Preparación y respuesta ante un ataque de *ransomware* en la organización

Mejores Prácticas en Ciberseguridad

B.07

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título *Mejores prácticas: Preparación y respuesta ante un evento de secuestro de datos (ransomware) en la organización.* © (2021) Dirección Nacional de Ciberseguridad de Israel.

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).

El documento original se encuentra disponible en el siguiente enlace: **https://www.gov.il/he/pages/rasomware_org**. 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."

Índice

Prólogo

La transformación digital y el reto de la ciberseguridad

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

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

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

Israel, líder en ciberseguridad a nivel mundial

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

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

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

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

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

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

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

¿Qué hace el BID para apoyar a la región?

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

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

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

El BID y la INCD: uniendo esfuerzos

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

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

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

Listado de siglas

Sigla	Definición
BCP	Plan de continuidad del negocio
CIO	Gerente de sistemas de información
CISO	Director de seguridad de la información
DDoS	(Ataque) distribuido de denegación de servicio
DFIR	Análisis forense digital y respuesta ante incidentes
DR	Recuperación ante desastres
INCD	Dirección Nacional de Ciberseguridad de Israel
IOA	Indicador de ataque
IOC	Indicador de compromiso
IOE	Indicador de exposición
MDR	Detección y respuesta gestionadas
MSSP	Proveedor de servicios de seguridad gestionados
RPO	Objetivo de punto de recuperación
RTO	Objetivo de tiempo de recuperación
SLA	Acuerdo de nivel de servicio

Introducción

El *ransomware*, o secuestro de datos, es un *software* malicioso (*malware*) que tiene como objetivo impedir que el usuario atacado pueda acceder a un activo cibernético y a la información almacenada en este. Como condición para eliminar la restricción de acceso, el atacante puede presentar varias condiciones al usuario atacado, como el pago de un rescate.

Un ataque con *ransomware* podría ser un incidente cibernético con una gran importancia para las organizaciones activas en el sector económico. En el marco de un ataque, es habitual que un atacante cifre la información en poder de la organización y condicione la remoción del cifrado al pago de una remuneración, por ejemplo, la transferencia de dinero digital al atacante. En otras palabras, el atacante puede chantajear a la organizar exigiendo una remuneración como condición para remover dicho cifrado. En caso de que la organización no cumpla con las exigencias del atacante y no tenga una manera efectiva de recuperar la información, podría sufrir daños irreversibles, y llegar incluso a la quiebra.

En los últimos años, se ha constatado que los atacantes en el ciberespacio emplean un modelo de ataque más avanzado al hacer uso de *ransomware*, la llamada doble extorsión (*double extortion*). Este modelo se basa en dos fases de ataque principales. En la primera, el atacante realiza una filtración de información sensible/confidencial de la organización. En la segunda fase, utiliza un cifrado para evitar el acceso a los activos cibernéticos y la información de la organización, tras lo cual puede publicar sus condiciones para eliminar la restricción de acceso. Para el atacante, la ventaja en este modelo es que, incluso si la organización consiguiese recuperar la información y los activos cibernéticos, su temor a que se divulgue la información sensible/confidencial (y de las consecuencias resultantes de ello) podría llevarla a cumplir con las exigencias del atacante.

Recientemente se han descubierto algunos casos en los que se empleó un modelo de ataque aún más avanzado, llamado triple extorsión (*triple extortion*), que, como su propio nombre indica, se basa en tres fases de ataque principales. En la primera, el atacante realiza una filtración de información sensible/confidencial de la organización. En la segunda, utiliza un cifrado para evitar el acceso a los activos cibernéticos y la información de la organización, tras lo cual publica sus condiciones para eliminar la restricción de acceso. Finalmente, en la tercera fase, el atacante se dirige a terceros (por ejemplo, clientes de la organización) a quienes exige el pago de un rescate como condición para no divulgar su información sensible/confidencial; o alternativamente, el atacante amenaza con realizar otro ataque contra la organización, por ejemplo, un ataque distribuido de denegación de servicio (DDoS, por sus siglas en inglés) si sus exigencias no se cumplen. Para el atacante, la ventaja de este modelo es que, incluso si la organización consiguiese recuperar la información y los activos cibernéticos, el temor de la organización atacada o del tercero de que se divulgue la información sensible/confidencial (y de las consecuencias de ello), sumado a la posibilidad de recibir un ataque adicional, podría llevar a la organización a cumplir con las exigencias del atacante.

De esta forma, aunque la organización lograse recuperarse con éxito de un ataque con *ransomware*, aún existirá un alto nivel de exposición de la organización y de la información de terceros (por ejemplo, los clientes de la organización).

Cabe destacar que, en los últimos años, los atacantes en el ciberespacio han comenzado a adoptar un modelo de *ransomware* como servicio (RaaS, por sus siglas en inglés), lo que les da acceso a herramientas de ataque avanzadas a aquellos con capacidades tecnológicas limitadas o que no estén interesados en invertir amplios recursos en investigación y desarrollo.

Por otra parte, hay una serie de informes de diversos países acerca del uso de un *ransomware* que implementa varias capas de cifrado independientes. En este tipo de ataques, cada capa de cifrado tiene una clave de descifrado única y se exige un pago por separado para recibir cada una de las claves. Asimismo, existe un informe inicial acerca de la existencia de modelos comerciales más avanzados por parte de los atacantes que emplean *ransomware*, tales como la venta de claves de descifrado adaptadas según parámetros, como el volumen de información que pueda recuperarse, el tipo de archivos que puedan recuperarse, la velocidad/duración esperada del descifrado, el descifrado de metadatos (*metadata*) únicamente o el descifrado de información bruta completa.

/01.
Finalidad y objetivos

La finalidad de la presente publicación es ayudar al Director de Seguridad de la Información/ Gerente de Ciberseguridad (CISO, por sus siglas en inglés) y a las partes responsables pertinentes a hacer frente a un incidente de *ransomware* en la organización.

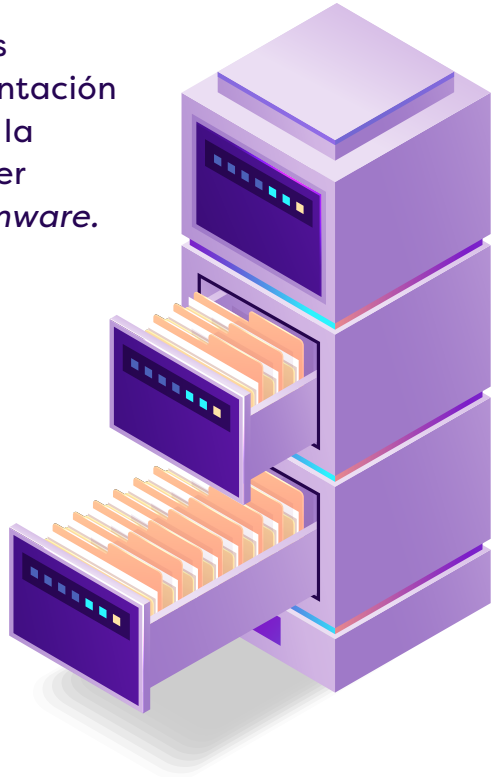
/02.
Grupo destinatario

Esta publicación ha sido elaborada para los CISO y las partes responsables pertinentes en la organización.

Otras partes que podrían beneficiarse con este documento son los Gerentes de Sistemas de Información (CIO, por sus siglas en inglés), los profesionales de metodología de ciberseguridad, los profesionales de implementación de ciberseguridad, los responsables de tecnologías de ciberseguridad (arquitectos de ciberseguridad), así como el personal de comunicación de datos/informática/tecnologías de la información (TI) y sistemas.

/03. Alcance de la publicación

La publicación se centra en las recomendaciones de implementación para mejorar la capacidad de la organización a la hora de hacer frente a incidentes con *ransomware*.



Cabe mencionar que esta publicación no incluye una ampliación relativa a cuestiones sobre las que la INCD ha elaborado y publicado documentos específicos. Un ejemplo es la protección individual del sistema y la infraestructura, que se aborda en el marco de la ***Metodología de ciberdefensa para organizaciones 2.0***, elaborada y publicada por la INCD.[2]

2. La ***Metodología de ciberdefensa para organizaciones 2.0*** se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-20-mejores-practicas-en-ciberseguridad**.

/04. Amenazas resultantes de un ataque de *ransomware*

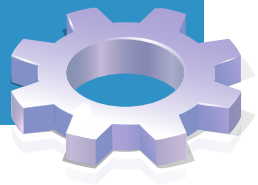
En esta sección se describen las principales amenazas que resultan de un ataque de *ransomware*.

Cuadro 1. Principales amenazas resultantes de un ataque de *ransomware*

N.°	Amenaza	Descripción
1	Denegación de acceso a la información	a. El atacante podría cifrar la información, de manera de impedir que accedan a ella las personas autorizadas. b. El atacante podría borrar información, incluyendo las copias de seguridad existentes.
2	Enmascaramiento de datos	El atacante podría enmascarar datos, afectando a la fiabilidad de la información. Un ejemplo de ello sería cambiar el orden de aparición o la ubicación de registros en las bases de datos.
3	Filtración de información sensible/ confidencial	El atacante podría filtrar información sensible/ confidencial como paso previo a la activación del *ransomware*, o bien durante su activación.

N.°	Amenaza	Descripción
4	Extorsión	a. El atacante podría exigir una remuneración económica o de otro tipo como condición para facilitar la clave del cifrado o el enmascaramiento. b. Doble extorsión: el atacante podría amenazar con lanzar otra amenaza en paralelo al *ransomware* (por ejemplo, realizar un ataque DDoS) a fin de incrementar la intensidad de los daños. c. Triple extorsión: el atacante podría dirigirse a un tercero y exigirle una remuneración, indicando que, en caso de no cumplir su pedido, se filtraría su información sensible/confidencial. d. Extorsión inversa (*reverse extortion*): el atacante podría introducir en la organización información incriminatoria y amenazar con divulgarla o presentar una denuncia en caso de no recibir una remuneración.

La realidad muestra que hay casos en los que partes internas (por ejemplo, el personal del sistema) han realizado acciones con *ransomware* de manera proactiva en la organización en la que trabajan. Debido a esto, se recomienda que la organización se asegure de tener un plan coordinado a la hora de hacer frente a las amenazas internas.[3]

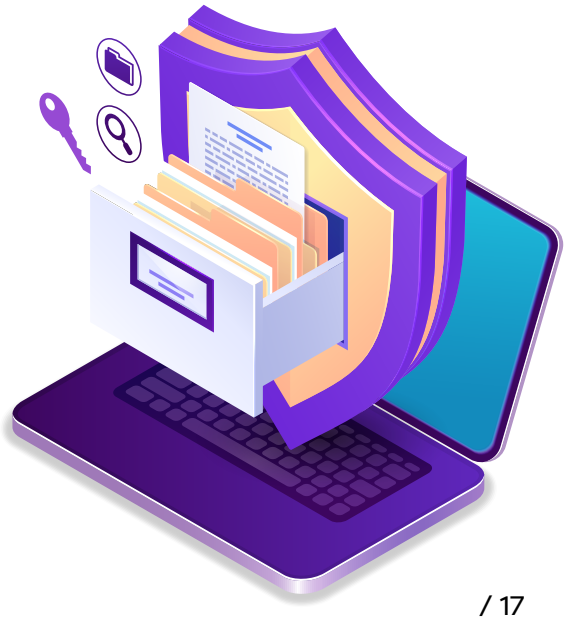


3. Para ampliar este tema, consulte el documento ***Recomendaciones de defensa: La amenaza interna*** disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/recomendaciones-de-defensa-la-amenaza-interna-adaptacion-de-la-organizacion-en-el-ciberespacio**.

/05.
Cursos de acción recomendados ante un incidente de *ransomware* en la organización

En esta sección se describen los cursos de acción recomendados para prepararse y responder ante un incidente de *ransomware* en la organización.

A continuación, el Cuadro 2 presenta un listado exhaustivo de acciones que deben llevarse a cabo para prepararse ante un incidente de *ransomware*.



Cuadro 2. Lista de tareas recomendadas para prepararse ante un incidente de *ransomware*

N.°	Asunto	Descripción	Parte responsable
General			
1	Ciberinteligencia	¿La organización recibe información de inteligencia sobre ataques con *ransomware*? ¿De qué manera utiliza la organización esta información para mejorar su sistema de defensa y su proceso de gestión de riesgos? ¿La organización tiene conocimiento previo de los sitios reconocidos para obtener información/soporte en caso de ser necesario? Por ejemplo, **The No More Ransom Project**.[4]	Equipo de ciberseguridad
2	Acuerdos de servicio	¿La organización dispone de acuerdos de servicio que puedan brindar ayuda en caso de producirse un ataque con *ransomware*? ¿Se han contemplado medidas pertinentes en el contrato entre las partes? ¿De qué manera se examina el cumplimiento de las medidas establecidas por parte de los proveedores? Al respecto, se debe tener en cuenta la autoridad de la organización en caso de haber un incidente de *ransomware* que se origine en una parte de la cadena de suministro de la organización.	Departamento de sistemas de información
3	Capital humano	¿La organización dispone del personal adecuado para prepararse y hacer frente a un incidente de *ransomware* a cualquier hora del día? En caso negativo, ¿tiene un contrato con un proveedor relevante (por ejemplo, un proveedor especializado en análisis forense digital y respuesta ante incidentes [DFIR, por sus siglas en inglés] o en recuperación de datos)?	Departamento de sistemas de información Equipo de ciberseguridad
Continuidad de las actividades y copias de seguridad			
4	Equipo de gestión de crisis	¿La organización cuenta con un equipo de gestión de crisis? En caso negativo, ¿quién formará parte del equipo? ¿Es necesario contratar a un tercero que pueda brindar ayuda cuando sea preciso? ¿Quién está autorizado a realizar un escalamiento y en qué condiciones?	Junta Directiva de la organización
5	Continuidad de las actividades	¿Existe un plan de continuidad del negocio (BCP, por sus siglas en inglés)? ¿Los ataques de *ransomware* están incluidos en la lista de escenarios a los que hacer frente? ¿La Junta Directiva trata estos escenarios de manera regular? ¿Se abordan escenarios extremos, como el borrado o la pérdida de toda la información de la organización? ¿Se han establecido medidas reconocidas para todos los activos/procesos centrales (por ejemplo, objetivo de tiempo de recuperación, objetivo de punto de recuperación [RTO/RPO, por sus siglas en inglés])? ¿Qué se hace con el resto de los empleados de la compañía en caso de crisis? ¿Se mantiene la rutina de trabajo o es necesario hacer cambios en la jornada laboral?	Junta Directiva de la organización

4. Para conocer más de este proyecto, visite: **https://www.nomoreransom.org/es/index.html**.

N.°	Asunto	Descripción	Parte responsable
Continuidad de las actividades y copias de seguridad (cont.)			
6	Sitio web alternativo (recuperación ante desastres [DR, por sus siglas en inglés])	¿La organización tiene un plan de recuperación ante desastres? ¿Dispone de un sitio web alternativo? En caso negativo, ¿por qué no lo tiene? ¿Cuándo se activará el sitio web alternativo? ¿Cuánto tiempo tomará su activación? ¿El sitio web alternativo garantiza el cumplimiento de las medidas establecidas para la continuidad de las actividades?	Junta Directiva de la organización
7	Copias de seguridad	¿El sistema de copias de seguridad es inmune a los ciberataques? ¿De qué manera se examinan las copias de seguridad? ¿La política de copias de seguridad cumple con los requisitos del BCP? ¿Existe un contrato con un proveedor de servicios que pueda brindar ayuda en caso de producirse una falla/un problema al realizar la recuperación? Para ampliar este tema, véase: ***Integración de principios de ciberseguridad en los procesos de respaldo y recuperación***.[5]	Departamento de sistemas de información

5. El documento ***Integración de principios de ciberseguridad en los procesos de respaldo y recuperación*** será publicado próximamente dentro de esta serie de guías de buenas prácticas en ciberseguridad.

N.°	Asunto	Descripción	Parte responsable
Pruebas de preparación y adecuación			
8	Práctica cibernética	¿La organización ha realizado una práctica durante el último año con el sistema de ciberdefensa que haga referencia a escenarios de ataques con *ransomware*? En caso afirmativo, ¿cuáles han sido los resultados? ¿La práctica incluía un escalamiento en caso de ser necesario? ¿Se han implementado las conclusiones de la práctica? ¿Se ha integrado a terceros, como un proveedor de servicios de seguridad gestionados (MSSP, por sus siglas en inglés) o detección y respuesta gestionadas (MDR, por sus siglas en inglés)? ¿El plan de recuperación ante desastre incluye un capítulo específico sobre la práctica? ¿Hay otros ámbitos en los que se requiera una práctica? Para ampliar este tema, véase la publicación ***Práctica cibernética: Creación y edición de ejercicios de ciberseguridad para organizaciones***.[6]	Equipo de gestión de crisis
9	Reducción de la superficie de ataque	¿La organización ha implementado los controles de la ***Metodología de Ciberdefensa para Organizaciones*** en su versión más reciente? En caso negativo, ¿cuál es la fecha objetivo para ello? ¿Qué recursos deben asignarse a fin de completar una implementación efectiva? ¿Existen barreras que deban abordarse para que este proceso tenga éxito?	Equipo de ciberseguridad

6. El documento está disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/practica-cibernetica-creacion-y-edicion-de-ejercicios-de-ciberseguridad-para-organizaciones-mejores**.

N.°	Asunto	Descripción	Parte responsable
Pruebas de preparación y adecuación (cont.)			
10	Pruebas de resiliencia	¿La organización lleva a cabo pruebas de resiliencia de manera periódica, cubriendo escenarios de ataques con *ransomware*?	Equipo de ciberseguridad
11	Análisis de puntos débiles o vulnerabilidades	¿La organización realiza un análisis de puntos débiles o vulnerabilidades, que aborde los indicadores de exposición (IOE, por sus siglas en inglés) que los *softwares ransomware* suelen aprovechar?	Equipo de ciberseguridad
12	Procedimiento de respuesta a incidentes cibernéticos	¿La organización dispone de un procedimiento de respuesta ante incidentes cibernéticos? En caso afirmativo, ¿el procedimiento está actualizado? ¿Quién es responsable de actualizarlo? ¿El procedimiento se ha elaborado de acuerdo con los métodos más recientes en ese campo? ¿Existe una copia impresa de dicho procedimiento que pueda utilizarse en caso de que la infraestructura de tecnologías de la información y la comunicación (TIC) no estuviese disponible?	Equipo de ciberseguridad
13	Monitoreo permanente y continuo (*continuous monitoring*)	¿La organización dispone de procesos de monitoreo permanente y continuo? En caso negativo, ¿la organización tiene un acuerdo de servicio adecuado con un MSSP/MDR? ¿Existen medidas adecuadas para examinar la efectividad?	Equipo de ciberseguridad

Por norma general, el equipo de gestión de crisis deberá incluir, al menos, a los siguientes representantes: el Director General o Director General Adjunto, un miembro de la Junta Directiva que represente al departamento comercial que trate con los clientes, un asesor jurídico, un CIO, un CISO y un portavoz. Asimismo, deberá considerarse el nombramiento de un sustituto en caso de que algunos de los representantes de la lista anterior no estuviese disponible.

El Cuadro 3 presenta un listado de acciones a llevar a cabo para responder a un incidente de *ransomware*.

Cuadro 3. Lista de tareas recomendadas para hacer frente a un incidente de *ransomware*

N.°	Asunto	Descripción	Parte responsable
Identificación: realización de un estudio inicial sobre la posibilidad de sufrir incidentes cibernéticos, adoptando medidas inmediatas para hacer frente a tal incidente			
1	Monitoreo cibernético	¿Quién es la parte responsable de detectar e identificar el *ransomware*? ¿Cuál es la parte responsable de asegurarse de que no se trate de una falsa alarma o una falla operacional? ¿Qué fiabilidad tiene la fuente de los informes (el sistema o dispositivo de informes)? ¿Existe un procedimiento de gestión de incidentes cibernéticos? En caso afirmativo, ¿qué pasos comprende? ¿Quién es responsable de realizar cada paso? ¿Cuál es la parte responsable de documentar las actividades realizadas en el contexto del incidente (gestión del registro de incidentes)? ¿Se han identificado indicadores de compromiso (IOC, por sus siglas en inglés) conocidos o existe un comportamiento anormal/una anomalía que deba ser examinada? ¿Se han realizado acciones para mejorar la calidad del monitoreo?	Equipo de ciberseguridad
Análisis: realización de un estudio exhaustivo y en profundidad del incidente a fin de adoptar los cursos de acción necesarios, examinando posibles alternativas para la contención y gestión del incidente			
2	Gobernanza empresarial	¿Existe un proceso para realizar una adquisición rápida en caso de ser necesario?	Departamento de sistemas de información Adquisición
3		¿Existe un BCP? ¿Quién es responsable de su aplicación e implementación? ¿Qué medidas se han establecido para cada proceso/activo cibernético (RPO/RTO, etc.)? ¿Cuál es la parte que informa al equipo de gestión de crisis? ¿Qué ocurre si esta parte no estuviese disponible?	Junta Directiva de la organización
4		¿Existe un procedimiento de gestión de crisis? En caso afirmativo, ¿qué pasos comprende?	Equipo de gestión de crisis
5	Control de daños inicial	¿Las copias de seguridad se encuentran en buen estado? ¿Cómo puede saberse que lo están?	Departamento de sistemas de información
6		¿Qué activos cibernéticos se han visto afectados? ¿Se han visto/se verán afectados terceros? ¿Se trata de una cortina de humo (*smoke screen*) para ocultar otro ataque? ¿Se han aprovechado los IOE conocidos (según la ciberinteligencia, etc.)? ¿Se han identificado nuevos IOE? ¿Es posible rastrear los medios de pago?	Equipo de ciberseguridad

N.°	Asunto	Descripción	Parte responsable
Análisis: realización de un estudio exhaustivo y en profundidad del incidente a fin de adoptar los cursos de acción necesarios, examinando posibles alternativas para la contención y gestión del incidente (cont.)			
6	Control de daños inicial (cont.)	¿Cuál es el alcance y la calidad de la información que se ha visto afectada (datos del titular de la tarjeta, información no clasificada controlada, información sanitaria protegida, información personal identificable, etc.)? ¿El atacante ha sacado la información de las instalaciones/los límites de la organización? ¿El atacante ha exigido un pago? ¿Quién es el responsable de asegurarse de que las pruebas se recojan y se almacenen de acuerdo con el principio de cadena de custodia (*chain of custody*)? ¿De qué manera se asegura de esto? ¿Durante cuánto tiempo deben almacenarse las pruebas/información forense y cuál es el alcance del almacenamiento (todos los activos cibernéticos, solo los servidores, solo los activos cibernéticos que se vean afectados, una imagen completa, solo la configuración, solo los archivos sospechosos, otros)?	Equipo de ciberseguridad
7		¿De qué tipo de *ransomware* se trata? ¿Cuáles son sus capacidades de ataque? ¿De qué manera penetra? ¿Es posible eliminar el *ransomware*? ¿Cuál es el grado de seguridad de que pueda hacerse? ¿La información filtrada se ha publicado en Internet? ¿En las redes sociales? ¿En la *darknet*?	Equipo de gestión de crisis

N.°	Asunto	Descripción	Parte responsable
Análisis: realización de un estudio exhaustivo y en profundidad del incidente a fin de adoptar los cursos de acción necesarios, examinando posibles alternativas para la contención y gestión del incidente (cont.)			
7	Control de daños inicial (cont.)	¿Cuál es el propósito del atacante? ¿Dinero? ¿Daños a la reputación? ¿Otro? ¿Quién es el atacante (si puede identificarse)? ¿Existen publicaciones fuera de la organización acerca del incidente? ¿Cómo se hace frente a la desinformación? ¿Los clientes/proveedores se han puesto en contacto con la organización con quejas? ¿Se han presentado demandas contra la organización y/o sus funcionarios? ¿Se han presentado quejas/reclamos contra la organización y/o sus funcionarios? ¿Qué ocurrirá si no se realiza el pago? ¿De qué forma podría recibirse una indemnización/compensación o un servicio pertinente de la compañía de seguros?	Equipo de gestión de crisis
8		Si el origen del incidente fuese una parte de la cadena de suministro de la organización, ¿quién está autorizado a comunicarse con ella? ¿Qué obligaciones tiene esta parte para con la organización? ¿Es posible enviar personal de DFIR de la organización a dicha parte?	Equipo de gestión de crisis

N.°	Asunto	Descripción	Parte responsable
Análisis: realización de un estudio exhaustivo y en profundidad del incidente a fin de adoptar los cursos de acción necesarios, examinando posibles alternativas para la contención y gestión del incidente (cont.)			
9	Personal	¿Los miembros relevantes del equipo de sistemas están disponibles y tienen acceso a los activos cibernéticos? ¿Es necesario reforzar al equipo de sistemas con terceros (por ejemplo, un experto en copias de seguridad)? En caso afirmativo, ¿cuál es el acuerdo de nivel de servicio (SLA, por sus siglas en inglés)?	Departamento de sistemas de información
10		¿La organización debe reforzar la plantilla existente con terceros profesionales? En caso afirmativo, ¿existe un contrato laboral con dichos profesionales? ¿Cuál es el SLA?	Equipo de gestión de crisis
11		¿La organización cuenta con personal de DFIR? En caso afirmativo, ¿cuál es el acuerdo a nivel de organización (OLA, por sus siglas en inglés)? En caso negativo, ¿existe un contrato laboral con profesionales externos? En caso negativo, ¿a quién se recurrirá? ¿Cuál es el SLA?	Equipo de ciberseguridad
12	Ciberseguro	¿La organización tiene un seguro cibernético vigente? ¿Con qué compañía de seguros? ¿Quién es el agente de seguros de la organización? ¿El seguro existente cubre problemas de naturaleza cibernética? En caso afirmativo, ¿qué servicios cubre? ¿Cuál es el SLA en relación con cada servicio?	Equipo de gestión de crisis

N.°	Asunto	Descripción	Parte responsable
Análisis: realización de un estudio exhaustivo y en profundidad del incidente a fin de adoptar los cursos de acción necesarios, examinando posibles alternativas para la contención y gestión del incidente (cont.)			
12	Ciberseguro (cont.)	¿Las partes externas a las que la organización desee recurrir están reconocidas y autorizadas por la compañía de seguros? ¿Se debe recibir la autorización de la compañía de seguros antes de proceder? ¿Cuál es el alcance de la indemnización/compensación? ¿Vale la pena ponerse en contacto con la compañía de seguros? ¿Quién es la parte en la organización que está autorizada para ponerse en contacto con el agente/la compañía de seguros? ¿El agente/la compañía de seguros está disponible para consultas en este momento? ¿Hay una persona de contacto específica en la compañía de seguros que esté disponible a cualquier hora del día?	Equipo de gestión de crisis
13	Prueba de las copias de seguridad	¿Las copias de seguridad se encuentran en buen estado? ¿Cómo puede saberse que lo están? ¿Cuál es la fecha de la última copia de seguridad? ¿Cuánto tiempo llevará recuperar el activo/la información? ¿Cuánta información/tiempo de trabajo se ha perdido tras la recuperación de la información? ¿Cuál es el orden de la recuperación? ¿En función de qué se determina este orden?	Departamento de sistemas de información

N.°	Asunto	Descripción	Parte responsable
Análisis: realización de un estudio exhaustivo y en profundidad del incidente a fin de adoptar los cursos de acción necesarios, examinando posibles alternativas para la contención y gestión del incidente (cont.)			
13	Prueba de las copias de seguridad (cont.)	¿Qué se hará si se descubre que la copia de seguridad no funciona correctamente o está infectada? ¿Es posible hacer uso de la capacidad integrada en el sistema de almacenamiento/entorno virtual para volver a una "instantánea" (*snapshot*) determinada? ¿Es posible traer un sistema de copia de seguridad adicional a fin de acortar el tiempo de recuperación? ¿El equipo de sistemas cuenta con licencias, imágenes y *software* de una fuente fiable que permitan realizar un reinicio o instalación desde cero cuando sea necesario? ¿Las actividades destinadas a la recuperación destruirán las pruebas necesarias? En ese caso, ¿qué medidas deberían tomarse para proteger dichas pruebas?	Departamento de sistemas de información
14		¿Las copias de seguridad en poder de la organización no contienen *malware*? ¿Cómo se puede estar seguros de que la información recuperada no contenga *malware*?	Equipo de ciberseguridad
15	Sitio web de DR	¿Cuál es el nivel de preparación y adecuación del sitio web de DR?	Departamento de sistemas de información
16		¿Es necesario omitir el sitio web de DR? ¿Cuál es la probabilidad de éxito de una transición según las medidas definidas?	Equipo de gestión de crisis

N.°	Asunto	Descripción	Parte responsable
Contención: control inicial del incidente para contenerlo y detener un agravamiento de su impacto en las actividades de la organización			
17	Reducción del impacto de los daños	¿Es necesario interrumpir la conexión con interfaces externas, como Internet? ¿Qué consecuencias podría tener esto? ¿Quién está autorizado para aprobar esta medida? ¿Es necesario interrumpir la conexión con interfaces internas, como la conexión al sitio web de DR? ¿Qué consecuencias podría tener esto? ¿Quién está autorizado para aprobar esta medida? ¿Es necesario desconectar el sistema de respaldo/almacenamiento de la red? ¿Qué consecuencias podría tener esto? ¿Quién está autorizado para aprobar esta medida? ¿Se han desconectado de la red los activos cibernéticos que se hayan visto afectados? En caso negativo, ¿por qué no? ¿Es necesario realizar acciones adicionales para reducir la superficie de ataque/aumentar los muros? ¿Se trata de un *malware* conocido? ¿Existe la posibilidad de extraer la clave? ¿El uso de la clave permitiría recuperar la información? ¿La organización tiene en su poder documentación (registros, archivos de historial, etc.) y otros artefactos que puedan resultar de ayuda en la investigación? ¿La organización cuenta con las herramientas adecuadas para realizar la investigación? ¿Existe alguna señal sobre el nivel de complejidad (por ejemplo, capacidad de evasión) del *malware*? ¿Cuánto tiempo ha durado el control del atacante?	Equipo de ciberseguridad

N.°	Asunto	Descripción	Parte responsable
Contención: control inicial del incidente para contenerlo y detener un agravamiento de su impacto en las actividades de la organización (cont.)			
18	Obligación de informar	¿Quiénes son las partes interesadas que deban ser informadas: los clientes, los proveedores, los reguladores? ¿Cuál es el canal de información (correo electrónico, teléfono, otro)? ¿Es necesario utilizar el protocolo de luces de semáforo (TLP, por sus siglas en inglés) al transmitir información?[7] ¿Es necesario verificar la llegada del informe/mensaje? ¿Cuál es el intervalo de tiempo para enviar el mensaje? ¿Hay casos en los que es necesario informar acerca de la evolución del incidente después del informe inicial? ¿Cuál es el factor determinante para la presentación de informes continuos y quién es la parte autorizada para enviar un informe? ¿Se ha notificado a la INCD acerca del incidente? En caso negativo, ¿por qué no?	Equipo de gestión de crisis

7. Para más información acerca de este protocolo, véase el documento ***Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí*** disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/principios-de-operacion-del-equipo-de-respuesta-ante-emergencias-ciberneticas-cert-israeli-mejores**.

N.°	Asunto	Descripción	Parte responsable
Contención: control inicial del incidente para contenerlo y detener un agravamiento de su impacto en las actividades de la organización (cont.)			
19	Interfaces de comunicación interna/externa	¿La organización hablará con los medios de comunicación? ¿La organización tiene una plantilla preparada con el mensaje que vaya a publicar? ¿Quién es la parte autorizada para hablar con los medios de comunicación? ¿Los empleados de la organización han sido informados en relación con la sensibilidad de este asunto? ¿Tienen permitido o prohibido hablar sobre este asunto? ¿El grupo responsable de la gestión del incidente ha sido informado adecuadamente con respecto a los mensajes, etc.? ¿Se ha establecido un proceso de transparencia frente a los clientes y proveedores acerca de esta situación? ¿Se les informará sobre qué ha sucedido, cuál es el daño estimado y cuáles son las recomendaciones para proveedores/clientes cuyos datos se encuentren en peligro? ¿Se les notificará sobre qué se les recomienda hacer? ¿Se les informará sobre cómo se está trabajando frente al incidente y qué sucederá a continuación? ¿Se les notificará sobre el teléfono/correo electrónico al que pueden dirigirse? ¿Hay alguna publicación sobre el incidente en los medios de comunicación? ¿Hay alguna publicación sobre el incidente en las redes sociales? ¿Ha habido algún impacto en el valor de las acciones? ¿Ha habido consultas de inversores? ¿Ha habido consultas de otras partes?	Equipo de gestión de crisis

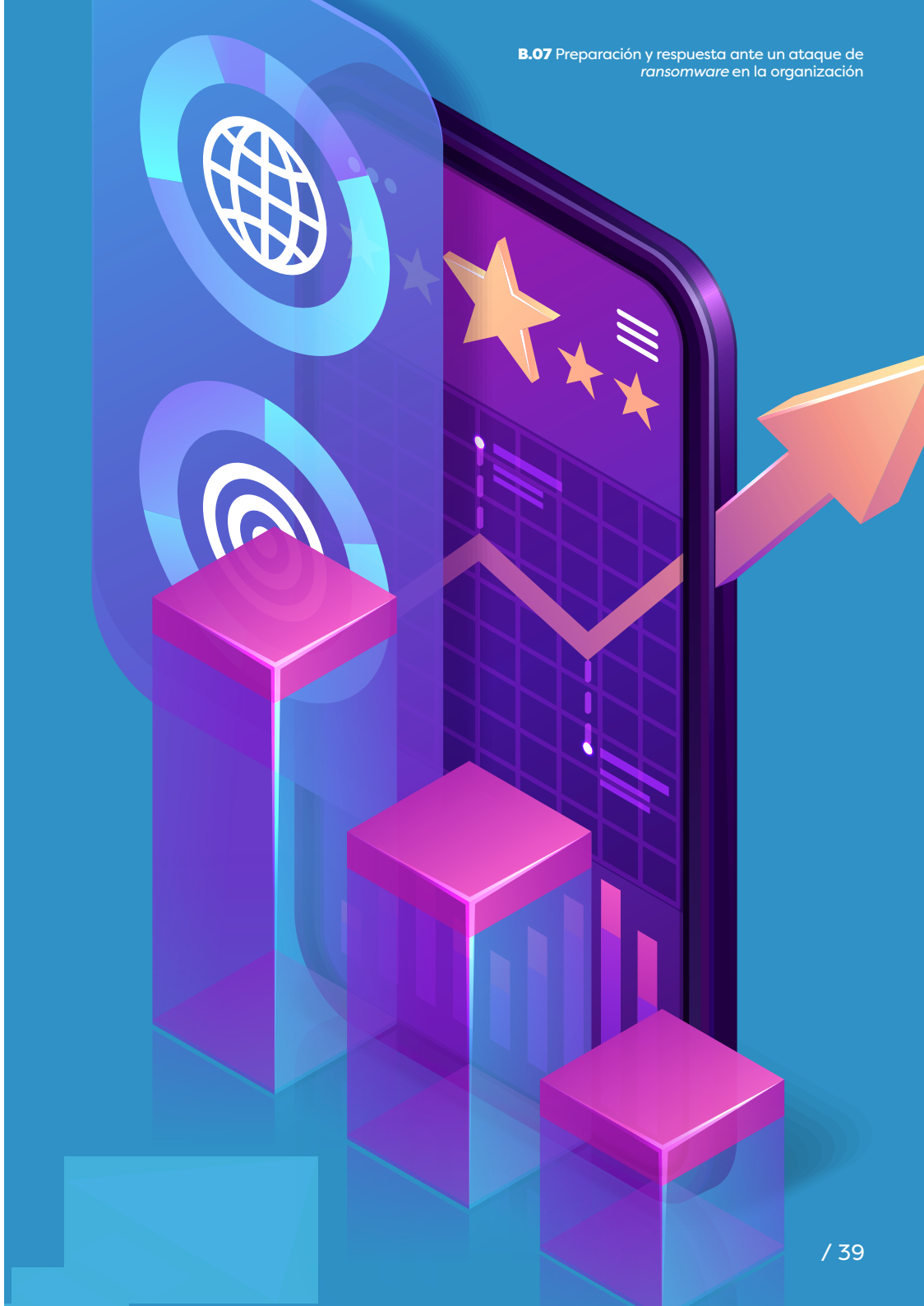
N.°	Asunto	Descripción	Parte responsable
Contención: control inicial del incidente para contenerlo y detener un agravamiento de su impacto en las actividades de la organización (cont.)			
20	Negociaciones	¿Quién llevará a cabo las negociaciones? ¿Cuáles serán los objetivos de la organización en una negociación (por ejemplo, ganar tiempo, etc.)? ¿Quién supervisará que se lleven a cabo las acciones pertinentes? ¿Cuál es el propósito del atacante? ¿Es posible ganar tiempo hasta que se completen las acciones de emergencia? ¿Hay alguna exigencia especial por parte del atacante? ¿El atacante ha divulgado información específica? ¿Qué se hará si no fuese posible recuperar la información? ¿Se han recibido instrucciones concretas de un regulador o de otra entidad?	Equipo de gestión de crisis
Decisión: neutralización de componentes del ataque que se encuentren en los sistemas de la organización, con el objetivo de minimizar los daños ocasionados por el ataque			
21	Eliminación del *malware*	¿Se ha eliminado el *malware*? ¿Todos los activos cibernéticos están limpios? ¿Qué evitará que los activos cibernéticos vuelvan a ser infectados? ¿Hay identificadores que puedan calibrarse (indicadores de ataque [IOA, por sus siglas en inglés], IOC) en el sistema de seguridad? ¿Existen instrucciones organizadas para eliminar el *malware*? ¿Cómo se puede saber si el *malware* ha sido eliminado, si no hay *malware* adicionales y si no afectan a la infraestructura y los sistemas de la organización?	Equipo de ciberseguridad

N.°	Asunto	Descripción	Parte responsable
Decisión: neutralización de componentes del ataque que se encuentren en los sistemas de la organización, con el objetivo de minimizar los daños ocasionados por el ataque (cont.)			
22	Eliminación del *malware* (cont.)	¿Quién es la parte responsable de monitorear/controlar la realización de las acciones requeridas? ¿Qué se hará si no fuese posible recuperar la información? ¿Se han recibido instrucciones concretas de un regulador o de otra entidad?	Equipo de gestión de crisis
23		¿El equipo de sistemas sabe qué debe hacer para eliminar el *malware*? ¿El equipo de sistemas deberá reinstalar los sistemas operativos desde cero? ¿El equipo de sistemas deberá realizar la eliminación del *malware* mediante comandos (*scripts*) u otro método? ¿Será necesario realizar una copia de seguridad de la información cifrada, de modo que pueda recuperarse en el futuro si se obtiene una clave?	Departamento de sistemas de información
24	Eliminación de información filtrada	¿Es posible eliminar la información filtrada a Internet, la *darknet* o las redes sociales? En caso afirmativo, ¿de qué manera?	Equipo de ciberseguridad
25	Control de daños	¿Qué daños se han ocasionado a la organización hasta ahora? ¿Qué efectos tendrá esto a corto y largo plazo? ¿Existe la posibilidad de reducir los daños? ¿Qué sucederá si se descubriese que el incidente no ha terminado e incluso se ha agravado?	Equipo de gestión de crisis

N.°	Asunto	Descripción	Parte responsable
Restauración: retorno de la organización atacada al funcionamiento normal y a la actividad comercial plena			
26	Recupera-ción de la información	¿La velocidad y calidad de la recuperación cumplen con los criterios requeridos? En caso negativo, ¿qué podría hacerse para mejorar la situación? A juicio del equipo de sistemas, ¿se han completado correctamente las acciones de recuperación?	Departamento de sistemas de información
27		¿El entorno en que se restaurará la información está libre de *malware*? ¿Quién será responsable, y de qué manera lo será, de comprobar que el atacante no controle la red de la organización para ocasionar una nueva infección y escalar el incidente? ¿Hay señales (IOA, IOC o de tácticas, técnicas y procedimientos [TTP, por sus siglas en inglés]) de que el incidente se esté repitiendo?	Equipo de ciberseguridad
28		¿Cuáles son las partes empresariales que comprobarán que el proceso de recuperación haya funcionado según lo esperado y que pueda trabajarse con los activos?	Equipo de gestión de crisis
29	Ciberseguro	Desde un punto de vista económico, ¿vale la pena solicitar una indemnización/compensación de la compañía de seguros? ¿De qué manera podría obtenerse una indemnización/compensación de la compañía de seguros por los daños sufridos? ¿Qué se hará si la compañía de seguros rechazase pagar?	Equipo de gestión de crisis

N.°	Asunto	Descripción	Parte responsable
Restauración: retorno de la organización atacada al funcionamiento normal y a la actividad comercial plena (cont.)			
30	Retorno a una rutina bajo supervisión	¿Se están realizado procedimientos reconocidos para volver a una rutina bajo supervisión (un período en el que se lleven a cabo acciones para detectar e identificar a un posible atacante)? ¿Cuánto tiempo llevará esto (se recomienda un mínimo de 75 días)? ¿Qué sucederá si de descubriese que el incidente no ha terminado e incluso se ha agravado?	Equipo de gestión de crisis
31	Gestión de la investi-gación y conclusiones	¿Se está llevando a cabo una investigación por parte de un agente independiente sin influencias internas? ¿Cuáles son las fallas en el sistema de seguridad que han permitido que el ataque tenga éxito? ¿Qué debe mejorarse en el sistema de seguridad? ¿Quién es responsable de mejorar el sistema de seguridad? ¿De qué manera se puede verificar la eficacia de los controles de protección, a fin de evitar que el incidente se repita? ¿Quién es responsable de realizar un ejercicio cibernético para examinar la preparación y la adecuación de la organización, y cuándo se llevará a cabo?	Equipo de ciberseguridad
32		¿Quién gestionará la investigación, y cuándo lo hará? ¿Cuáles son los hallazgos de la investigación? ¿Qué es necesario hacer para evitar que el incidente se repita?	Equipo de gestión de crisis

N.°	Asunto	Descripción	Parte responsable
Restauración: retorno de la organización atacada al funcionamiento normal y a la actividad comercial plena (cont.)			
32	Gestión de la investigación y conclusiones (cont.)	¿Quién es responsable de implementar las recomendaciones de la investigación? ¿De qué manera verificará la organización que las recomendaciones de la investigación se hayan implementado de manera efectiva? ¿Quién será la parte responsable de asignar recursos al programa de actualización/mejora de la infraestructura informática? ¿Es necesario enviar los resultados de la investigación a un regulador o a otra entidad? ¿Es necesario publicar los hallazgos en informes públicos (por ejemplo, informes para los accionistas)? En caso afirmativo, ¿qué información se requiere y de qué manera puede evitarse divulgar información sensible/confidencial innecesariamente?	Equipo de gestión de crisis
33	Restauración de la reputación	¿Qué acciones deberán llevarse a cabo para restaurar la reputación de la organización (devolver la confianza a los clientes e inversores)? ¿Quién será responsable de hacer esto? ¿Qué recursos serán necesarios para ello? ¿De qué manera es posible asegurarse de que estas acciones de restauración hayan tenido éxito?	Equipo de gestión de crisis
34	Retorno a la rutina normal	¿En qué momento se anunciará el retorno a la rutina normal? ¿Se impondrán sanciones reglamentarias contra la organización o contra sus funcionarios? ¿Quién se encargará de ello? ¿Se presentarán denuncias contra la organización o contra sus funcionarios? ¿Quién se encargará de ello?	Equipo de gestión de crisis



Anexos

Anexo 1. Proceso de trabajo para la redacción de esta publicación

Este anexo brinda información al lector sobre la elaboración de la publicación, las partes que han intervenido en el proceso de redacción y el envío de reacciones y comentarios sobre el contenido, para lograr una mayor transparencia y una adecuada divulgación del proceso y las diferentes partes involucradas.

Cómo se ha elaborado el documento: estudio de mercado, temario, comparación a nivel mundial

01

Estudio de documentación y estandarización a nivel mundial, como el Instituto Nacional de Estandarización y Tecnología (NIST, por sus siglas en inglés), la Organización Internacional de Normalización (ISO, por sus siglas en inglés), etc. (los principales ejemplos se muestran en el anexo 2: **Documentos aplicables**).

02

Estudio de publicaciones aceptadas en este ámbito (los principales ejemplos se muestran en el anexo 2: **Documentos aplicables**).

03

Recepción de reacciones y comentarios del público sobre los borradores del documento publicados:

- Sr. Mario Lichtman
- Abg. Vered Zlaikha

Anexo 2. Documentos aplicables

Este anexo contiene las fuentes de información utilizadas a la hora de elaborar esta publicación.

Fuentes de información en español

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

- Cuestionario para proveedores para reforzar la cadena de suministro. Disponible en: **http://www.iadb.org/document.cfm?id=EZSHARE-37811622-6**.
- Integración de principios de ciberseguridad en los procesos de respaldo y recuperación (de próxima publicación).
- Metodología de ciberdefensa para organizaciones 2.0. Disponible en: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-20-mejores-practicas-en-ciberseguridad**.
- Práctica cibernética: creación y edición de ejercicios de ciberseguridad para organizaciones. Disponible en: **https://publications.iadb.org/es/practica-cibernetica-creacion-y-edicion-de-ejercicios-de-ciberseguridad-para-organizaciones-mejores**.
- Recomendaciones de defensa: la amenaza interna. Disponible en: **https://publications.iadb.org/es/recomendaciones-de-defensa-la-amenaza-interna-adaptacion-de-la-organizacion-en-el-ciberespacio**.

General

- The No More Ransom Project. Disponible en: **https://www.nomoreransom.org/es/index.html**.

Fuentes de información en inglés

Dirección Nacional de Ciberseguridad de Israel

- Concepto nacional de ciberseguridad para la preparación y gestión de crisis. Disponible en: **https://www.gov.il/BlobFolder/news/cybercrisispreparedness/he/Management%20of%20crisis%20situations%20english%20final.pdf**.

General

- RTF Report: Combatting Ransomware. Disponible en: **https://securityandtechnology.org/ransomwaretaskforce/report/**.

- Technical Guideline on Incident Reporting under the EECC. Disponible en: **https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc**.

Instituto Nacional de Estándares y Tecnología

- Draft NIST SP 800-137A: Assessing Information Security Continuous Monitoring (ISCM) Programs. Disponible en: **https://www.nist.gov/news-events/news/2020/01/assessing-information-security-continuous-monitoring-iscm-programs-nist**.

- NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Disponible en: **https://csrc.nist.gov/pubs/sp/800/137/final**.

Normativas

- PCI Security Standards

Regulaciones

- Reporting of Technological Failures and Cyber Incidents, Proper Conduct of Banking Business 366, Banco de Israel. Disponible en: **https://boi.org.il/media/p2ndlmdf/366_en.pdf**.

Fuentes de información en hebreo

Dirección Nacional de Ciberseguridad de Israel

- Fortalecimiento de la identificación de usuarios en los sistemas e infraestructuras de la organización mediante el uso de autenticación multifactor (MFA). Disponible en: **https://www.gov.il/he/pages/mfa**.

Legislación

- Ley de Archivos, 5715-1955
- Ley de Firmas Electrónicas, 5761-2001
- Ley de Prohibición del Blanqueo de Dinero, 5760-2000
- Ley de Protección de la Privacidad, 5741-1981
- Reglamento de Protección de la Privacidad (Seguridad de la Información), 5777-2017
- Reglamento General de Protección de Datos (RGPD)

Regulaciones

- Formulario de notificación de incidentes de seguridad graves, Autoridad de Protección de la Privacidad. Disponible en: **https://www.gov.il/he/pages/reporting_security_breach**.

- Guía Cibernética: Cumplimiento de las condiciones para la licencia de tóxicos en el campo cibernético en la industria, Ministerio de Protección del Medio Ambiente. Disponible en: **https://www.gov.il/he/pages/cyber_industry_toxins_permit**.

- Posición Jurídica No. 33-105: Divulgación en asuntos cibernéticos, Autoridad de Valores de Israel. Disponible en: **https://www.new.isa.gov.il/images/Fittings/isa/asset_library_pic///SLB_105-33_cyber.pdf**.

- Puesta al día de las obligaciones de divulgación en caso de incidente cibernético según la posición jurídica No. 33-105: Divulgación en asuntos cibernéticos, Autoridad de Valores de Israel. Disponible en: **https://web.archive.org/web/20211229054747/https://www.isa.gov.il/%D7%92%D7%95%D7%A4%D7%99%D7%9D %D7%9E%D7%A4%D7%95%D7%A7%D7%97%D7%99%D7%9D/Corporations/Hodaot_segaL/General/Documents/HODAA211220.pdf#search=%D7%93%D7%99%D7%95%D7%95%D7%97%20%D7%90%D7%99%D7%A8%D7%95%D7%A2**.

El *ransomware*, o secuestro de datos, es un *software* malicioso (*malware*) que tiene como objetivo impedir que el usuario atacado pueda acceder a un activo cibernético y a la información almacenada en este. Un ataque con *ransomware* podría ser un incidente cibernético con una gran importancia para las organizaciones activas en el sector económico. En caso de que la organización no cumpla con las exigencias del atacante y no tenga una manera efectiva de recuperar la información, podría sufrir daños irreversibles, y llegar incluso a la quiebra.

La finalidad de la presente publicación es ayudar al Director de Seguridad de la Información/Gerente de Ciberseguridad (CISO) y a las partes responsables pertinentes a hacer frente a un incidente de *ransomware* en la organización. Otros actores que podrían beneficiarse con este documento son los Gerentes de Sistemas de Información (CIO), los profesionales de metodología de ciberseguridad, los profesionales de implementación de ciberseguridad, los responsables de tecnologías de ciberseguridad (arquitectos de ciberseguridad), así como el personal de comunicación de datos/informática/tecnologías de la información (TI) y sistemas.

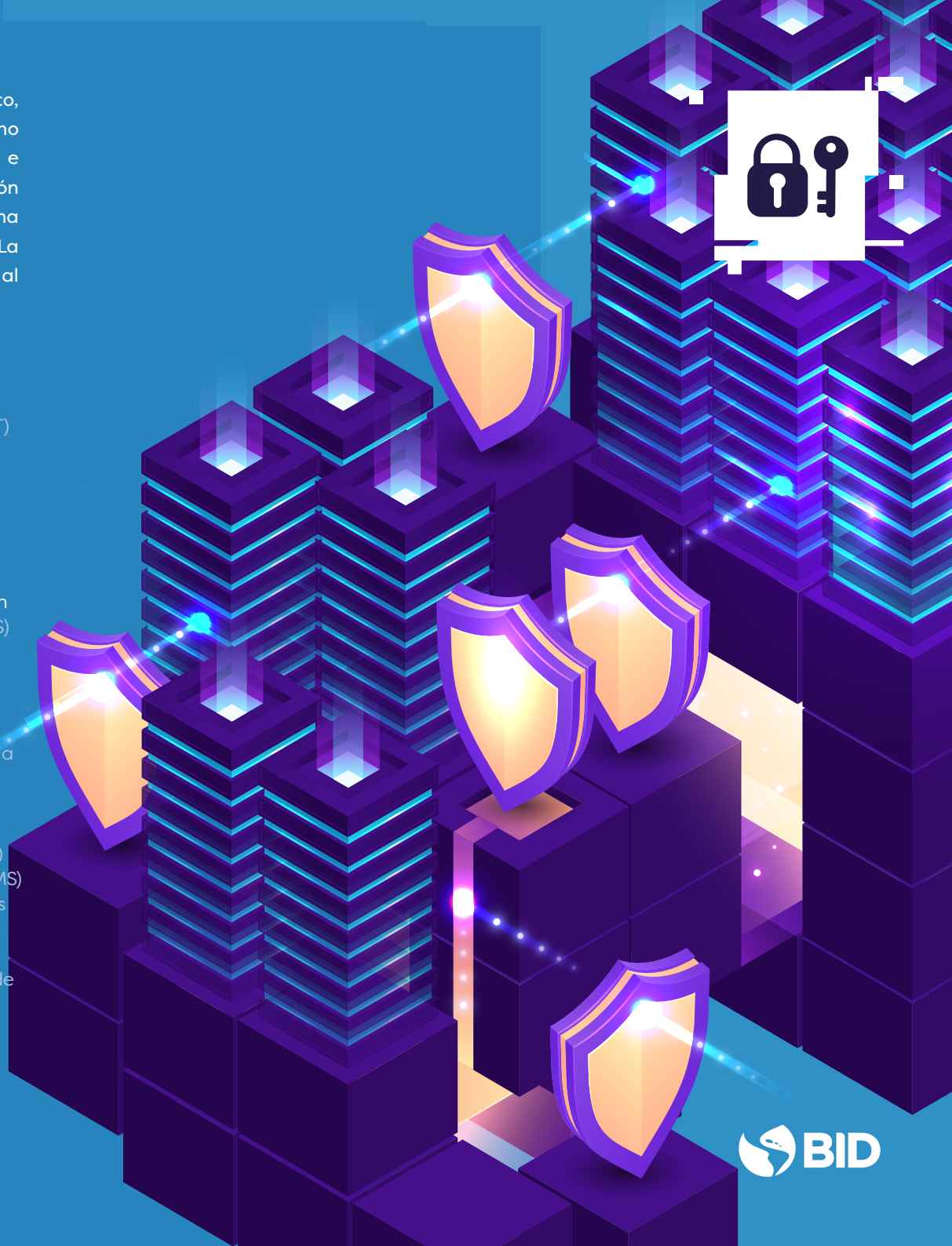
El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que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

Volumen A: Un enfoque metodológico

Volumen B: Un enfoque técnico

- **B.01** Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)
- **B.02** Seguridad de infraestructuras Access Point Name (APN)
- **B.03** Endurecimiento de sistemas informáticos
- **B.04** Reducción de riesgos de ciberseguridad en cámaras de videovigilancia
- **B.05** Reducción de los riesgos de ciberseguridad en los puntos finales de la organización
- **B.06** Seguridad de sistemas de planificación de recursos empresariales (ERP)
- **B.07** Preparación y respuesta ante un ataque de *ransomware* en la organización
- **B.08** Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.09** Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.10** Seguridad de infraestructuras de voz sobre protocolo de internet (VoIP)
- **B.11** Autenticación multifactor avanzada ante amenazas de ciberseguridad
- **B.12** Principales amenazas de ciberseguridad de las plataformas de asistencia remota a usuarios
- **B.13** Prevención y respuesta ante un secuestro de Border Gateway Protocol (BGP Hijacking)
- **B.14** Preparación ante ataques distribuidos de denegación de servicio (DDoS)
- **B.15** Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)
- **B.16** Ciberseguridad por medio de sistemas de gestión de dispositivos móviles (MDM/EMM)
- **B.17** Seguridad en la transferencia gestionada de archivos (MFT)
- **B.18** Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)
- **B.19** Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí
- **B.20** Seguridad de los sistemas multimedia
- **B.21** Integración de principios de ciberseguridad en los procesos de respaldo y recuperación

Volumen C: Desarrollo seguro de *software*



BID