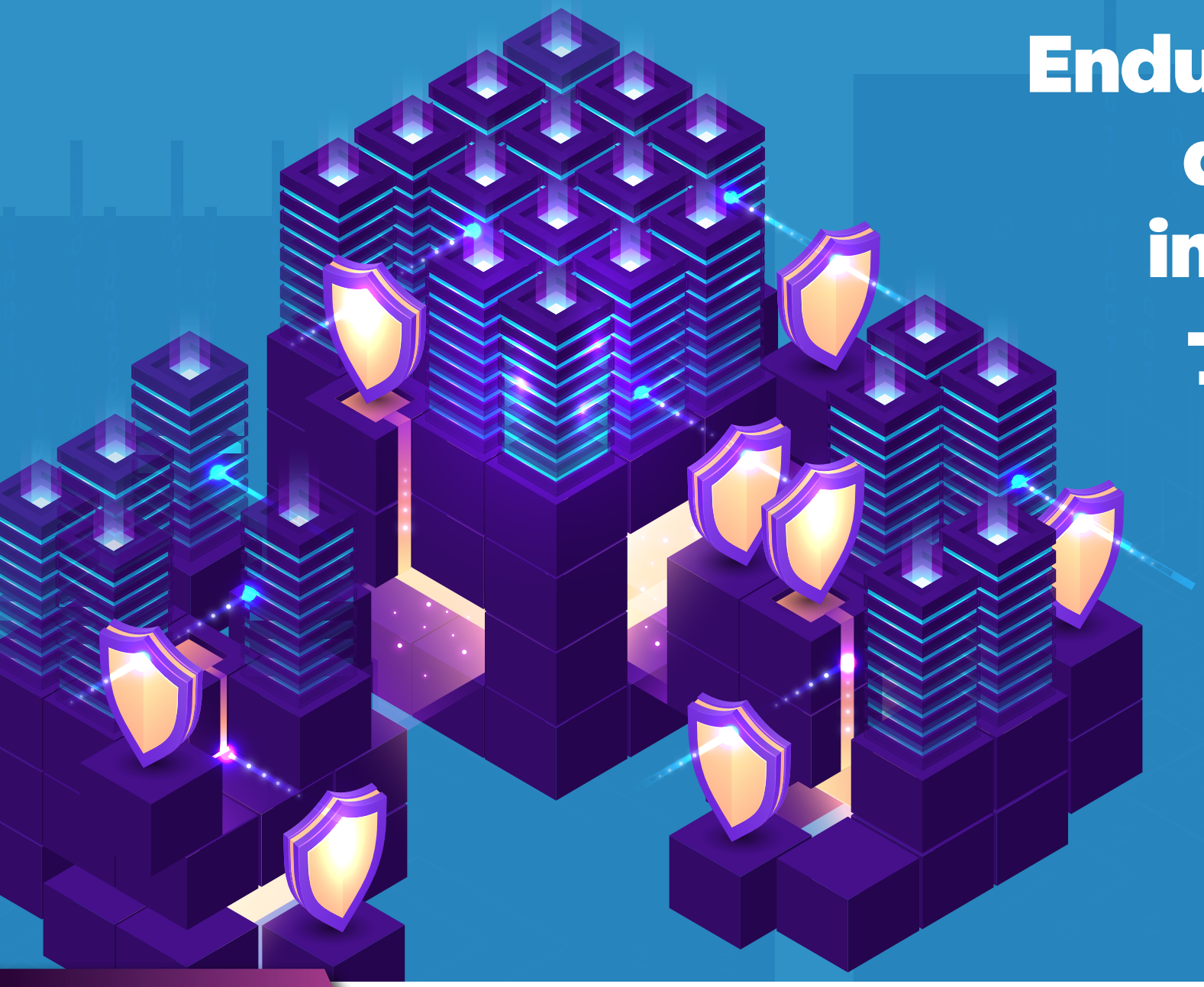


Endurecimiento de sistemas informáticos

Mejores Prácticas en Ciberseguridad

B.03

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Códigos JEL: D82, K24, L86, L96, M15, O20, O21, O33

Palabras clave: ciberseguridad, amenazas cibernéticas, riesgos cibernéticos, seguridad de sistemas, endurecimiento de sistemas, metodología de endurecimiento, activos cibernéticos, entorno de producción

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 *startups* 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 Grupo de Datos y Gobierno Digital (DDG) de la División de Capacidad Institucional del Estado (ICS) del BID, disponible en: **https://www.iadb.org/es/quienes-somos/topicos/modernizacion-del-estado/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.

Introducción

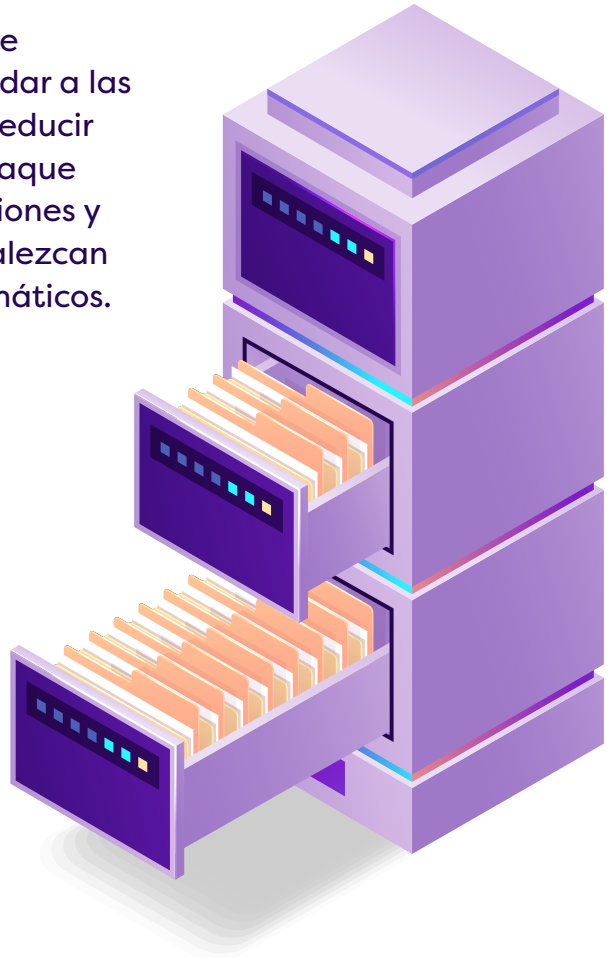
La superficie de ataque en el ciberespacio representa todas las interfaces a través de las cuales un adversario potencial puede interactuar con el sistema informático de una organización. Un ejemplo de interacción no autorizada es cuando un adversario introduce información maliciosa en una interfaz de *software* con el objetivo de interrumpir el funcionamiento normal de un sistema informático u obtener acceso a información confidencial o privilegiada almacenada en el sistema informático.

Limitar la superficie de ataque es una medida efectiva que dificulta que los adversarios en el ciberespacio logren sus objetivos y mejora la protección de las organizaciones contra los ciberataques.

Uno de los métodos aceptables para reducir la superficie de ataque es el endurecimiento, que implica cambiar los parámetros o configuraciones de funcionamiento del sistema informático. Un ejemplo común de endurecimiento consiste en deshabilitar la operación de los servicios del sistema que no son esenciales para las actividades habituales o cambiar el umbral de un mecanismo de seguridad.

/01. Propósito

El propósito de este documento es ayudar a las organizaciones a reducir su superficie de ataque realizando operaciones y controles que fortalezcan sus sistemas informáticos.



/02.
Público objetivo

El presente documento va dirigido a los directores de seguridad de la información (CISO, por sus siglas en inglés), arquitectos de ciberdefensa y tecnólogos de ciberseguridad, profesionales de ciberseguridad y equipos de sistemas.

/03. Etapas de trabajo

El entorno de trabajo moderno depende de la existencia de una infraestructura informática basada en interfaces que permiten el intercambio de información u órdenes operativas entre: i) módulos integrados en el sistema informático; ii) un sistema informático y otro; y iii) un usuario humano y el sistema informático. Estas interfaces forman la superficie de ataque que un adversario podría explotar para lograr sus propósitos.

El control sobre estas interfaces implica cambios en los parámetros o configuraciones operativos. Se puede hacer un número significativo de estos cambios a nivel de *software*.

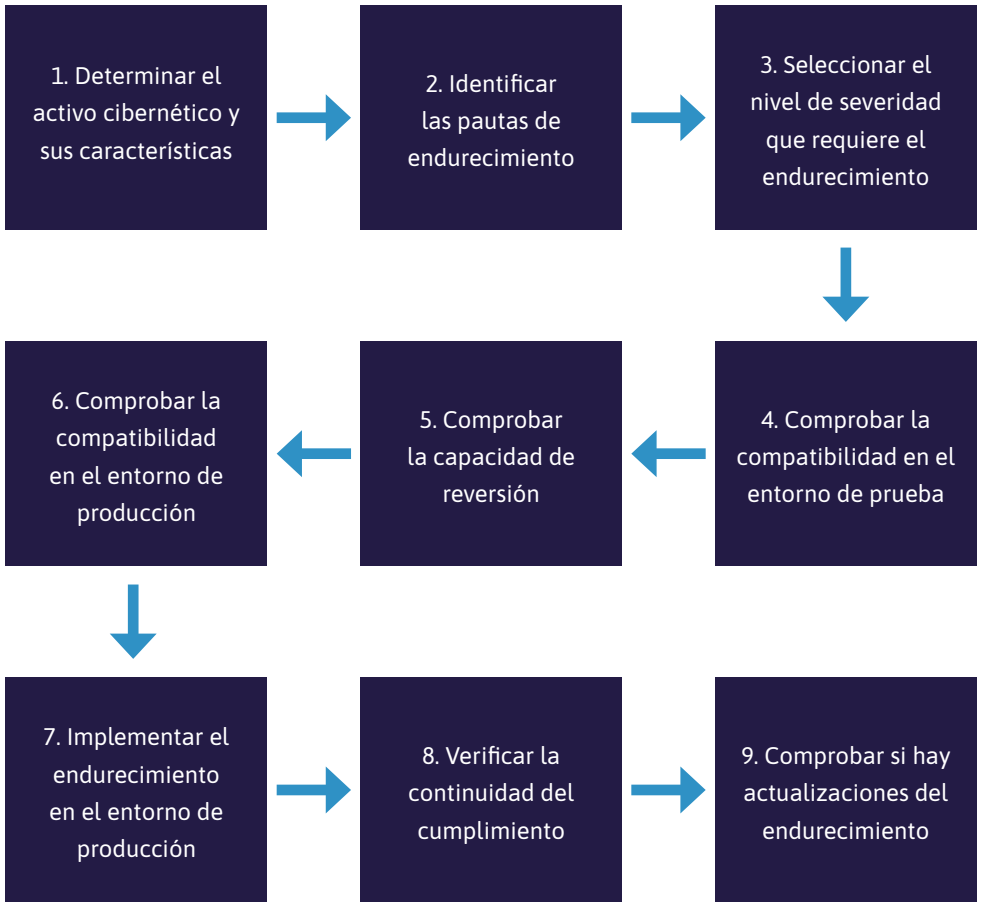
En el mundo se utilizan comúnmente varias metodologías de endurecimiento. Las principales metodologías son las creadas por la Agencia de Sistemas de Información de Defensa (DISA, por sus siglas en inglés) del Departamento de Defensa de los Estados Unidos y por la organización internacional sin fines de lucro Centro para la Seguridad de Internet (CIS, por sus siglas en inglés). Además, algunos fabricantes publican periódicamente pautas de endurecimiento, aunque en la mayoría de los casos no lo hacen de manera regular, y en ocasiones los usuarios u organizaciones necesitan manejar una gran cantidad de documentos para compilar el conjunto completo de pautas necesarias para llevar a cabo el endurecimiento.

Nota: Este documento se centra en el endurecimiento mediante *software* y no mediante *hardware* (como puede ser cambiar un circuito eléctrico utilizando un interruptor de apagado físico).

Cada metodología ofrece un conjunto de definiciones para la implementación de acuerdo con el nivel de gravedad y el tipo o versión del activo cibernético relevante.

La implementación de una metodología de endurecimiento incluye varias etapas clave (gráfico 1 y cuadro 1).

Gráfico 1. Etapas para implementar una metodología de endurecimiento



Cuadro 1. Explicación de las etapas para implementar una metodología de endurecimiento

N.°	Etapa	Explicación complementaria	Ejemplo
1.	**Determinar el activo cibernético y sus características**	Tales como la función del activo cibernético, el nombre del fabricante, la edición o la versión.	Servidor de base de datos fabricado por Israel Israeli Ltd., edición empresarial, versión 2019.
2.	**Identificar las pautas de endurecimiento**	Acceder al sitio web del proveedor de la metodología y descargar la documentación para llevar a cabo el endurecimiento (incluidos *scripts* u otras ayudas) que sea compatible con el activo cibernético previamente determinado.	Acceder al sitio web de las guías de implementación técnica de seguridad (STIG, por sus siglas en inglés) de la DISA y descargar la documentación y herramientas.
3.	**Seleccionar el nivel de severidad que requiere el endurecimiento**	Examinar la documentación relativa a los niveles de severidad y seleccionar el nivel de gravedad de acuerdo con el perfil de la amenaza.	La recomendación de la Dirección Nacional de Ciberseguridad de Israel (INCD, por sus siglas en inglés) es utilizar un nivel de severidad de, al menos, las categorías I + II de la DISA.[2]
4.	**Comprobar la compatibilidad en el entorno de prueba**	El endurecimiento del activo cibernético se implementa en un entorno de prueba *ad hoc* que simula una operación de producción para garantizar que la probabilidad de interrupción de la disponibilidad operativa sea baja. Si se descubre una restricción, analice si necesita actualizar las pautas de endurecimiento o la aplicación donde se descubrió la restricción.	Se endureció el sistema operativo de las estaciones terminales: a. El endurecimiento fue exitoso y no se descubrió ninguna restricción operativa. b. Debido a restricciones de aplicación, se decidió asumir el riesgo y no aplicar un requisito de seguridad particular.
5.	**Comprobar la capacidad de reversión**	Verificar la capacidad de regresar al estado anterior al endurecimiento para asegurarse de que, en caso de un problema en el entorno de producción, sea posible volver a una situación de trabajo normal.	Construir un plan de reversión y verificar su efectividad en el entorno de trabajo en la organización.
6.	**Comprobar la compatibilidad en el entorno de producción**	Realizar pruebas en una muestra representativa de activos cibernéticos en el entorno de producción para garantizar que la probabilidad de que la disponibilidad operativa se vea afectada después del endurecimiento sea baja. Si se descubre una restricción, analice si necesita actualizar las pautas de endurecimiento o el sistema informático al que se refiere la restricción.	Se endureció el sistema operativo de las estaciones terminales: a. El endurecimiento fue exitoso y no se descubrió ninguna restricción operativa. b. Debido a restricciones de aplicación, se decidió asumir el riesgo y no aplicar un requisito de seguridad particular.
7.	**Implementar el endurecimiento en el entorno de producción**	Implementar el endurecimiento gradualmente en el entorno de producción, ya sea al nivel de la imagen dorada o mediante algún otro método.	El sistema operativo de las estaciones terminales se endureció de acuerdo con los índices de implementación: 10%, 25%, 40%, 50%, 75%, 100%.

2. Las diferencias entre las principales categorías de endurecimiento de las guías STIG de la DISA se explican en el anexo 1.

N.°	Etapa	Explicación complementaria	Ejemplo
8.	**Verificar la continuidad del cumplimiento**	A fin de asegurarse de que el endurecimiento es efectivo y factible. En caso de anomalía, se vuelve a implementar el endurecimiento.	Realizar pruebas para verificar el endurecimiento utilizando un *software* automatizado para detectar vulnerabilidades; realizar evaluaciones de acuerdo con la metodología de endurecimiento (como la de la DISA) y el protocolo de automatización de contenido de seguridad (SCAP, por sus siglas en inglés).
9.	**Comprobar si hay actualizaciones del endurecimiento**	Verificar que el endurecimiento esté actualizado de acuerdo con las versiones recomendadas por el proveedor de la metodología de endurecimiento y con las ediciones o versiones de los sistemas informáticos de la organización.	Registrarse para ser agregado a una lista de correo que ofrezca actualizaciones de la metodología de endurecimiento. He aquí dos ejemplos: a. La metodología de endurecimiento que se utilizó para un sistema operativo en particular es la distribución 12, versión 2. El autor de la metodología publicó la distribución 12, versión 3. Por lo tanto, es necesario implementar el nuevo endurecimiento. b. Se publicó una actualización de *software* para un sistema operativo particular (que cambia el número de compilación de la versión del producto). Por lo tanto, debe verificar la compatibilidad con la metodología de endurecimiento recomendada.

Puntos importantes para una buena asimilación

1. Implementar el endurecimiento sin realizar pruebas preliminares para garantizar su compatibilidad puede causar la interrupción de las operaciones. Por lo tanto, se recomienda completar todas las operaciones de acuerdo con las etapas propuestas.

2. Realizar cambios en el entorno de trabajo, como instalar actualizaciones (parches) y llevar a cabo operaciones de mantenimiento, puede afectar el buen funcionamiento del endurecimiento. Por lo tanto, se recomienda asegurarse de que siga siendo efectivo después de realizar operaciones de este tipo.

3. Garantizar una capacidad de reversión rápida y eficaz es esencial para minimizar las interrupciones del entorno de producción en caso de que se detecte un problema.

4. Automatizar los procesos de endurecimiento y prueba, incluida su incorporación en el desarrollo de *software* y operaciones de tecnología de la información (DevOps, por sus siglas en inglés) y en el proceso de control de calidad de la organización, puede reducir significativamente los insumos organizativos requeridos.

A continuación se muestra un ejemplo de cómo se asignan las categorías de activos cibernéticos según el nivel de severidad recomendado de las vulnerabilidades que requieren endurecimiento (con las referencias a las fuentes de la metodología de endurecimiento).

Cuadro 2. Mapeo de activos cibernéticos de acuerdo con el nivel de severidad recomendado

N.°	Categoría de activo	Nivel de severidad recomendado para el endurecimiento	Fuente de la metodología de endurecimiento
1.	Sistemas operativos	Categorías de las STIG de la DISA niveles I + II	STIGs Document Library de la DISA, disponible en: **https://www.cyber.mil/stigs/downloads**.
2.	Soluciones de virtualización		
3.	Servidores web		
4.	Servidores de correo electrónico		
5.	Servidores de bases de datos		
6.	Equipo de comunicación		
7.	*Software* de oficina o *back office*	Categorías de las STIG de la DISA niveles I + II o recomendaciones del fabricante	STIGs Document Library de la DISA, disponible en: **https://www.cyber.mil/stigs/downloads**, o el sitio web del fabricante del activo, y/o recomendaciones específicas del equipo de asistencia del fabricante.
8.	Impresoras	Categorías de las STIG de la DISA niveles I + II o recomendaciones del fabricante	STIGs Document Library de la DISA, disponible en: **https://www.cyber.mil/stigs/downloads**, o el sitio web del fabricante del activo, y/o recomendaciones específicas del equipo de asistencia del fabricante.
9.	Sistemas de almacenamiento	Recomendaciones del fabricante	Sitio web del fabricante de activos o recomendaciones específicas del equipo de asistencia del fabricante.
10.	Sistemas de respaldo		
11.	Servicios en la nube pública		
12,	Sistema de seguridad de datos		

Nota: La recomendación predeterminada de la INCD es utilizar la metodología de las STIG de la DISA. Si no se tiene acceso a la documentación adecuada para esta metodología, se sugiere seguir las recomendaciones del fabricante.

Anexos

Anexo 1. Principales diferencias entre las categorías comunes de endurecimiento en las STIG de la DISA

A continuación se muestra la lista de las categorías de endurecimiento comunes en las STIG de la DISA. Cada categoría define un conjunto de requisitos de endurecimiento para la implementación de acuerdo con el perfil de la amenaza. Como regla general, la recomendación mínima de la INCD es aplicar los requisitos de endurecimiento que aparecen en las categorías I y II.

Cuadro A1.1. Principales diferencias entre las categorías comunes de endurecimiento en las STIG de la DISA

Categoría I	Categoría II	Categoría III
Cualquier vulnerabilidad que, si se explota, compromete **de manera directa e inmediata** la confidencialidad, disponibilidad, fiabilidad o integridad.	Cualquier vulnerabilidad que, si se explota, **podría comprometer** la confidencialidad, disponibilidad, fiabilidad o integridad.	Cualquier vulnerabilidad que **disminuya la capacidad de defensa** contra amenazas a la confidencialidad, disponibilidad, fiabilidad o integridad.

Escala de vulnerabilidad

(+) (-)

Anexo 2. Documentos aplicables

Esta sección contiene las fuentes de información utilizadas a la hora de elaborar este documento.

Fuentes de información en español

Dirección Nacional de Ciberseguridad de Israel (incluidos dentro de esta serie de guías de buenas prácticas en ciberseguridad)

- Metodología de ciberdefensa para organizaciones, versión 1.0. Disponible en: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad.**

Fuentes de información en inglés

- CIS Benchmarks. Disponibles en: **https://www.cisecurity.org/cis-benchmarks/.**
- NIST SP 800-70 Rev. 4.0 - National Checklist Program for IT Products – Guidelines for Checklist Users and Developers, febrero. Disponible en: **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf.**
- NIST SP 800-123 - Guide to General Server Security, julio. Disponible en: **https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf.**
- PCI. Data Security Standard (Requirements and Security Assessment Procedures), Version 3.2.1, mayo. Disponible en: **https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss.**
- STIGs Document Library. Disponible en: **https://www.cyber.mil/stigs/downloads.**

La superficie de ataque en el ciberespacio representa todas las interfaces a través de las cuales un adversario potencial puede interactuar con el sistema informático de una organización. En este sentido, limitar la superficie de ataque es una medida efectiva que dificulta que los adversarios en el ciberespacio logren sus objetivos y mejora la protección de las organizaciones contra los ciberataques.

El propósito de esta publicación es ayudar a las organizaciones a reducir su superficie de ataque a través de operaciones y controles de endurecimiento que fortalezcan sus sistemas informáticos mediante el ajuste de parámetros o configuraciones de funcionamiento. El documento va dirigido a los directores de seguridad de la información (CISO, por sus siglas en inglés), arquitectos de ciberdefensa y tecnólogos de ciberseguridad, profesionales de ciberseguridad y equipos de sistemas.

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
- **B.21** Integración de principios de ciberseguridad en los procesos de respaldo y recuperación
- **B.22** Protección de los servicios de nube pública ante amenazas de *ransomware*

Volumen C: Desarrollo seguro de *software*