

# Recomendaciones de ciberseguridad y reducción de riesgos cibernéticos para pequeñas empresas

Mejores Prácticas en Ciberseguridad



## A.08

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 seguridad de la información y reducción de riesgos cibernéticos para pequeñas empresas”. © (2018) 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), en colaboración con la división de Competitividad, Tecnología e Innovación (IFD/CTI), 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/he/Departments/policies/small\\_bussines](https://www.gov.il/he/Departments/policies/small_bussines). 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. Recomendaciones para pequeñas empresas

/Pág. 8

Recomendación 1: Capacitación de empleados

Recomendación 2: Mapeo de datos y evaluación de riesgos

Recomendación 3: *Software* con licencia

Recomendación 4: Antivirus

Recomendación 5: Actualización de *software*

Recomendación 6: Contraseñas sólidas de identificación y configuración de bloqueo luego de varios intentos fallidos de identificación

Recomendación 7: Cifrado de información como parte de la protección, ocultamiento de información comercial y datos de clientes

Recomendación 8: Copias de seguridad

Recomendación 9: Redes inalámbricas

Recomendación 10: Ciberseguros

## 02. ¿Su negocio está protegido?

/Pág. 16

# 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. Proliferaaron 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.

## Recomendaciones para pequeñas empresas

### Recomendación 1

### Capacitación de empleados

Es necesario priorizar e invertir en recursos para orientar a los trabajadores. En la mayoría de los casos, los ataques cibernéticos se basan en ingeniería social y debilidades humanas, lo cual permite engaños y fraudes dirigidos a los empleados de la organización. A su vez, esto posibilita que los ataques se extiendan al resto de los equipos conectados a la red corporativa.

Por lo tanto, un pilar muy importante es la implementación, coordinada por el área de

recursos humanos, de un programa de formación y concientización de empleados que contribuya a reforzar la seguridad y a prevenir ataques que utilizan ingeniería social, estafas de suplantación de identidad (*phishing*) o secuestro de datos (*ransomware*), bloqueo de archivos, etcétera.

Para obtener más detalles, consulte los identificadores 20.2 y 20.4 de la *Metodología de Ciberdefensa para Organizaciones* de la Dirección Nacional de Ciberseguridad.<sup>2</sup>

### Recomendación 2

### Mapeo de datos y evaluación de riesgos

La conectividad entre computadoras, las aplicaciones móviles y el uso de la nube, en-

tre otros factores, aumentan las oportunidades de ataques y la superficie de ataque. **Un proceso de mapeo permitirá identificar los riesgos existentes en activos y sistemas informáticos de la empresa.** Esto debe hacerse con la ayuda de un experto en ciberseguridad —ya sea empleado propio o externo— y con base en las amenazas más conocidas, las debilidades que presentan los sistemas y las medidas de seguridad existentes.

Este proceso es fundamental e influye en la definición de políticas de seguridad informática, en **el plan a implementar y en el establecimiento de prioridades para hacer frente a las fallas de seguridad y mitigar de manera concreta los potenciales riesgos.**

Un ejemplo de mapeo de datos y evaluación de riesgos puede darse en el contexto de un sistema de compensación de clientes que incluya una descripción general de cómo se realiza la compensación, cuál es el nivel de protección de dicho sistema en puntos de venta, cómo se procesa la información y base de clientes, el nivel de permisos y usuarios, etcétera.

Para obtener más detalles, véase el apartado sobre asignación de activos de la *Metodología de Ciberdefensa para Organizaciones* de la Dirección Nacional de Ciberseguridad. En el cuadro 1 se presenta un ejemplo de mapeo de riesgos.



2. La *Metodología de Ciberdefensa para Organizaciones* se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad.

Recomendación 3

Software con licencia

Su uso garantiza un proceso ordenado de actualizaciones de seguridad. Utilizar *software* sin licencia o pirateado es una oportunidad atractiva para un ataque, en parte debido a que se pueden explotar vulnerabilidades en ausencia de actualizaciones de seguridad recientes. Por este motivo, debe asegurarse la equipación e instalación de *software* con licencia en el proceso de adquisición de bienes y servicios.

Recomendación 4

Antivirus

Es un *software* diseñado para detectar virus informáticos y proteger la actividad de sus equipos. Su finalidad es localizar el *software* malicioso (*malware*) mediante firmas predeterminadas. Compruebe con su personal de tecnologías de la información (TI) o con los proveedores de servicios informáticos que el *software* antivirus se instalará en todas las computadoras de la empresa, incluidos los servidores, y que se actualizará con frecuencia, al menos una vez al día. Puede instalarse de manera local, aunque también existen versiones en línea y de diferentes tipos.<sup>3</sup>

Para obtener más detalles, véase el identificador 7.3 de la *Metodología de Ciberdefensa para Organizaciones* de la Dirección Nacional de Ciberseguridad, que está disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad.



3. Más información disponible en: <https://www.gartner.com/reviews/market/endpoint-protection-platforms>.

Cuadro 1. Mapeo de riesgos

Tipo de activos	Nombre y fabricante	Propósito	Local / nube	Interfaces	Observaciones
Aplicación organizacional					Por ejemplo, almacén de datos (DWH, por sus siglas en inglés), gestión de relaciones con clientes (CRM, por sus siglas en inglés), planificación de recursos empresariales (ERP, por sus siglas en inglés), sistema informatizado de gestión de almacenes (WMS, por sus siglas en inglés), sistema de nómina, portal de la organización, etc.
Infraestructura					Por ejemplo, equipos de comunicación, telefonía, correo electrónico, almacenamiento.
Red					Por ejemplo, red de área local/ red de área amplia (LAN/WAN, por sus siglas en inglés), inalámbrica, óptica, satelital.
Tecnología operativa (OT)					Por ejemplo, circuitos cerrados de televisión, sistemas de interfaz hombre-máquina (HMI, por sus siglas en inglés), controladores, etc.

Fuente: Dirección Nacional de Ciberseguridad (2017).

Recomendación 5

Actualización de software

El personal informático debe configurar actualizaciones automáticas en todo el *software* instalado. Esto es especialmente crítico en sistemas operativos y en *software* utilizado de manera frecuente, como por ejemplo Microsoft Office.

Esto asegurará que el *software* instalado en la empresa tenga siempre las últimas actualizaciones de seguridad y se reduzca significativamente la capacidad de un atacante de explotar vulnerabilidades en el *software* de la empresa. Para obtener más detalles, véase el identificador 7.9 de la *Metodología de Ciberdefensa para Organizaciones* de la Dirección Nacional de Ciberseguridad.

## Recomendación 6

## Contraseñas sólidas de identificación y configuración de bloqueo luego de varios intentos fallidos de identificación

Uno de los canales de ataque más comunes es el intento de ciberataque basado en descifrar contraseñas. El atacante está equipado con una especie de diccionario de contraseñas que consta de millones de combinaciones posibles y que se ejecuta durante el proceso de ataque.

Por lo tanto, utilizar una contraseña simple permite descifrar y acceder con facilidad a los sistemas informáticos. Es recomendable entonces que a través del equipo de TI de la empresa o de los proveedores de servicios informáticos se establezcan contraseñas extensas y difíciles de descifrar, que consistan en una combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Además, utilizar un mecanismo de autenticación de dos factores (2FA) crea una capa de seguridad adicional, genera una buena respuesta a los intentos de robo de contraseñas e incluso es efectivo en casos de *phishing*. Estos sencillos pasos reducen el riesgo de ataques basados en la predicción de contraseñas.

## Recomendación 7

## Cifrado de información como parte de la protección, ocultamiento de información comercial y datos de clientes

Su propósito es mantener la confidencialidad de los datos de terceros no autorizados. Las soluciones criptográficas proporcionan un mecanismo para almacenar la información de forma cifrada tanto en los servidores como en las computadoras de la empresa, además de circuitos de seguridad adicionales. Un ejemplo de ello es requerir el protocolo seguro de transferencia de hipertexto (HTTPS, por sus siglas en inglés) al proveedor de *hosting*. El proceso de encriptación realizado por el equipo de TI de la empresa o a través del proveedor de servicios requiere equiparse con el *software* apropiado, gestión de claves de cifrado, etcétera.



## Recomendación 8

## Copias de seguridad

Un proceso regulado de respaldo habilita la capacidad de recuperarse de distintos tipos de ciberataque. El mejor ejemplo se da en el caso del secuestro de datos, mediante el cual un *software* malicioso cifra toda la información existente en una computadora específica o en la red corporativa.

En esas circunstancias se puede restaurar la información a través de copias de seguridad actualizadas y así evitar daños más severos en el negocio. Existen diversos métodos de copia de seguridad: local, en la nube o a través de la impresión de una copia física. También puede realizarse una triple copia de seguridad destinada a reducir la pérdida de información en el proceso de respaldo inicial o secundario.

Estas copias de seguridad pueden alojarse en discos externos que contengan información crítica de la organización. La forma de identificar y localizar dicha información es a través del mapeo de datos.

Las copias de seguridad también pueden efectuarse en un sitio alternativo al que se traslade el negocio ante un eventual desastre. La modalidad de respaldo se seleccionará de acuerdo a la naturaleza única del negocio, del nivel

de criticidad y de la capacidad de la empresa para invertir en diversas soluciones de respaldo. Es necesario asegurarse con el personal de TI de que existe un proceso de copias de seguridad acorde a las recomendaciones.

Para obtener más detalles, véase el identificador 25.12 de la *Metodología de Ciberdefensa para Organizaciones* de la Dirección Nacional de Ciberseguridad (disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad).

## Recomendación 9

## Redes inalámbricas

Su uso es muy común en estos días, tanto con el objetivo de operar los sistemas informáticos de la empresa como para brindar a los clientes servicio y acceso a Internet. Al instalar una red inalámbrica en la oficina, es aconsejable instruir al personal de TI para que se adhieran a las siguientes reglas:

# 01

Realizar una separación completa entre la red comercial y la red del cliente. Se recomienda configurar dos redes inalámbricas diferentes, de modo que los clientes (o quienes utilicen el servicio) no puedan obtener acceso no autorizado a los sistemas comerciales.



## 02

Requerir al proveedor de infraestructura la siguiente configuración en la red empresarial:

- **Cifrado:** utilización del medio de cifrado más fuerte. Al momento de escribir esta publicación es el sistema Wi-Fi Protected Access 3 (WPA3).
- **Contraseña:** una clave de red larga y compleja que se reemplace periódicamente.
- **Endurecimiento basado en direcciones de control de acceso a medios (MAC,** por sus siglas en inglés) que se conectan al router inalámbrico, como el filtrado de listas blancas.
- **Ocultamiento de la red** (identificador del conjunto de servicios [SSID, por sus siglas en inglés]) para quienes escanean las redes inalámbricas de la zona.
- **Gestión del router:** debe modificarse la contraseña predeterminada para el administrador del router.



## 03

Probar las soluciones de cifrado para componentes inalámbricos adicionales tales como teclados, mouses e impresoras.

### Recomendación 10

## Ciberseguros

A pesar de todos los mecanismos de defensa existentes, los ataques cibernéticos logran aun así dañar a las empresas. La forma de minimizar el daño económico de un ataque exitoso es contratar un seguro cibernético, que cubrirá al negocio en caso de perjuicio económico como resultado de un ciberataque. Debe tenerse en cuenta que, como cualquier otro seguro, el cibernético requiere que la empresa implemente un nivel básico de protección para tener derecho a una indemnización. Más allá de minimizar el daño económico, este proceso ayudará a la supervivencia empresarial y a recuperarse frente a eventuales desastres.



# /02.

## ¿Su negocio está protegido?

En el cuadro 2 se presenta un compendio de recomendaciones de ciberseguridad y reducción de riesgos cibernéticos para pequeñas empresas



**Cuadro 2.** Recomendaciones de ciberseguridad y de reducción de riesgos cibernéticos

Recomendaciones	Implementación	Frecuencia	Adicional
Concientización de empleados	Programa de orientación, página de instrucciones, correo electrónico, carteles en todas las oficinas.	A medida que aumente la frecuencia de la implementación, mayor será la conciencia de los empleados. La frecuencia mínima es una vez al año.	Puede obtener ayuda de empresas especializadas en campañas de concientización para empleados.
Mapeo de datos y evaluación de riesgos	Entrevistas a todos los miembros de la empresa para conocer la localización de todos los datos de la empresa. Evaluaciones de riesgo orientadas a señalar áreas donde se requiere mayor seguridad.	Alineación inicial y luego actualización anual.	Se recomienda preparar un cuestionario con anticipación. Véase el cuadro 1 sobre mapeo de riesgos.
Software con licencia	Comprobar que todo el software instalado posea la licencia correspondiente para la empresa, como parte de un proceso que garantice las actualizaciones de seguridad.	La encuesta de software legítimo se realiza una sola vez, después de la cual cada nuevo software debe adquirirse con una licencia válida.	Es recomendable establecer un procedimiento de trabajo para la compra de software, a fin de asegurarse de que todos los empleados de la organización sean conscientes de la importancia de utilizar software legal y actúen en consecuencia.

Recomendaciones	Implementación	Frecuencia	Adicional
Antivirus	Configurar actualizaciones automáticas.	Depende de la gestión de riesgos y necesidades de la organización o de las recomendaciones del fabricante.	
Actualización de software	La prioridad más alta es para el sistema operativo. Todos los sistemas operativos incluyen la opción de actualizaciones automáticas. Es recomendable asegurarse de que todos los sistemas informáticos de la empresa estén realmente configurados para garantizar el cierre de brechas mediante parches de seguridad.	Evaluar la efectividad de las actualizaciones automáticas frente a las periódicas.	La mayoría del software se configura automáticamente para efectuar las actualizaciones del fabricante.
Contraseñas sólidas de identificación	Se recomienda buscar la ayuda de un consultor de seguridad informática o un integrador de sistemas sólidos de identificación para la creación de una política de contraseñas adecuada. Incorporar un mecanismo de autenticación de dos factores (2FA) contra intentos de <i>phishing</i> y robo de contraseñas.	El establecimiento de un sistema de identificación fuerte se hace una sola vez.	

Recomendaciones	Implementación	Frecuencia	Adicional
Cifrado de datos	Pruebe y asegúrese de que el tráfico y almacenamiento de información confidencial se realice en una plataforma cifrada.	La evaluación de riesgos se relaciona con la sensibilidad de los datos en cada combinación de una nueva aplicación o software.	
Copias de seguridad	El método de respaldo depende del volumen de información respaldada y la frecuencia requerida. Se puede realizar con varios métodos, como copia de seguridad en frío ( <i>offline</i> ) o en caliente ( <i>online</i> ), de manera que permita la recuperación y accesibilidad de la información si es necesario.	Depende del nivel de importancia de la información de la copia de seguridad.	Se recomienda buscar la ayuda de un especialista en copias de seguridad y recuperación ante desastres.
Redes inalámbricas	Se debe solicitar al proveedor de servicios de internet o configurar el router para fortalecer las contraseñas.	Ajustes preliminares se hacen una única vez. Las contraseñas deben modificarse una vez al año.	Se recomienda guardar las contraseñas en una copia impresa, en un lugar protegido.
Ciberseguros	Como cobertura adicional ante ciberataques y como plan de continuidad del negocio (BCP, por sus siglas en inglés) y capacidad de recuperación ante desastres.		



Las amenazas cibernéticas constituyen un riesgo para la sociedad y la economía israelí. Como tales, están dirigidas a todos los sectores y no distinguen entre grandes, medianas o pequeñas empresas.

En los últimos años, los ataques dirigidos a los sectores económicos se han basado en tecnologías y métodos sofisticados. La piratería informática ejercida sobre pequeñas empresas puede causar daños significativos, como la eliminación de bases de datos, daños operacionales, financieros y reputacionales. Los ataques pueden incluso paralizar y destruir la actividad empresarial.

Actualmente, el nivel de seguridad promedio de una organización pequeña es insuficiente frente a las amenazas cibernéticas y sus métodos de ataque. Las pequeñas empresas son una parte importante de la economía israelí y su relevancia para la economía es significativa. Por ende, es necesario aumentar la robustez de su ciberseguridad.

En consecuencia, el propósito de esta publicación es orientar a las pequeñas empresas y esbozar un nivel básico de protección, que ayude a reducir los riesgos cibernéticos y minimice los daños potenciales.

La información también es adecuada para empresas que no empleen personal de ciberseguridad a tiempo completo, ya que describe los pasos básicos para la protección de sistemas informáticos, información empresarial y de clientes. De esta manera, es posible exigir como requisitos estos pasos a técnicos de la empresa, proveedores de servicios informáticos y de TI.

Además, se debe prestar atención a la posibilidad de que se apliquen costos adicionales al negocio, en virtud de estar sujeto a las regulaciones existentes (en términos de privacidad, materiales peligrosos, etcétera).



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*

