Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí

Mejores Prácticas en Ciberseguridad

B.19

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 *Principios operativos del centro nacional de asistencia para hacer frente a las amenazas cibernéticas*. © (2015) 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/principles**. 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.

/01. Definiciones

01

Incidente cibernético: una violación o amenaza real de violación de una política de defensa cibernética en un sistema computarizado o daños al uso del mismo, según fue diseñado, o a su seguridad, incluyendo lo siguiente:

- Alteración del correcto funcionamiento de una computadora o interrupción de su uso.
- Eliminación de material informático, introducción de modificaciones en este o alteración de su uso de cualquier manera.
- Almacenamiento de información fraudulenta en una computadora o muestra en pantalla de una salida falsa (*false output*), es decir, información o salida que pueda llegar a engañar al usuario, según los objetivos de su uso.
- Infiltración no autorizada en material informático.
- Escuchas no autorizadas de la comunicación entre computadoras.
- Exposición de la información guardada en la computadora a una parte no autorizada.

02

Partes con las que existen colaboraciones: las partes involucradas en el ámbito de la defensa cibernética con las que el equipo de respuesta ante emergencias cibernéticas (CERT, por sus siglas en inglés) colabora en el marco de su propósito, incluyendo organismos paralelos en otras partes del mundo, la comunidad de seguridad, la Policía de Israel, la Autoridad de Protección de la Privacidad en el Ministerio de Justicia, foros internacionales, así como compañías globales de comunicaciones, informática y defensa cibernética.

03

Defensa cibernética: un conjunto de acciones destinadas a prevenir, neutralizar, investigar y hacer frente a ciberamenazas e incidentes cibernéticos, así como a reducir el impacto y daños que provoquen, antes, durante y después de que ocurran.

04

CERT: un centro de asistencia para hacer frente a ciberamenazas, constituido en el marco de la Dirección Nacional de Ciberseguridad de Israel (INCD, por sus siglas en inglés).

05

INCD: la Dirección Nacional de Ciberseguridad de Israel, de conformidad con la decisión gubernamental 2444 relativa al "Fomento de la Preparación Nacional para la Defensa Cibernética" de fecha 15 de febrero de 2015.

06

Información con valor de seguridad (información accionable): cada uno de los siguientes puntos:

- **Indicadores:** datos sobre acciones de los que pueda inferirse que se ha producido, puede producirse o se está produciendo un incidente cibernético (incluyendo información integral sobre la detección, identificación e investigación de amenazas e incidentes, y haciendo énfasis en información tecnológica en bruto).
- **Vulnerabilidades:** puntos débiles en sistemas computarizados, en sus componentes o en procedimientos relacionados a estos que puedan aprovecharse para crear un incidente cibernético.
- **Amenazas:** una amenaza de que se produzca un incidente cibernético.
- **Artefactos y *software* maliciosos (*malware*):** habilidades y herramientas utilizadas para aprovechar vulnerabilidades.
- **Metodologías y herramientas:** metodologías, habilidades y herramientas destinadas a identificar ciberamenazas y maneras de abordarlas y de contener incidentes cibernéticos.

07

Información no identificada: información, incluyendo aquella protegida, que el individuo o la organización que la describe no puede identificar por medios razonables.

08

Información protegida: cada uno de los siguientes puntos:

- Información a la que se aplica la Ley de Protección de la Privacidad [israelí] de 1981.
- Información sobre la organización que no sea de dominio público.
- Secretos comerciales, de conformidad con la Ley de Agravios Comerciales [israelí].

09

Sistemas del CERT: los sistemas de *hardware* y *software* que se utilizan para realizar las tareas del CERT.

10

Público destinatario (circunscripciones): las partes en la economía a las que el CERT ayuda en el marco de su propósito, incluyendo organizaciones y compañías de todos los sectores, oficinas gubernamentales, proveedores de comunicaciones e Internet, compañías de productos, asesoramiento y servicios de defensa cibernética, profesionales de la defensa cibernética y público general.

/02. Propósito

01

El CERT fue establecido en el marco de la INCD y de su propósito.

02

El propósito del CERT es ofrecer asistencia para hacer frente a las ciberamenazas para toda la economía, incluyendo:

- Mejorar la resiliencia en materia de defensa cibernética.
- Proveer asistencia para lidiar con las ciberamenazas.
- Proporcionar asistencia para lidiar con incidentes cibernéticos.
- Recopilar e intercambiar información valiosa relativa a la seguridad con todas las partes en la economía.
- Ser un punto de interfaz central entre los organismos de seguridad y las partes en la economía en materia de defensa cibernética.

03

El CERT no llevará a cabo acciones que no estén relacionadas con este propósito.

04

El CERT se asegurará de que exista un equilibrio entre las necesidades de defensa cibernética y la protección de los derechos básicos durante la ejecución de su propósito.

05

La lista de los servicios del CERT figura en el anexo 1 y se actualiza periódicamente en el sitio web de la INCD: **https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page** (en inglés).

/03. Responsabilidad y gestión adecuada

01

La responsabilidad general del cumplimiento de los principios de operación del CERT en el marco de las acciones de la INCD recae en el director de la INCD, tal y como se detalla a continuación:

- Nombrar al director del CERT entre los empleados de la INCD.
- Supervisar la redacción de procedimientos detallados para el CERT según estos principios y examinar la necesidad de actualizarlos al menos una vez al año en función de sus actividades.
- Establecer mecanismos de supervisión para el cumplimiento de los principios.

02

Los principios de operación descritos en este documento se implementarán en las actividades del CERT aplicando los métodos y herramientas que se detallan a continuación, según corresponda:

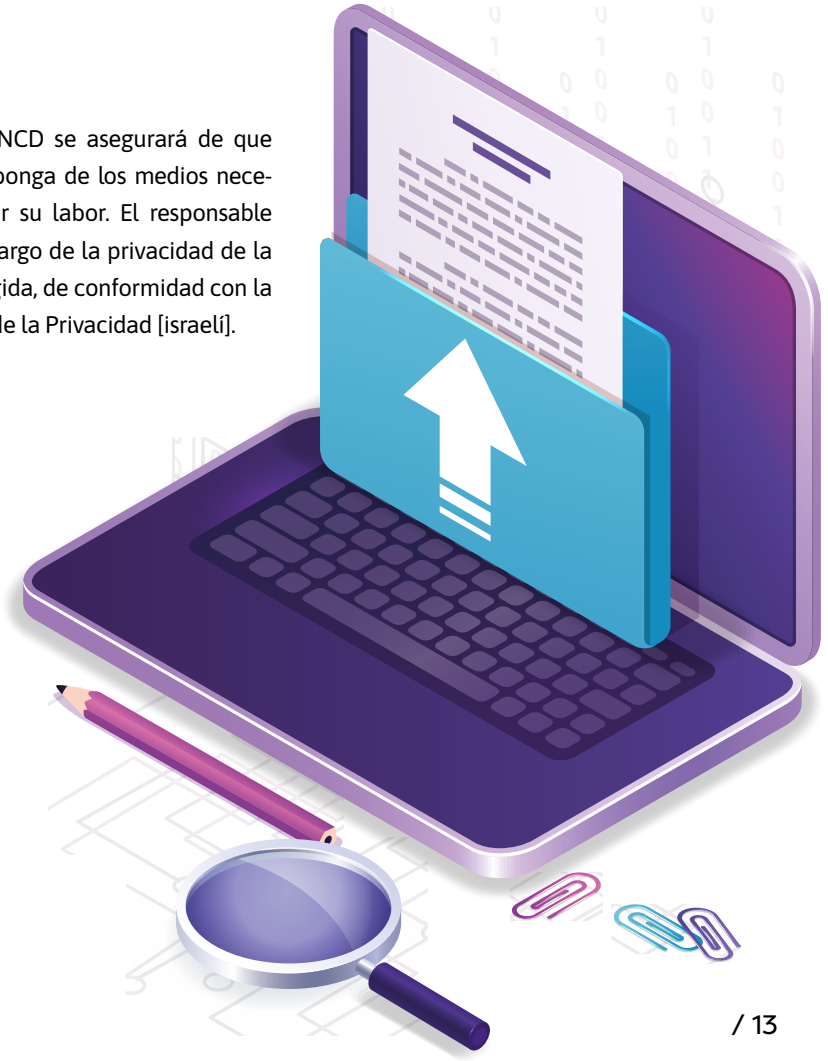
- Diseño tecnológico de los sistemas del CERT.
- Controles tecnológicos en los sistemas del CERT y procesos de trabajo de apoyo.
- Procedimientos de trabajo reguladores.

03

El director de la INCD nombrará a un empleado (en lo sucesivo, "el responsable") entre los trabajadores de la INCD, que tenga la formación adecuada para supervisar el cumplimiento de estos principios con respecto a la información protegida y la realización de controles para su implementación.

04

El director de la INCD se asegurará de que el responsable disponga de los medios necesarios para realizar su labor. El responsable también estará a cargo de la privacidad de la información protegida, de conformidad con la Ley de Protección de la Privacidad [israelí].



/04. Recepción y recopilación de información

El CERT recopilará información con valor de seguridad para su propósito y lo hará de las fuentes que se mencionan a continuación.

01

De una parte del público destinatario, después de que ocurra lo siguiente:

- Que se hayan presentado a la parte principal estos principios.
- Que se haya presentado a la parte una descripción del protocolo de luces de semáforo (TLP, por sus siglas en inglés) para su difusión entre el público destinatario u otro protocolo según el capítulo 7 (segundo punto) para la clasificación de la información, tal y como se detalla en el anexo 2.
- Que la parte haya aceptado facilitar la información de acuerdo con estos principios.
- Si en el marco de la relación contractual pudiese recopilarse información protegida a la que se aplique la Ley de Protección de la Privacidad [israelí] de 1981, que la parte haya notificado a sus empleados y a sus clientes sobre la colaboración con el CERT, incluyendo la transferencia de información con valor de seguridad al CERT, de acuerdo con la redacción distribuida por el CERT.

02

De partes con las que colabore.

03

De partes que estén obligadas a proporcionar información al CERT.

04

De cualquier otra fuente legal.

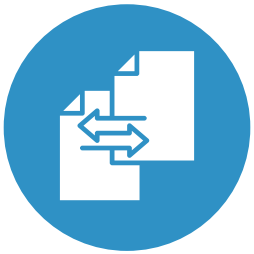
La recopilación de información que contenga información protegida se llevará a cabo con el menor alcance necesario para el propósito del CERT. En caso de que el CERT constate que se ha recopilado información a la que se aplique la Ley de Protección de la Privacidad [israelí] de 1981, no se hará uso de ella y se eliminará, a menos que se cumpla uno de los siguientes puntos:

01

Que el CERT se haya asegurado de que la recopilación y uso de la información se realizan con el consentimiento de la persona a la que se refiera la información, de conformidad con la Ley de Protección de la Privacidad [israelí] de 1981, en función del grado de sensibilidad y la forma de uso de la información.

02

Que el asesor jurídico del CERT haya confirmado que el uso de la información se requiere urgentemente para hacer frente a un incidente cibernético y que, en función de cada caso, dado el grado de sensibilidad de la información y la gravedad del incidente, el uso de esta no constituirá una infracción de las disposiciones de la Ley de Protección de la Privacidad [israelí]. Si se contase con la aprobación del asesor jurídico de acuerdo con este apartado, el CERT informará de ello al fiscal general.



/05.
Almacenamiento de la información en los sistemas del CERT

01

El CERT implementará normas de etiquetado de la información que permitan indicar su grado de sensibilidad, su nivel de intercambio y los permisos relativos a su uso.

02

En la medida de lo posible, la información se guardará de tal manera que sea información no identificada.

03

El CERT tomará medidas para extraer la información con valor de seguridad de la información protegida en el momento de su recepción, de modo que se reduzca la necesidad de almacenar la información protegida en bruto.

04

La información en bruto que tenga una posibilidad razonable de contener información protegida se almacenará por separado y el acceso a ella se limitará a procesos y empleados específicos de la INCD.

05

La información protegida se almacenará durante el período de tiempo mínimo razonablemente necesario para su uso.

/06.
Procesamiento de la información

01

La actividad de procesamiento e investigación de la información en los sistemas del CERT se centrará en localizar y producir información con valor de seguridad, así como en las actividades requeridas para la defensa cibernética.

02

La información no será procesada para fines que no estén en el marco del propósito del CERT y la INCD.

/07.
Difusión de información al público destinatario

01
El CERT solo difundirá información con valor de seguridad al público destinatario.

02
El CERT difundirá información al público destinatario de acuerdo con el TLP u otro protocolo publicado por el CERT. De esta forma, el CERT difundirá al público destinatario información sobre la parte que la facilite de forma no identificada, a menos que la parte en cuestión haya dado su consentimiento.

03
El CERT tomará medidas razonables para comprobar la fiabilidad de la información difundida.

04
El CERT no se hará responsable del modo en que se use la información difundida en los sistemas de la organización receptora.

05
El CERT solo difundirá información con valor de seguridad que incluya información protegida a la que se aplique la Ley de Protección de la Privacidad [israelí] de conformidad con las condiciones estipuladas en el capítulo 4 de este documento.

/08.
Defensa cibernética y seguridad de la información en las actividades del CERT

01
El CERT utilizará tecnología, procedimientos y métodos destinados a proteger los sistemas del CERT y la información incluida en ellos contra cualquier alteración, modificación o acceso no autorizado, prestando atención a los riesgos pertinentes.

02
Estos principios también se aplicarán a los sistemas de respaldo y a la información guardada en estos.

/09.
Personal: privilegios de acceso y compartimentación

01
El director del CERT determinará los privilegios de acceso para los sistemas del CERT sobre la base de la definición del rol o función (*role-based*). Los privilegios de acceso serán solo los necesarios para desempeñar la función.

02
Los privilegios de acceso a la información se otorgarán, en la medida de lo posible, de forma que sea información no identificada, teniendo en cuenta el propósito del CERT.

03
Los sistemas del CERT dispondrán de un mecanismo de documentación automático que permita controlar y auditar el acceso a la información allí contenida.

04
Los privilegios se asignarán a los sistemas del CERT de acuerdo con las instrucciones del director tras consultarlo con el responsable, luego de tomar medidas aceptadas para comprobar su idoneidad para el acceso y uso de los sistemas.

05
El responsable de la información protegida impartirá instrucciones a los empleados acerca de sus obligaciones en relación con estos principios y la legislación aplicable a la información protegida.

/10.
Controles

01
En la medida de lo posible, el CERT dispondrá de mecanismos automáticos en sus sistemas que permitan controlar la observancia de los principios y procedimientos correspondientes.

02
El responsable supervisará los mecanismos de control a fin de detectar incidentes en los que se sospeche un uso indebido.

/11.
Transparencia en las actividades de procesamiento de la información del CERT

01

Estos principios estarán disponibles para su consulta en el sitio web de la INCD.

02

El CERT publicará recomendaciones para las partes con las que colabore sobre cómo notificar a sus empleados y sus clientes acerca de la colaboración con el CERT.

Anexos

Anexo 1. Servicios del CERT

La lista de servicios se actualiza periódicamente en el sitio web de la INCD: **https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page** (en inglés).

Servicios

El objetivo del CERT es ofrecer una serie de servicios en función de las características de la amenaza, del incidente y del público destinatario, sujeto a las reglas de sus actividades. Los tipos de servicios se definen según la metodología desarrollada por los principales organismos mundiales:

01

Servicios reactivos: se ofrecen frente a un incidente, indicación, informe o solicitud individual, e incluyen, entre otros: alertas y advertencias, asistencia para lidiar con incidentes, e investigación tecnológica para identificar y analizar *software* malicioso.

02

Servicios proactivos: brindan asistencia e información para mejorar el nivel de preparación y protección ante futuros eventos, e incluyen, entre otros: formación, capacitación y práctica, y pruebas proactivas para detectar amenazas.

03

Servicios complementarios de gestión de seguridad.

Anexo 2. Protocolo de luces de semáforo (TLP)

El llamado TLP se utiliza para clasificar información sensible que no haya sido catalogada desde el punto de vista de la seguridad. Su objetivo es facilitar el intercambio de información, definiendo limitaciones y condiciones para su difusión. Este método crea una convención entre los socios acerca del uso adecuado de la información para permitir transferir información importante protegida a todas las partes pertinentes, a la vez que se reduce el temor de causar daños a la parte emisora.

Cuadro A2.1. Protocolo de luces de semáforo

Limitaciones de uso compartido de la parte receptora	Clasificación	Propósito de la clasificación
La información clasificada como **"roja"** no debe compartirse con ninguna parte fuera del público destinatario original.		Casos en los que la información tiene un valor de seguridad efectivo para otras partes y puede resultar en daños a la privacidad, la reputación o las actividades de la parte emisora si se utiliza indebidamente.
La información clasificada como **"amarilla"** solo puede compartirse con partes de la misma organización, y únicamente cuando sea necesario para brindar una respuesta eficaz.		Casos en los que el uso efectivo de la información requiere la participación de otras partes, pero una ampliación de la difusión podría resultar en daños a la privacidad, la reputación o las actividades de la parte emisora.
La información clasificada como **"verde"** puede compartirse con todas las partes que puedan beneficiarse de su uso. Sin embargo, no debe compartirse en canales públicos, como sitios web, redes sociales o medios de comunicación de masas.		Casos en los que la información podría beneficiar a muchas partes y compartirla no implica un riesgo para la parte emisora.
La información clasificada como **"blanca"** puede compartirse con todos los públicos destinatarios, incluso a través de canales públicos.		Casos en los que parezca existir un riesgo mínimo o no existir ningún riesgo al difundir la información, sujeto a los derechos de propiedad intelectual.

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, operando 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.

En este contexto, el equipo de respuesta ante emergencias cibernéticas (CERT) israelí fue establecido en el marco de la INCD y de su propósito. Su objetivo es ofrecer asistencia para hacer frente a las ciberamenazas que afectan a toda la economía, incluyendo organizaciones y compañías de todos los sectores, oficinas gubernamentales, proveedores de comunicaciones e Internet, compañías de productos, asesoramiento y servicios de defensa cibernética, profesionales de la defensa cibernética y público general, mediante la recopilación y el intercambio de información valiosa relativa a la seguridad con todas estas partes.

Este documento describe los principios de operación del CERT israelí, su propósito, principios de gestión y políticas para el procesamiento y uso compartido de la información, con el objeto de garantizar la transparencia de las actividades y de asegurar que exista un equilibrio entre las necesidades de defensa cibernética de la nación y la protección de los derechos básicos del público durante la ejecución de su propósito.

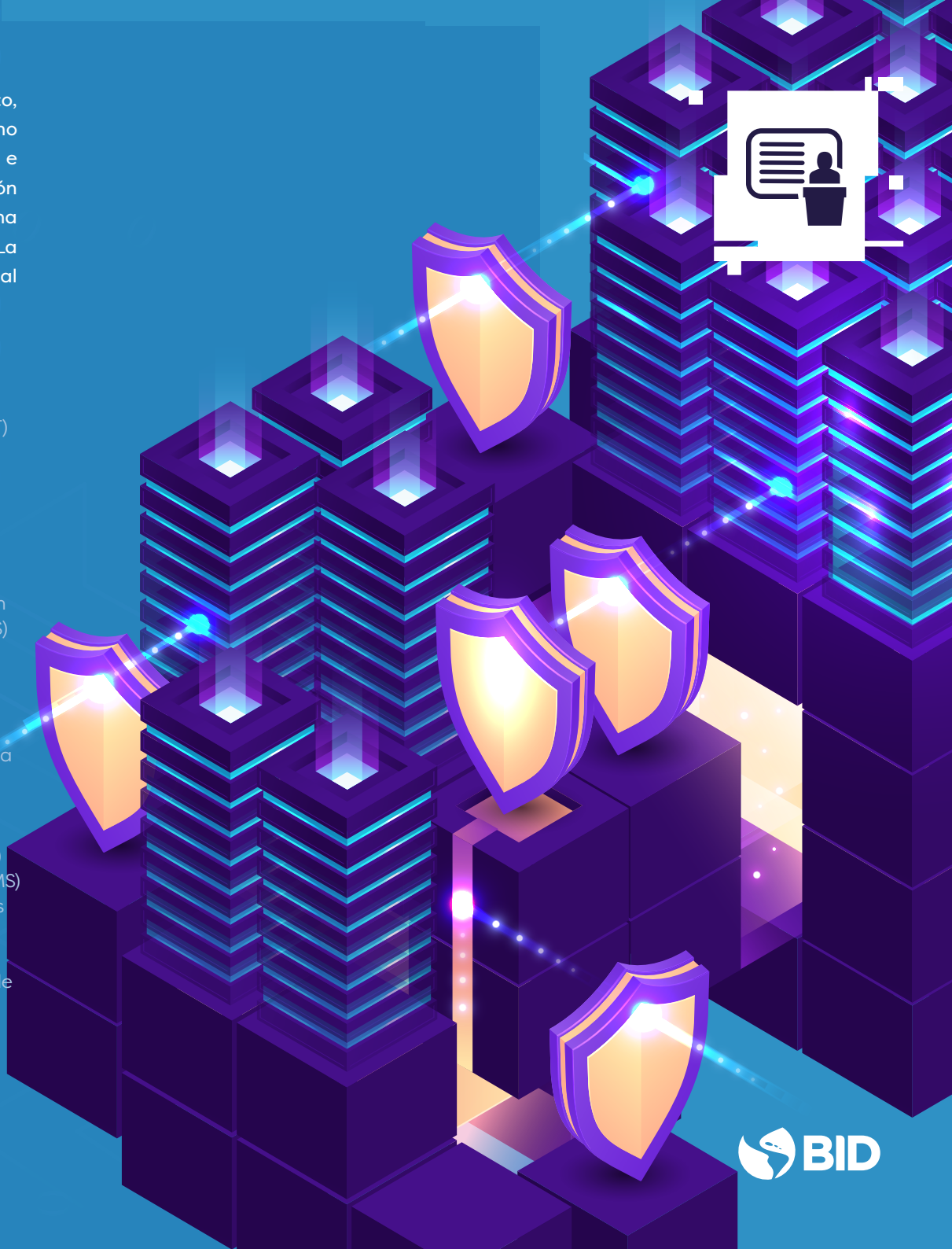
El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que 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