

# Recomendaciones de defensa: La amenaza interna

## Adaptación de la organización en el ciberspacio

Mejores Prácticas en Ciberseguridad



# A.04

Volumen A:  
Un enfoque metodológico



**Cyber Israel**  
National Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título “Recomendaciones de defensa – Adaptación de la organización en el ciberespacio: La amenaza interna”.

© (2019) Dirección Nacional de Ciberseguridad de Israel.

© (2022) Banco Interamericano de Desarrollo por esta traducción.

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) 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, si bien 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 referencias a la normativa israelí o a sus organismos gubernamentales).

Esta publicación puede descargarse, copiarse y distribuirse, siempre que se otorgue la debida atribución a la Dirección Nacional de Ciberseguridad para la versión original en hebreo y al BID para la traducción en español, y que la publicación no se modifique. Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del BID, de su Directorio Ejecutivo, ni de los países que representa.

El documento original se encuentra disponible en el siguiente enlace: [https://www.gov.il/en/Departments/General/coping\\_thret](https://www.gov.il/en/Departments/General/coping_thret). Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

“El presente documento ha sido redactado por el Dirección Nacional de Ciberseguridad con el fin de fomentar la ciberseguridad en la economía israelí. Todos los derechos reservados para el Estado de Israel - Dirección Nacional de Ciberseguridad. El documento ha sido elaborado para beneficio del público. La copia del documento o su incorporación en otros documentos estará sujeta a las siguientes condiciones: el reconocimiento de la autoría de la Dirección Nacional de Ciberseguridad en el formato que aparece a continuación; la utilización de la última versión del documento; la no realización de modificaciones en el documento. El documento contiene información de carácter profesional, cuya implementación requerirá el conocimiento de los sistemas y la adaptación a las características de estos por parte de un profesional en el ámbito de la ciberseguridad. Cualquier comentario o referencia se puede enviar por correo electrónico a: [tora@cyber.gov.il](mailto:tora@cyber.gov.il).”

# Índice

## Prólogo

/Pág. 2

## 01. Introducción

/Pág. 8

## 02. Público destinatario

/Pág. 10

## 03. La amenaza

/Pág. 11

## 04. Recomendaciones de defensa

/Pág. 15

## Referencias

/Pág. 39

## Anexos

/Pág. 40

# 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 de-

tectaron 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 refuerzen 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.<sup>1</sup>

## 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 orga-

nizaciones 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.



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>.

# /01.

## Introducción

Es común clasificar las amenazas cibernéticas de una organización en dos familias: la **amenaza externa** de una persona que no pertenece a la organización y que trata de entrar en la organización a través de sus sistemas informáticos y de comunicaciones y causar daños, y la **amenaza interna** de una persona que desde dentro de la organización comete actividades maliciosas.

Una amenaza interna puede llevarla a cabo un empleado de la organización, **un proveedor de servicios, un contratista o socio comercial que actualmente está empleado o lo estuvo anteriormente** y que cumple con estos dos criterios:<sup>2</sup>

### 01

**Tiene o ha tenido autorizaciones de acceso a la red de la organización,** sus sistemas o la información almacenada en ellos.

### 02

**Rebasó deliberadamente sus privilegios originales** o los usó para comprometer la integridad, disponibilidad o confidencialidad de los procesos y la información de la organización.<sup>3</sup> Los motivos de una persona de dentro de la organización para cometer actos maliciosos son diversos y pueden ser psicológicos, como vengarse de un empleador, económicos, como robo o chantaje por parte de un tercero, e ideológicos.

Los siguientes son unos cuantos ejemplos de amenaza interna:

### 01

El caso de Edward Snowden, quien filtró una cantidad considerable de información de la Agencia de Seguridad Nacional de los Estados Unidos, organización para la cual trabajó.

### 02

Un programador de una compañía de software en Israel, que robó el software desarrollado en la compañía para comercializarlo en la red oscura.

### 03

Un incidente en una compañía de tarjetas de crédito en Israel, cuyos empleados recopilaban información confidencial de los clientes y amenazaron con publicarla si no se les pagaba millones de dólares.

Enfrentarse a las amenazas internas es complejo, entre otras cosas, porque choca con el deseo y la necesidad de la organización de confiar en sus empleados.

**La suposición subyacente de esta publicación es que no hay contradicción entre la confianza y el monitoreo.** Por un lado, la organización confía en sus empleados, pero, por el otro, monitorea sus actividades con fines de defensa, dentro de los límites de la ley.

A pesar de estas definiciones, extendidas en la literatura y documentos profesionales, también puede existir una amenaza interna sin que la parte que está siendo explotada lo sepa, como cuando una parte externa explota los privilegios de acceso de una persona dentro de la organización.

La ingeniería social, que se basa en la manipulación y la suplantación con el objetivo de eludir los mecanismos de seguridad, permite a un atacante que practica suplantación de identidad (*phishing*) engañar a los iniciados, utilizando tácticas de engaño y persuasión, para que descarguen un archivo “inocente” que en realidad contiene código malicioso (*malware*). En etapas más avanzadas, el atacante se hace con la estación de trabajo del usuario para extraer información de la organización.

También puede haber un error humano y, a veces los empleados pueden causar inadvertidamente un incidente de seguridad de datos. Ejemplos de ello son enviar un correo electrónico a la dirección incorrecta, insertar inocentemente un medio extraíble en una computadora o cargar información confidencial en un sitio público por error.

2. La definición de “amenaza” se basa en el documento Insider Threat, del CERT Coordination Center, Carnegie Mellon University.

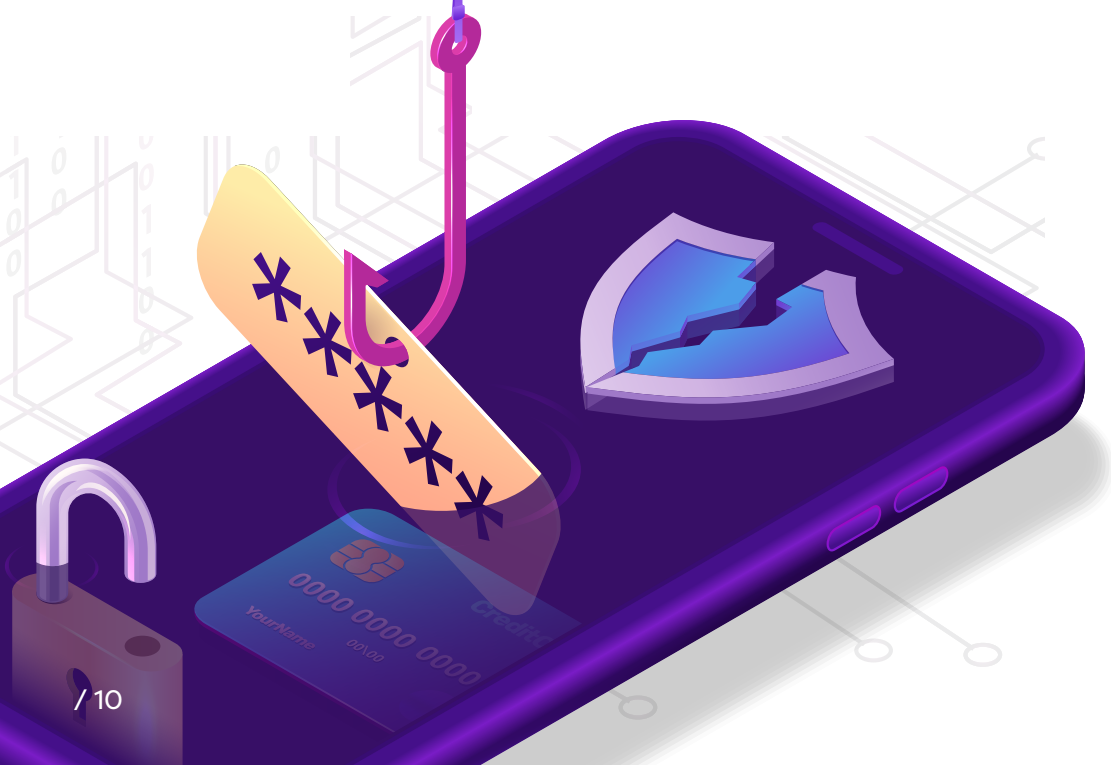
3. Una persona de dentro de la organización también puede causar daños por error. Esta publicación se enfoca en aquellos que causan daños intencionadamente; sin embargo, muchos controles también son aplicables al daño inadvertido.

# /02.

## Público destinatario

Esta publicación está destinada a gerentes de empresas, gerentes de seguridad de datos, personal de recursos humanos y oficiales de seguridad responsables de la integridad de los empleados, y también a Directores de Seguridad de la Información (CISO, por sus siglas en inglés) que desean mejorar su capacidad para hacer frente a las amenazas cibernéticas internas.

Debido a la naturaleza técnica de algunas de las recomendaciones, deben ser aplicadas por profesionales con calificaciones y experiencia relevantes.



# /03.

## La amenaza

Los siguientes pueden ser ejemplos de situaciones de amenazas que proceden de una persona de dentro de la organización:

### 01

**Filtrar información protegida de la organización** fuera de la organización por correo electrónico o teléfono (como información médica, información sobre un plan de negocios, una lista de clientes, transacciones, etcétera).

### 02

**Acumular un gran volumen de archivos** con el objetivo de copiarlos en un medio extraíble y fugarse con ellos tras dejar la organización.

### 03

**Propagar código malicioso** como resultado de conectar medios privados no autorizados a la red de la organización.

### 04

**Alterar datos** en los sistemas de datos de una organización. Esta amenaza puede materializarse de varias maneras:

- **Robo físico** de una computadora portátil o medio extraíble.
- **Configuraciones de software de alerta** para abrir canales de ataque internos (como definiciones en un Active Directory).
- **Robo de información** ya sea copiándola o enviándola fuera de la organización.
- **Fugas de información utilizando una unidad USB.**
- **Escaneo no autorizado de la red de la organización** para identificar y localizar información confidencial.
- **Obtención de privilegios de acceso elevados** sin permiso.

- **Explotación de terminales** con el fin de filtrar información.
- **Eliminación de información.**
- **Alteración de la configuración de la red** para permitir un ciberataque.

Cyber Security Insiders y Crowd Research Partners (2018) emitieron su Informe 2018 sobre las amenazas internas. Allí analizaron los activos de las tecnologías de la información (TI) de las organizaciones que fueron el blanco principal de la explotación por parte de personas

de dentro de la organización, y presentaron un gráfico que muestra los activos de TI más vulnerables durante los ataques internos.

Debido a la necesidad comprensible de las organizaciones de confiar en sus empleados y a la percepción de que los atacantes que amenazan a la organización son personas externas, las organizaciones centran la mayor parte de sus esfuerzos de defensa en personas hostiles ajenas.

Como resultado, las de dentro cuentan con una ventaja sobre las de fuera: están dentro

de la organización, tienen los privilegios de acceso necesarios para realizar su trabajo y están en posición de superar muchas medidas de defensa.

Un estudio realizado por IBM X Force encontró que las personas de dentro de la organización son responsables del 60% de los incidentes cibernéticos en las organizaciones.<sup>4</sup>

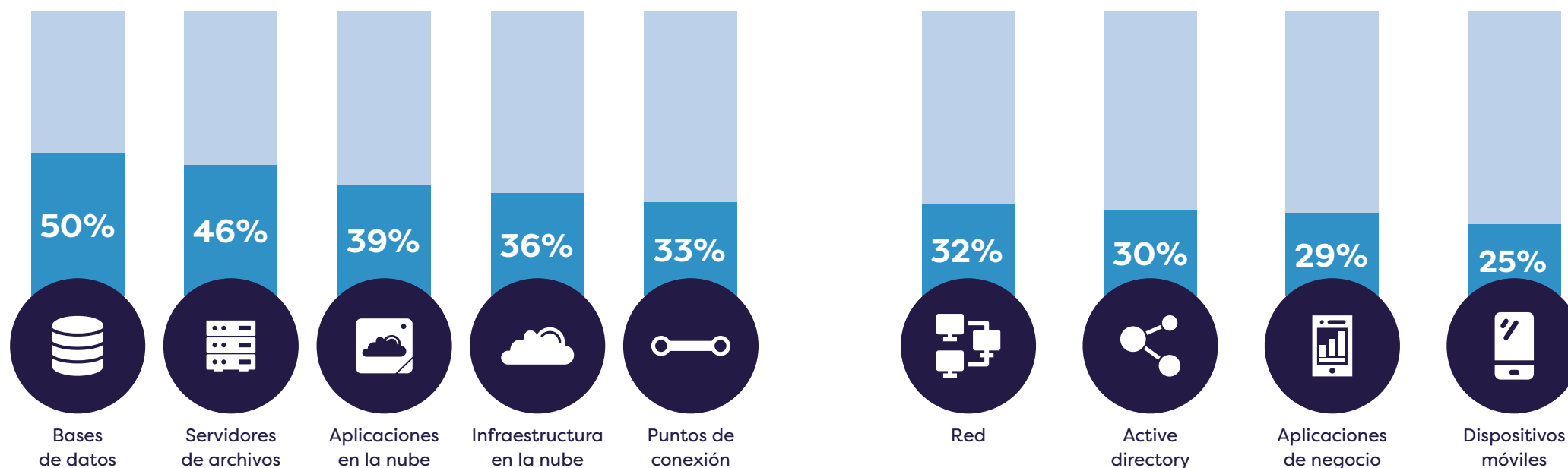
La suposición subyacente recomendada para la política de defensa cibernética de una organización es que no hay contradicción entre confiar en un empleado y monito-

rear sus actividades. Los controles estrictos sobre las actividades de los empleados son necesarios porque las amenazas también están aumentando entre el personal con privilegios de acceso elevados. Con el objeto de hacer frente a las amenazas internas, se deben instituir varias operaciones que abarquen a toda la organización.

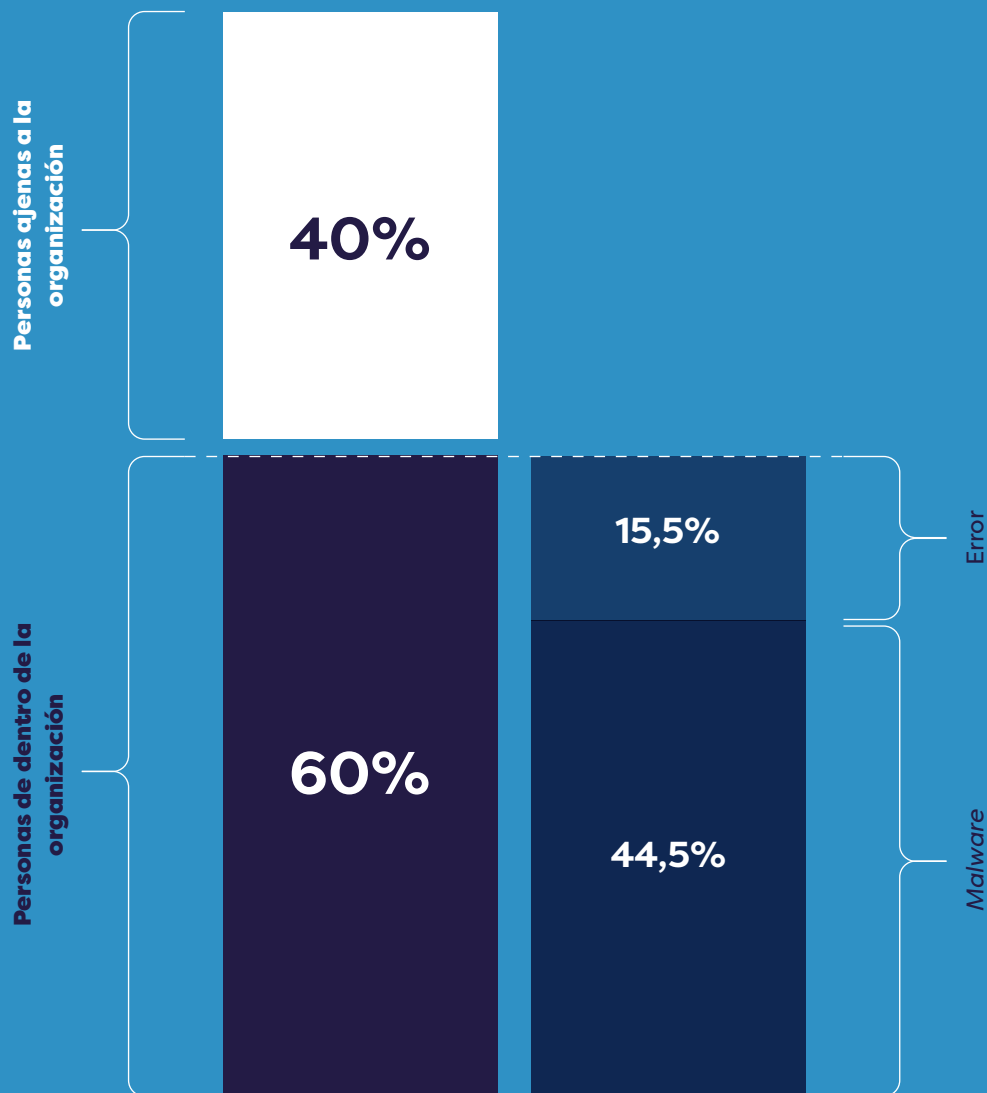
4. Más información disponible en: <https://www-05.ibm.com/services/europe/digital-whitepaper/security/index.html>.

**Gráfico 1.** Activos de TI más vulnerables durante los ataques internos

**Fuente:** Cyber Security Insiders y Crowd Research Partners (2018: 9).





**Gráfico 2.** Responsabilidad de personas internas y externas en los ciberataques

Fuente: IBM X Force.

# /04. Recomendaciones de defensa

## Tecnologías de defensa

Existen numerosas tecnologías que ayudan a gestionar los riesgos derivados de las amenazas internas. Estas permiten la detección de una respuesta y la defensa contra amenazas cibernéticas. Todas estas herramientas son necesarias para optimizar las configuraciones. Es esencial que las organizaciones optimicen las configuraciones y apliquen las mejores prácticas para utilizar de manera óptima las tecnologías a fin de obstaculizar a los atacantes y eliminar las amenazas.

## Aplicar el monitoreo del comportamiento del usuario

El software de monitoreo del comportamiento del usuario (UBM, por sus siglas en inglés) es también una herramienta efectiva para detectar amenazas internas, ataques

dirigidos, fraude financiero, etc. **Estas soluciones monitorean los patrones de comportamiento del usuario** mediante el análisis de algoritmos y la realización de análisis estadísticos. La analítica empaquetada, como los productos recomendados por Gartner,<sup>5</sup> detectan anomalías y descubren amenazas e incidentes potenciales. La tecnología de monitoreo del comportamiento del usuario ayuda a las organizaciones a crear perfiles de riesgo de usuario basados en algoritmos que comparan anomalías en las actividades de un empleado en particular con las de otros empleados con el mismo perfil de usuario en la organización. Esta tecnología permite a las organizaciones detectar discrepancias con respecto al comportamiento básico estándar y los perfiles de usuario.

5. Para más información, visítese: <https://www.gartner.com/reviews/market/user-and-entity-behavior-analytics>.

Los sistemas de monitoreo del comportamiento del usuario proporcionan las siguientes capacidades:

# 01

## Uso de aplicaciones y sitios web designados:

la mayoría de los empleados usan las mismas aplicaciones y sitios web durante las horas de trabajo. Por ejemplo, casi todos los empleados de oficina usan Microsoft Word y Excel, Google Chrome y el correo electrónico, mientras que el departamento de desarrollo también necesita usar Visual Studio y otras aplicaciones de programación.

# 02

**Privilegios de acceso:** las organizaciones no siempre los definen sobre la base de una “necesidad de saber”, debido a razones operativas y de otro tipo. Mediante el uso del software de monitoreo del comportamiento del usuario, si un empleado con un perfil de “usuario ordinario” intenta acceder a una carpeta que contiene objetivos de marketing y estratégicos, se generará un aviso de que ha realizado una acción anómala.

# 03

**Razonabilidad y factores contextuales:** indicadores psicolingüísticos, por ejemplo, el

uso de un lenguaje que difiere del habitual en la cultura en una organización puede ser un indicador de una fuga de datos.

# 04

**Datos que no sean de TI:** además de los datos técnicos, las herramientas de monitoreo del comportamiento del usuario pueden recopilar datos del departamento de recursos humanos y de otras aplicaciones comerciales. Estos datos proporcionan al sistema de monitoreo del comportamiento del usuario información sobre los períodos de vacaciones de los empleados, el tiempo de permanencia en sus puestos y los proyectos de la organización. También se puede recopilar información de los sistemas de seguridad, por ejemplo, qué empleados están en el lugar de trabajo, determinar la localización geográfica de un empleado, etcétera.

# 05

**Autenticaciones mediante identificación biométrica:** el análisis biométrico se utiliza para identificar a un usuario ilegítimo (por ejemplo, analizar el comportamiento de un usuario de acuerdo con la velocidad de escritura de su teclado, la forma en que usa el ratón o sus movimientos oculares sobre la pantalla ayuda a identificar si la persona en cuestión es el usuario legítimo u otra persona).

## Recopilación de datos para análisis

La interfaz de los productos de monitoreo del comportamiento del usuario con los sistemas de información de seguridad y gestión de eventos puede ayudar a reducir el volumen de alertas recibidas por el equipo de monitoreo.

El gráfico 3 muestra un ejemplo de monitoreo de incidentes tras incorporar las recomendaciones anteriores.

Estas capacidades ayudan a investigar los incidentes sospechosos en la organización no solo desde el punto de vista técnico sino también con vistas a corroborar una sospecha basada en el historial y el comportamiento de los usuarios implicados en un proceso.



Gráfico 3. Ejemplos de monitoreo de incidentes





Durante el proceso de asimilación, el sistema de monitoreo del comportamiento del usuario se centra en las siguientes etapas:

## 01

**Adquisición de información sobre la organización y creación perfiles de usuario y patrones de actividad** de los usuarios en la organización durante un período de tiempo. Se trata de un período de aprendizaje que dura entre 30 y 90 días, durante el cual el sistema aprende los patrones de actividad de los usuarios mediante la recopilación de datos de los sistemas de TI.

## 02

**Con base en patrones de trabajo idénticos**, creación de perfiles y características de usuario.

## 03

**Proceso de comparación de comportamientos de usuarios similares** una vez que se han creado los perfiles de usuario.

## 04

**Reenvío de un informe en tiempo real** en caso de que el sistema detecte anomalías.

Algunos ejemplos de definiciones de eventos potencialmente críticos basados en el comportamiento anómalo del usuario son los siguientes:

## 01

Un usuario con altos privilegios de acceso intenta **acceder a un servidor de archivos en mitad de la noche** (un momento en el que no hay una razón justificada para acceder a este servidor).

## 02

Un usuario de la organización intenta **acceder a una carpeta sin autorización**.

## 03

Un usuario **intenta cambiar la configuración**.



## 04

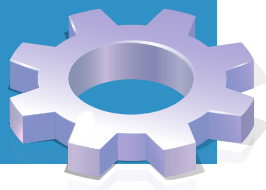
**Antes de dejar la empresa, un empleado recopiló un volumen inusual de documentos y archivos de la organización.**

## 05

**Un usuario común imprime un volumen anómalo de páginas** (por ejemplo, 50), cuando el volumen de impresión promedio para los empleados con el mismo perfil es de cinco páginas.

**Recuadro 1.** Caso real: comportamiento anómalo de acumular documentos de la organización en una carpeta y filtrarlos fuera de la organización

**Tomado de una sentencia judicial (Caso de delito grave 17959-01-10 del 30/10/2011, aprobado para su publicación):** Durante su servicio militar en las Fuerzas de Defensa de Israel, la acusada sirvió en la sede del Comando Central del Cuartel General del Ejército entre agosto de 2005 y junio de 2007. Mientras servía en su puesto, estuvo expuesta a muchos documentos clasificados y presentaciones, incluidos planes para operaciones militares, movilizaciones y órdenes de batalla para militares de las Fuerzas de Defensa de Israel, resúmenes de debates internos de las Fuerzas de Defensa de Israel, evaluaciones de la situación de las Fuerzas de Defensa de Israel, objetivos de las Fuerzas de Defensa de Israel, etc. (en adelante, “los documentos”). La acusada almacenó los documentos en una carpeta especial y, justo antes de su alta de las Fuerzas de Defensa de Israel, por motivos ideológicos y con la intención de divulgar los documentos al público en general, los copió en dos discos, uno para documentos y el otro para presentaciones. Posteriormente, la acusada se llevó los discos a su casa y los copió en su computadora, sin autorización alguna para ello. El disco copiado contenía 2.085 documentos, de los cuales alrededor de 700 estaban clasificados como “secreto” y “de alto secreto”.



## Aplicar la prevención de pérdida de datos

Los productos de prevención de pérdida de datos se han desarrollado para clasificar y proteger información confidencial. Estos sistemas están diseñados para identificar y prevenir la exposición y la filtración de información organizacional sensible tanto dentro como fuera de la organización, y para reportar tales incidentes. Para clasificar la información de acuerdo con los niveles de sensibilidad, estos sistemas dependen de la información de la organización. Los productos de prevención de pérdida de datos proporcionan una solución integral para identificar y mantener el reenvío controlado de información de la organización a varias plataformas mediante unidades USB, acceso a Internet, impresión, etcétera.

Antes de asimilar e implementar productos de prevención de pérdida de datos, las organizaciones deben asegurarse de lo siguiente:

## 01

**Se ha definido y creado una matriz de clasificación de documentos** y los empleados han asimilado el proceso de clasificación.

## 02

Se ha realizado **una evaluación de riesgos y un mapeo de documentos confidenciales en la red de la organización** (como documentos estratégicos, documentos de marketing, listas de empleados, archivos que contienen información personal, información financiera, etcétera).

## 03

**Se ha instituido un proceso para aprender y comprender la cultura organizacional y los procesos de flujo de la información**, tanto dentro como fuera de la red organizacional (en los sistemas informáticos y en general).

## 04

**Se han definido posibles escenarios de pérdida de información** y una respuesta acorde en caso de que se produzcan tales incidentes.



**Metodología de Ciberdefensa para Organizaciones > Categoría: Proteger la información > 5.5**



## Restringir el uso de medios extraíbles

Una de las formas más comunes de transferir información es mediante el uso de memorias USB. Para minimizar la amenaza de fugas de información y dificultar que cualquier persona de la organización que intente utilizar un dispositivo USB extraiga información, **las organizaciones deben bloquear el acceso de USB a sus sistemas mediante un sistema de control de dispositivos, sistemas de prevención de pérdida de datos o**

**definiciones del BIOS.** El bloqueo se puede hacer usando medios lógicos (dentro del marco de la política de la compañía y un proceso de monitoreo) o, alternativamente, usando medios físicos (prohibición general del uso de dispositivos USB).



**Metodología de Ciberdefensa  
para Organizaciones > Categoría:  
Proteger la información > 5.1**

### Recuadro 2. Caso real: uso de medios de almacenamiento para extraer información de la organización

En una de las empresas tecnológicas emergentes (*start-up*) en Israel, un empleado **conectó un medio extraíble a una de las computadoras de la organización con el fin de robar información** y, al hacerlo, causó daños a la propiedad intelectual de la empresa, a la propia empresa y también al Estado. De acuerdo con la demanda, cuya publicación fue permitida (Caso de delito grave 06-18): “Dentro de las competencias de su trabajo en la empresa, el acusado tenía acceso a los servidores informáticos de la empresa (en adelante, ‘los servidores’), a las herramientas desarrolladas por la empresa que se almacenaron en los servidores y al código fuente de los productos de la empresa, que también se almacenaron en los servidores. Parte de la información a la que tenía acceso el acusado no era directamente necesaria para el desempeño de su trabajo en la empresa y, sin embargo, se le dio acceso a este material como parte de las autorizaciones que se otorgaron al equipo de automatización, al que pertenecía el acusado [...] El 13/02/2018, durante las primeras horas de la mañana, el acusado conectó un disco duro externo de su propiedad (en adelante, ‘la unidad externa’) a su estación de trabajo [...] Aproximadamente a las 18:45, el acusado completó la operación de copia antes mencionada y luego desconectó la unidad externa de su estación de trabajo y dejó el lugar de trabajo con la unidad externa que contenía la información de la computadora que él había copiado [...] El acusado abandonó la empresa con el sistema [...]”.

## Restringir el acceso a los servicios de almacenamiento en la nube

El uso de servicios en la nube es frecuente en las organizaciones. El uso de servicios de almacenamiento en la nube (tales como Google Drive, DropBox, Gmail, etc.) aumenta el riesgo de que una persona de dentro de la organización pueda explotar estas soluciones para reenviar información fuera de la organización (con la intención de usarla para beneficio personal). Las organizaciones pueden bloquear el acceso a los sitios de almacenamiento en la nube mediante el cortafuegos (*firewall*) de la organización o mediante soluciones de control del navegador, como un proxy. Las organizaciones deben tener en cuenta que las redes con conexiones a Internet están expuestas al riesgo de que la información se filtre a cualquier sitio web (por ejemplo, al transferir información o fragmentos de información hasta acumular una determinada cantidad mediante respuestas [*talkbacks*] o al cambiar una fuente estándar a una fuente que no se usa comúnmente o es rara, por lo que los sistemas de monitoreo no pueden leerla, etc.). En consecuencia, este tipo de bloqueo está lejos de ser hermético.



**Metodología de Ciberdefensa  
para Organizaciones > Categoría:  
Proteger la información > 5.5**

## Administrar permisos de privilegios de acceso de usuarios

Como parte de las iniciativas para proteger la información en la red de las amenazas internas, las organizaciones deben administrar y supervisar los diversos tipos de permisos de usuario. Se debe realizar una gestión de las autorizaciones de usuario. Eso significa, entre otras cosas, **otorgar a cada usuario los permisos mínimos necesarios** para realizar las tareas relacionadas con su trabajo (compartimentación, fechas de vencimiento de autorizaciones, etcétera). Como parte del proceso de gestión y minimización de riesgos, se recomienda revisar periódicamente los permisos que se han otorgado a los empleados de la organización y actualizarlos en consecuencia: empleados que abandonaron la organización, cambios por rotación entre empleos, etcétera.



**Metodología de Ciberdefensa  
para Organizaciones > Categoría:  
Control de acceso > 4.10**

## Implantar un cortafuegos interno

El uso de un cortafuegos interno permite a las organizaciones monitorear la actividad

anómala y minimizar la capacidad de un atacante de dentro de la organización de pagar su ataque en la red. Por lo general, un cortafuegos interno viene como parte de un paquete que también incluye una aplicación de cortafuegos, un sistema de prevención de intrusiones (IPS, por sus siglas en inglés) y herramientas adicionales que pueden aumentar el nivel de seguridad en la red en su conjunto y evitar que una persona de dentro de la organización que haya obtenido privilegios de acceso abuse de ellos para difundir un ataque en toda la red. El cortafuegos interno monitorea todo el tráfico en la red y bloquea el tráfico no autorizado (como un intento de permitir que dos estaciones terminales se comuniquen entre sí).



**Metodología de Ciberdefensa para Organizaciones > Categoría: Seguridad de la red > 9.10**

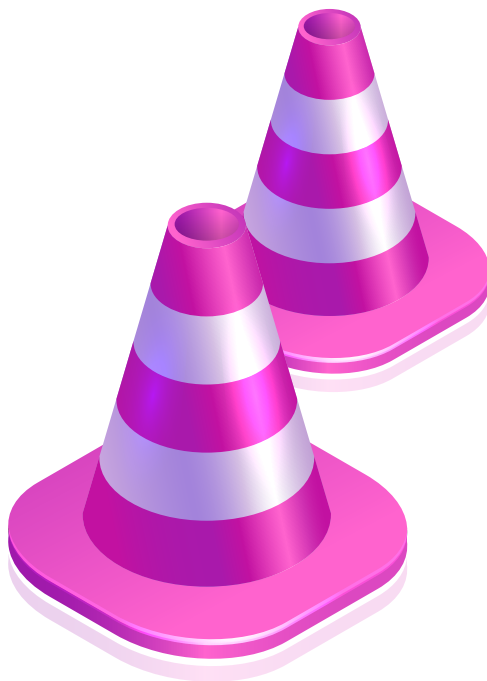
## Bloquear dispositivos de comunicación

El bloqueo de dispositivos de comunicación no autorizados evitará cualquier conexión maliciosa de dichos dispositivos (como un receptor wifi por USB) a las computadoras en la red y, por lo tanto, evitará la apertura de un canal

para filtrar información hostil que pueda utilizar una persona de dentro de la organización. Este bloqueo se realiza definiendo un objeto de directiva de grupo (GPO, por sus siglas en inglés) o utilizando un software designado.



**Metodología de Ciberdefensa para Organizaciones > Categoría: Seguridad de los soportes físicos > 15.1**



## Defensa cibernética proactiva

Una defensa cibernética proactiva permite que una organización verifique constantemente sus líneas de defensa contra ataques cibernéticos y alteraciones. Al planificar e implantar este tipo de defensa, es aconsejable pensar desde la perspectiva del atacante y realizar simulaciones controladas de ataques a la infraestructura de la organización (como parte de las verificaciones de los sistemas). De esta manera, se trata de imaginar, por ejemplo, cómo se puede filtrar la información de una manera que eluda los sistemas de seguridad, etcétera.

### Hacer revisiones de seguridad de la información: abordar las amenazas internas

Como parte de la construcción de la arquitectura de red y la implementación de medidas de seguridad, las organizaciones

deben asegurarse de estar protegidas contra diversos escenarios, incluida la materialización de una amenaza interna, comenzando con riesgos cibernéticos en las estaciones de trabajo y hasta amenazas para toda la red de la organización. Es importante hacerlo realizando tanto revisiones teóricas (por un profesional que verifique la arquitectura) como prácticas (como pruebas de penetración y herramientas de mapeo de redes). Los resultados de las revisiones permitirán a las organizaciones identificar fallas en su arquitectura e implementación y repararlas en función de la gestión de riesgos.



**Metodología de Ciberdefensa para Organizaciones > Categoría: Evaluación de los controles de seguridad > 22.2 y 22.4**

## Identificar las fugas de información

Las organizaciones pueden identificar eventos de fuga de información buscando información sobre la propia organización en Internet (también en la web profunda). Estos eventos pueden deberse, entre otras cosas, a que una persona de dentro de la organización filtró la información de forma maliciosa o inadvertida.

Esta metodología puede implementarse de varias maneras:

# 01

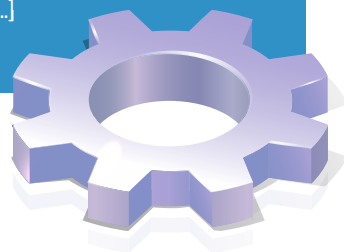
**Incluyendo textos subliminales en los documentos de la empresa** y luego buscando el texto en el motor de búsqueda de Internet.

# 02

**Contratando empresas de inteligencia cibernética** para identificar información sobre la organización que se filtró a Internet y a las redes profundas (canje de información, productos, etcétera).

## Recuadro 3. Caso real: uso de medios de almacenamiento para extraer información de la organización

En una de las empresas emergentes en Israel, **un empleado conectó un dispositivo móvil a una de las computadoras de la organización con el fin de robar información** y, al hacerlo, causó daños a la propiedad intelectual de la empresa, a la propia empresa y también al Estado. De acuerdo con la demanda, cuya publicación fue permitida (Caso de delito grave 06-18): “El 12/05/2018, entre las 16:30 y las 17:00, o alrededor de esa hora, y el 27/05/2018 alrededor de las 23:20, el acusado buscó en Internet utilizando el motor de búsqueda de Google para aprender cómo comerciar con capacidades cibernéticas de las que había tomado posesión y ver a quién podría vendérselas. [...] Para este fin, el acusado se conectó al servicio de correo electrónico Mail2Tor, un servicio encriptado anónimo que opera en la red oscura y está diseñado para evitar rastrear a sus usuarios [...] Alrededor del 2/06/2018, ofreció a [...] venderle todas sus capacidades por US\$50.000.000”.



Metodología de Ciberdefensa para Organizaciones > Categoría: Ciberdefensa proactiva > 23.2



## Implementar honeypots

Otra forma de identificar amenazas internas es mediante el uso de un enfoque proactivo para crear y planificar trampas de miel (*honeypots*).

Un *honeypot* crea un atractivo cebo de información para capturar a personas de la organización o partes que son puestas a prueba dentro de la organización, de quienes se sospecha que intentan conseguir información confidencial y llegar a determinadas carpetas o directorios (como la base de datos de clientes de la organización).

**El objetivo de utilizar un honeypot es identificar ataques en su entorno controlado y extraer conclusiones a fin de aumentar el nivel de defensa de la red.** Hay dos tipos de honeypots:

### 01

**Honeypots de investigación:** se utilizan para aprender las tácticas y técnicas de los hackers, los indicadores de ataque, etcétera.

### 02

**Honeypots de producción:** es el más común y lo utilizan las organizaciones en un entorno de trabajo aislado. Son efectivos, relativamente fáciles de planificar y operar, y pro-

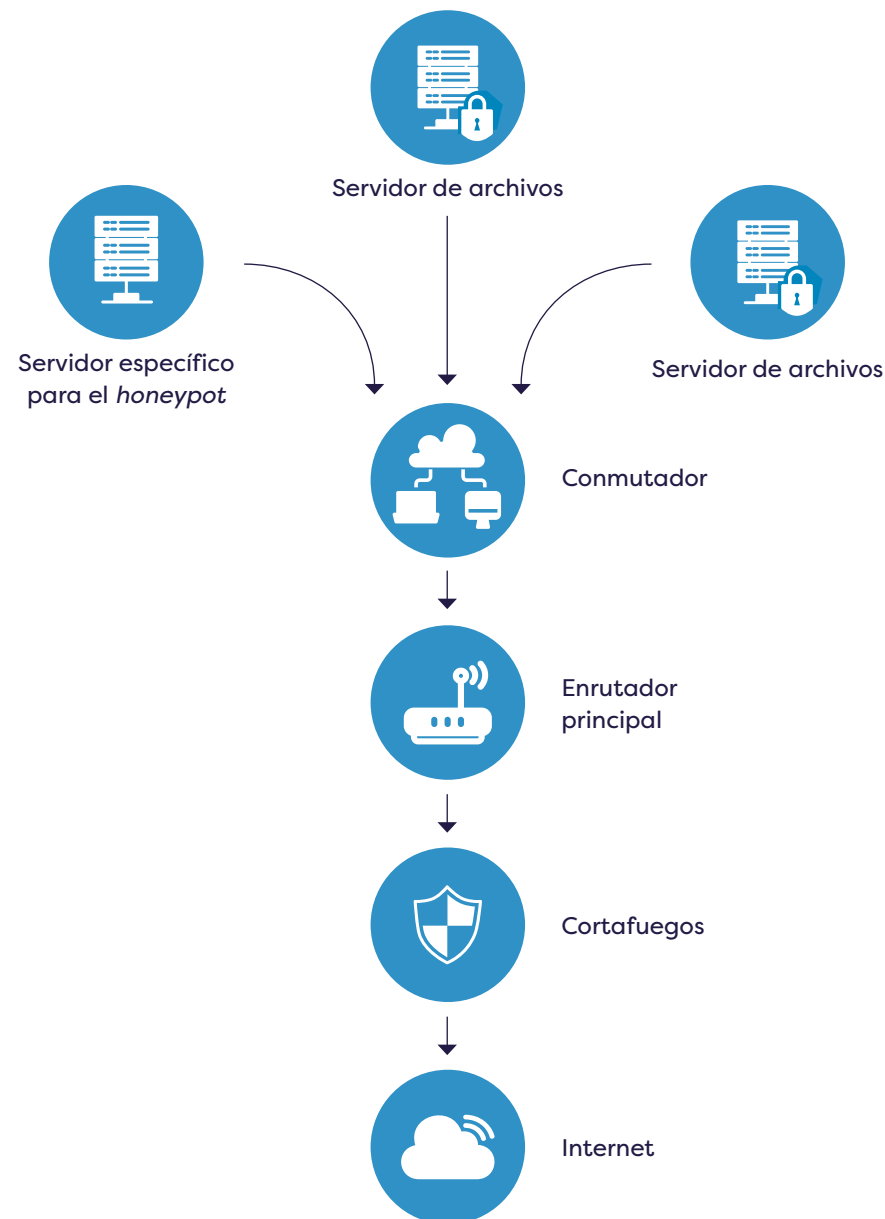
porcionan una defensa inmediata para los recursos de la organización.

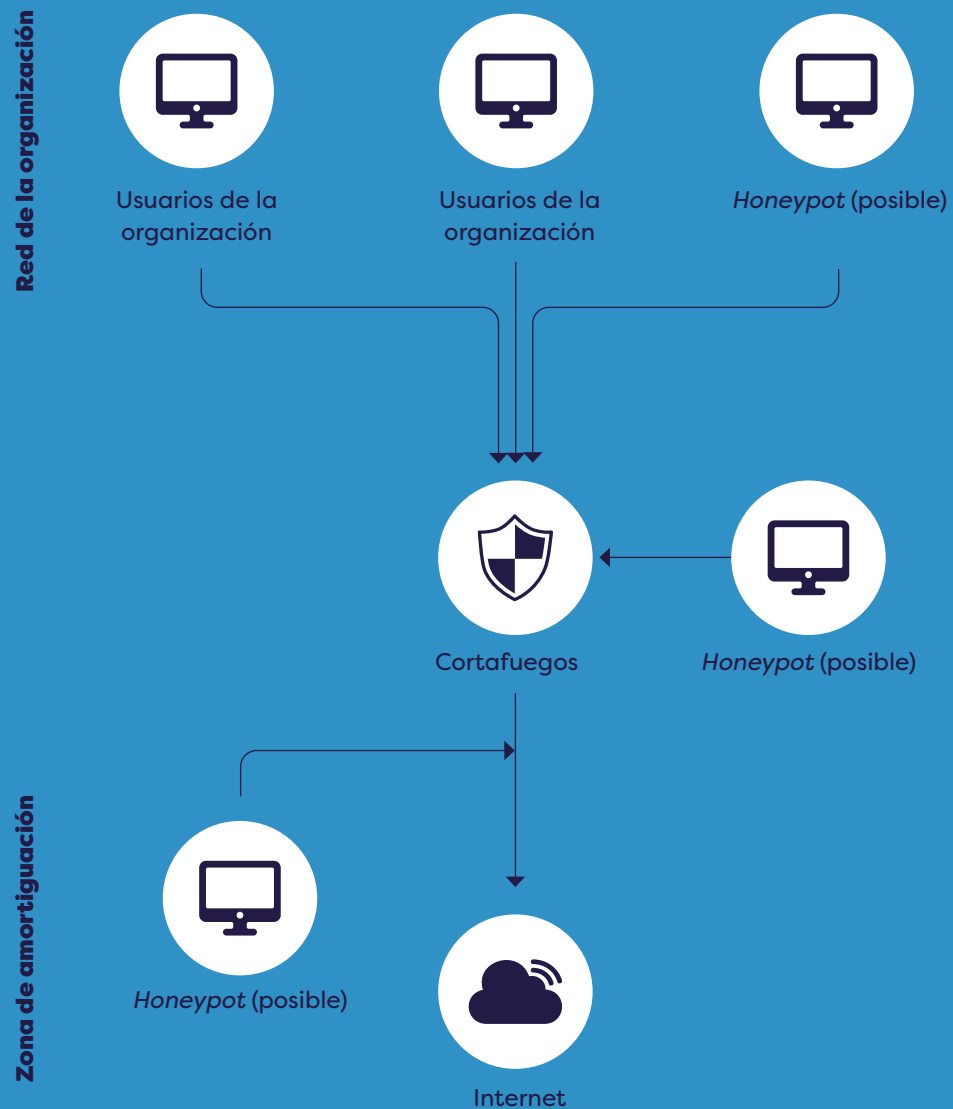
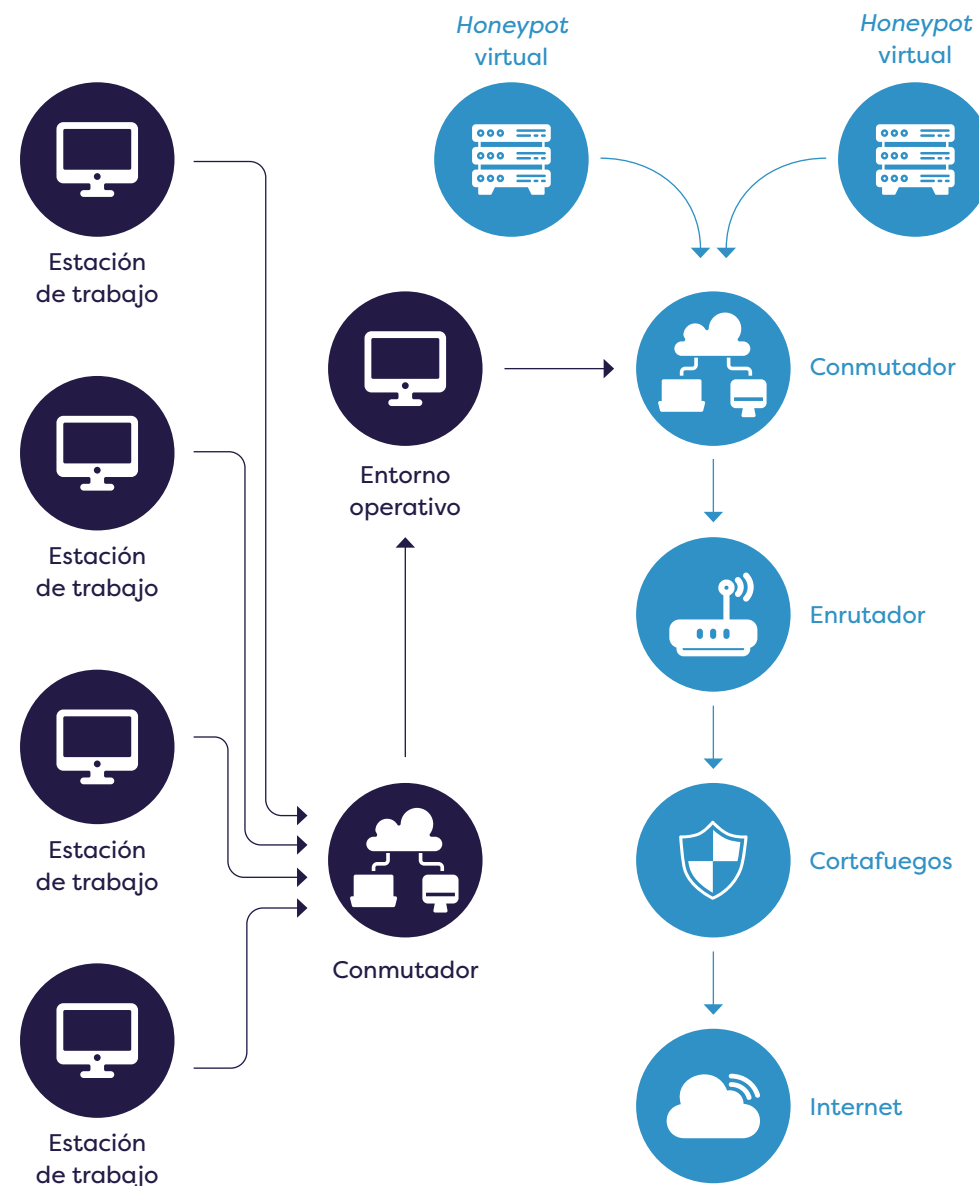
La planificación de un *honeypot* se basa en activos ficticios o recursos que se ponen en la red de la organización que incitan a una parte hostil a tratar de comunicarse con ellos y exponen el hecho de que se está llevando a cabo una actividad ilegítima en la red. Colocar un *honeypot* en una red permite detectar actividades sospechosas que podrían indicar una amenaza por parte de una persona de dentro de la organización, o por alguien que esté siendo explotado. Se puede colocar en una red de servidor, en una estación de trabajo o en usuarios de la red. **El honeypot diseñado debe ser atractivo y vulnerable a los ataques**, pero la ventaja de usar un *honeypot* es que no pone en peligro las aplicaciones y servicios de red reales de la organización. Existen productos que establecen *honeypots* en una red o, alternatively, se pueden crear *honeypots* de manera independiente (a nivel de la organización), por ejemplo, mediante el monitoreo de archivos ficticios etiquetados con un nombre sensible (como “salarios de los empleados”, “resúmenes de reuniones de gestión”, “base de datos de clientes de la empresa”, etcétera).

La estrategia para crear un *honeypot* se basa en la capacidad de engañar y hacer que un atacante caiga en la trampa y quede expuesto.

La planificación de un *honeypot* en varios entornos puede verse en los gráficos 4, 5 y 6.

**Gráfico 4.** *Honeypot* en un entorno de red (colocado detrás del cortafuegos)



**Gráfico 5.** Honeypot en un entorno de red (colocado delante del cortafuegos)**Gráfico 6.** Honeypot en un entorno de red (duplicando un entorno organizacional)



Como parte del proceso de planificación y con el fin de establecer un entorno creíble, se deben crear “usuarios del honeypot” para generar un volumen de actividad y simular un entorno organizacional. **Las principales recomendaciones para definir a los usuarios del honeypot son las siguientes:**

# 01

Elija nombres de usuarios del honeypot que resulten creíbles.

# 02

Cree usuarios locales con privilegios específicos, en lugar de usuarios con privilegios de dominio.

# 03

Otorgue a los usuarios del honeypot todas las autorizaciones legítimas en la organización para que los nombres de usuario no despierten la sospecha del hacker.

# 04

Defina los nombres de los usuarios del honeypot en el software de monitoreo espe-

cífico para que reciba alertas adecuadas si ocurre un evento.



**Metodología de Ciberdefensa para Organizaciones > Categoría: Ciberdefensa proactiva > 23.5**

## Gestionar y notificar incidentes

Las organizaciones deben desarrollar procedimientos de respuesta frente a incidentes cibernéticos.

Los procedimientos de respuesta incluyen varias etapas: **identificar, contener, investigar, erradicar y restaurar la rutina**. Las organizaciones deben incluir escenarios de amenazas internas en estos procedimientos y desarrollar metodologías para manejar estos eventos de manera acorde.



**Metodología de Ciberdefensa para Organizaciones > Categoría: Gestión de eventos e informes > 24.7**



**A.04** Recomendaciones de defensa:  
La amenaza interna

## Recomendaciones legales

Las organizaciones deben hacer que todos sus empleados firmen una declaración de confidencialidad y una obligación de trabajar de conformidad con los procedimientos de la compañía. Además de servir como un mecanismo de concienciación, disuasión y aviso que utiliza el administrador de seguridad de datos, el acuerdo de confidencialidad puede proporcionar a las organizaciones una cobertura legal adecuada. Es aconsejable que todos los empleados firmen un acuerdo de confidencialidad al ser contratados y antes del cese de la relación laboral.



**Metodología de Ciberdefensa para Organizaciones > Categoría: Recursos humanos y sensibilización de los empleados > 19.2**



## Prevención de accesos y seguridad física

La seguridad física y la prevención de accesos a las computadoras y la infraestructura informática son esenciales. El objetivo de este perímetro de seguridad es evitar o limitar el acceso de los empleados a complejos o áreas que no son esenciales para el desempeño de sus trabajos y evitar que personas internas hostiles accedan a estas áreas. Al planificar los sistemas de seguridad física las pautas incluyen el establecimiento de controles de seguridad adecuados que impidan el acceso a los activos informáticos o, al menos, lo dificulten. Se recomienda que estos perímetros de seguridad física incluyan controles preventivos, como puertas bloqueadas y portones electrónicos, y controles de detección, como cámaras (que también serán útiles para investigar incidentes) y sistemas de alarma.

Otro principio importante cuando se planifican sistemas de seguridad física es el de acceso únicamente con permisos, a fin de prevenir y limitar la exposición de los empleados a áreas de trabajo que no son esenciales para su labor. La definición de permisos de entrada a áreas particulares según la naturaleza de sus trabajos y la “necesidad de saber” reduce el riesgo de que una persona de dentro de la organización obtenga acceso físico a sistemas informáticos sensibles (como servidores y salas de comunicaciones).

Es importante que el diseño de los sistemas de control de entrada incorpore varios controles de identificación:

# 01

**Algo que se tiene** (como una tarjeta de acceso, identificación por radiofrecuencia [RFID, por sus siglas en inglés], teléfono celular, etcétera).

# 02

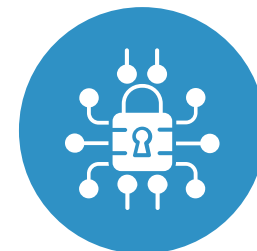
**Algo que se sabe** (como las contraseñas de acceso a un teclado numérico, RFID, teléfono celular).

# 03

**Algo que se es** (basado en una identificación biométrica, como una huella digital, escaneo de la retina, reconocimiento facial, etcétera).



**Metodología de Ciberdefensa para Organizaciones > Categoría: Seguridad de los soportes físicos > 15.3**



## Verificación de empleados y confiabilidad

La verificación de los empleados debe llevarse a cabo durante su proceso de selección y como parte de los procesos de evaluación, y su propósito es predecir si un candidato podría ser problemático. Un empleado con un perfil de comportamiento potencialmente problemático podría significar una amenaza cibernética en caso de que este sufra un problema financiero, personal o de otro tipo. La verificación de los empleados utiliza herramientas subjetivas y objetivas, y se puede hacer usando agencias de colocación privadas, dependiendo de lo delicado que sea el trabajo (por ejemplo, para los empleados a los que se otorgarán privilegios elevados para acceder a las computadoras de la organización), costos de verificación, leyes locales e implicaciones legales.

## Capacitación y sensibilización de los empleados

Muchos ataques son cometidos por terceros que engañan a los empleados de una organización. Un ejemplo típico de este tipo de ataque es un *phishing*, es decir, cuando un atacante se hace pasar por un contacto legítimo y se gana la confianza de la víctima para obtener acceso interno a los sistemas informáticos. Este tipo de ataque<sup>6</sup>, que se denomina ingeniería social, es un componente muy común de los ciberataques. Por lo tanto, los planes de trabajo de las organizaciones deben incluir análisis de riesgos cibernéticos, capacitación de los empleados y su concienciación sobre las amenazas cibernéticas (NIST, 2003). El plan de capacitación y concienciación debe proporcionar un nivel adecuado de información para que los empleados puedan reconocer los riesgos y familiarizarse con las tácticas y técnicas de los atacantes y poder así detectar incidentes sospechosos.

Aumentar la sensibilización de los empleados puede reducir el riesgo de que personas de la organización sean engañadas y explotadas por un atacante externo y minimizar así el daño potencial de un ataque.

Cuando se contrata a un nuevo empleado, este debe recibir instrucciones para aumentar su conocimiento de los riesgos cibernéticos y estar alerta ante las amenazas cibernéticas en su entorno de trabajo en la organización y en su propia estación de trabajo. Se debe proporcionar capacitación de manera regular para aumentar la concienciación de los empleados (al menos una vez al año).

La capacitación debe incluir herramientas y servicios que permitan a los empleados obtener experiencia práctica utilizando ataques de *phishing* simulados, ingeniería social, etcétera.



# Referencias

- Cyber Security Insiders y Crowd Research Partners. 2018. Insider Threat. 2018 Report. Disponible en: <https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf>.
- NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos). 2003. Building an Information Technology Security Awareness and Training Program. Disponible en: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>.

6. Conferencia de Patrick Reidy del Buró Federal de Investigaciones (FBI, por sus siglas en inglés) durante Black Hat Estados Unidos 2013, disponible en: [https://www.youtube.com/watch?v=\\_xKmp\\_t04il&feature=youtu.be](https://www.youtube.com/watch?v=_xKmp_t04il&feature=youtu.be).

# Anexos

## Anexo 1. Verificación de controles

**Cuadro A1.1.** Ejemplo de ejecución de evaluación de riesgos para un activo de información

Categoría	Control	Totalmente completado	Parcialmente completado	No realizado
Proteger	<b>Evitar el acceso a servicios de almacenamiento en la nube</b> Minimizar fugas de dentro de la organización			
	<b>Realizar defensa proactiva</b> Como parte de la verificación de la efectividad de las líneas de defensa			
	<b>Implementar un cortafuegos interno</b> Obstaculizar la capacidad de un atacante para difundir un ataque en toda la red			
	<b>Supervisar y administrar los permisos de los usuarios</b> Para limitar la capacidad de un atacante de ejecutar un código malicioso que el software antivirus no reconozca			

Categoría	Control	Totalmente completado	Parcialmente completado	No realizado
Proteger	<b>Implementar la prevención de pérdida de datos</b> Como parte de la solución para identificar y prevenir la pérdida de datos en la organización			
	<b>Verificar a los empleados</b> Como parte del mecanismo para identificar a los candidatos para un empleo que puedan tener un perfil de comportamiento problemático			
	<b>Capacitar a los empleados</b> Como parte del proceso de aumentar su conocimiento de las amenazas cibernéticas, con énfasis en las amenazas cibernéticas internas			
	<b>Prevenir el acceso y aumentar la seguridad física</b> Como parte de la restricción del acceso a áreas sensibles			
Proteger	<b>Restringir el acceso a dispositivos USB</b> Como parte del proceso de minimizar las fugas de información de la organización			

Categoría	Control	Totalmente completado	Parcialmente completado	No realizado
Detectar	<b>Realizar revisiones de seguridad de datos</b> Identificar posibles fallas			
	<b>Identificar información de fugas</b> Como parte del mecanismo para identificar la información filtrada			
	<b>Implementar honeypots</b> Para detectar actividades sospechosas			
Identificar	<b>Implementar un monitoreo de comportamiento del usuario</b> Como herramienta para identificar amenazas internas basadas en comportamientos anómalos			
	<b>Establecer mecanismos legales</b> Hacer que los empleados firmen acuerdos de confidencialidad en el momento de la contratación y antes de la terminación del empleo			







**Estimados CISO y expertos en seguridad de la información y ciberprotección:**

El propósito de esta publicación es proporcionar recomendaciones para implementar métodos de trabajo que faciliten un mayor nivel de robustez y la capacidad de lidiar con las amenazas cibernéticas internas mediante la creación de perímetros de seguridad y la incorporación de métodos y tecnologías recomendados.

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

**A.01** Metodología de Ciberdefensa para Organizaciones Versión 1.0

**A.02** Metodología de Ciberdefensa para Organizaciones Versión 2.0

**A.03** Uso de servicios en la nube: Adenda a la Metodología de Ciberdefensa para Organizaciones

### ✦ **A.04** Recomendaciones de defensa: La amenaza interna

**A.05** Preparación organizacional para una crisis cibernética

**A.06** Cadena de suministro

**A.07** Preguntas de orientación para formuladores de políticas cibernéticas

**A.08** Recomendaciones de ciberseguridad y reducción de riesgos cibernéticos para pequeñas empresas

**A.09** Práctica cibernética: creación y edición de ejercicios de ciberseguridad para organizaciones

**A.10** Gestión de riesgos cibernéticos en entornos de tecnologías operativas (OT)

**A.11** Plantilla de evaluación de riesgo en el sector minorista

**A.12** Práctica cibernética: creación de planes de concientización para organizaciones

## **Volumen B:** Un enfoque técnico

## **Volumen C:** Desarrollo seguro de *software*

