

Preparación organizacional para una crisis cibernética

Caracterización y requisitos de los equipos de gestión de crisis y de respuesta a incidentes

Mejores Prácticas en Ciberseguridad



A.05

Volumen A:
Un enfoque metodológico



Cyber Israel
National Cyber Directorate

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título “Preparación organizacional para una crisis cibernética”. © (2018) Dirección Nacional de Ciberseguridad de Israel.

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

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) en idioma hebreo. Su traducción al idioma español fue realizada por el equipo de ciberseguridad de la división de Innovación para Servir al Ciudadano (IFD/ICS) del Banco Interamericano de Desarrollo (BID), y se incluye como capítulo de la colección “Mejores Prácticas en Ciberseguridad”.

El lector debe tener presente que la ciberseguridad es un campo que evoluciona rápidamente. Aunque estos documentos reflejan principios establecidos, podrían actualizarse periódicamente según sea necesario para reflejar los avances en este campo. Adicionalmente, si bien se ha hecho lo posible para presentar las recomendaciones y recursos de manera que sean universalmente aplicables a las organizaciones de todo el mundo, el lector puede encontrar referencias que son específicas al ecosistema cibernético y contexto de Israel (tales como las sumas indicadas en Nuevos Shekels Israelíes [NIS], o referencias a la normativa israelí o a sus organismos gubernamentales).

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

El documento original se encuentra disponible en el siguiente enlace: <https://www.gov.il/en/Departments/news/cybercrisisforir>. 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

/Pág. 2

01. Introducción

/Pág. 8

02. Público destinatario

/Pág. 10

03. Equipos de gestión de crisis cibernéticas

/Pág. 12

04. Integración de los expertos en respuesta a incidentes en la organización

/Pág. 16

05. Requisitos para un equipo y un servicio de respuesta a incidentes calificado y profesional

/Pág. 19

Prólogo

La transformación digital y el reto de la ciberseguridad

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

conscientes de los riesgos de seguridad que estas conllevan. Las organizaciones también tuvieron que adaptarse rápidamente a los desafíos, estableciendo flujos de trabajo totalmente remotos, a menudo sin contar con todas las medidas de seguridad necesarias ni con la orientación adecuada para los empleados.

Sin duda, los ciberdelincuentes no tardaron en explotar la incertidumbre y vulnerabilidad de los usuarios desprevenidos. Proliferaron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se de-

tectaron casi un millón de intentos de ataque diarios contra las conexiones del protocolo de escritorio remoto (RDP), ampliamente utilizado entre las organizaciones para las conexiones remotas de los empleados. De hecho, los ataques al RDP fueron la forma más popular de ciberataque, superando incluso a los correos electrónicos de *phishing*. Durante la segunda mitad del año, a medida que más organizaciones reforzaban la seguridad de sus plataformas remotas, los *hackers* centraron sus esfuerzos en explotar las vulnerabilidades de los activos privados de los empleados y los dispositivos de acceso remoto para penetrar en sus organizaciones. Aunque estas amenazas se vieron maximizadas por este contexto global, no son novedosas ni desaparecerán; las personas siguen viviendo en un entorno de riesgo elevado, que es especialmente grave en regiones del mundo donde las políticas y tecnología de ciberseguridad están menos desarrolladas, y donde falta educación y concienciación ciudadana en torno a este tema. En otras palabras, aunque los cambios debidos a la pandemia de la COVID-19 acabarán por asentarse, estos han evidenciado la urgente necesidad de reforzar las protecciones individuales y colectivas contra los riesgos cibernéticos.

Reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, promover la confianza de las personas en las tecnologías digitales y apoyar el crecimiento

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

Israel, líder en ciberseguridad a nivel mundial

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

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

La Dirección Nacional de Ciberseguridad de Israel (INCD) es responsable de asegurar el ciberespacio nacional y de establecer y promover la resiliencia cibernética en el país. La INCD opera a nivel nacional para elevar constantemente el nivel de seguridad de las organizaciones y ciudadanos, prevenir y gestionar los ciberataques, y reforzar las capacidades de respuesta en caso de una emergencia cibernética. Su posición como parte de la oficina del Primer Ministro demuestra claramente la centralidad e importancia de sus competencias para el país. Sus objetivos también incluyen la preparación y capacitación del sector privado israelí y del público en general para protegerse de las ciberamenazas mediante la adopción de tecnologías ciberseguras, la publicación de mejores prácticas, la formación del personal y el aumento de la concienciación. Se encarga además

de establecer y reforzar la base científica y tecnológica de ciberseguridad mediante el desarrollo de un capital humano altamente cualificado, el apoyo a la investigación académica de vanguardia, la participación en una avanzada I+D tecnológica y el fomento de la ciberindustria. La INCD dedica sus esfuerzos a mantener un ciberespacio protegido, seguro y abierto para todos los habitantes y empresas del Estado de Israel y a facilitar su crecimiento y su base científica e industrial.

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

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

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

En cuanto a la capacidad de los países para gestionar y responder a los incidentes de ciberseguridad, el mismo estudio relevó que el 63% de los países contaba con equipos de respuesta a incidentes de seguridad, como Equipos de Respuesta a Emergencias Informáticas (CERT) o Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Sin embargo, de los 20 países que sí los tenían, solo tres habían alcanzado una madurez avanzada en su capacidad de coordinar dichas respuestas. De hecho, 23 de los 32 países se encontraban todavía en una fase inicial de madurez en este tema. Este hallazgo llamó la atención sobre la necesidad de que los países refuerzen la capacidad de sus equipos para coordinar eficazmente sus

respuestas a los ciberincidentes. Además, el informe examinó la disponibilidad de oportunidades educativas y de formación en ciberseguridad y descubrió que menos de la mitad de los países de la región ofrecían educación formal en ciberseguridad, como posgrados, maestrías o títulos técnicos. No hace falta decir que contar con suficientes profesionales formados es esencial para diseñar e implementar las políticas y medidas de ciberseguridad necesarias para garantizar la resiliencia de un país frente a ciberataques cada vez más sofisticados y complejos.

¿Qué hace el BID para apoyar a la región?

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

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

El BID y la INCD: uniendo esfuerzos

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

Esta colección ofrece una orientación práctica sobre una serie de cuestiones metodológicas y técnicas relevantes para el fortalecimiento

de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

El reto de proteger el espacio digital seguirá creciendo, junto con la necesidad de contar con experiencia probada para afrontarlo. Las reflexiones aquí contenidas pretenden servir como recurso para potenciar la tan necesaria formación profesional en ciberseguridad que se observa actualmente en ALC. Estas guías contribuirán a elevar los estándares organizacionales, a promover mayor conciencia y cultura de ciberseguridad dentro de las orga-

nizaciones y en el público en general, y a informar a los tomadores de decisiones, gerentes y líderes en sus iniciativas de ciberseguridad. Confiamos en que estas guías servirán de hoja de ruta para los profesionales y líderes de ALC, trabajando juntos para construir un futuro más seguro y próspero.



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

/01.

Introducción

En los últimos años, los incidentes cibernéticos se han convertido en un fenómeno muy común en Israel y en todo el mundo. Esos incidentes afectan a todo tipo de organizaciones, desde las más pequeñas hasta sectores completos e infraestructuras críticas, y pueden afectar a todo el país.

La complejidad de los incidentes y la creciente sofisticación mostrada por los atacantes, que utilizan tecnologías avanzadas, obligan a los defensores a actuar en diversas esferas: derecho, imagen pública, empresas

y, por supuesto, tecnología. Las organizaciones necesitan contar con conocimientos especializados en materia de contenidos, herramientas y tecnologías para hacer frente a tales amenazas. Sin una respuesta experta, profesional y apropiada, las amenazas cibernéticas pueden extenderse, penetrar más en la organización e incluso extenderse a otras organizaciones.

Los incidentes a nivel mundial muestran que el efecto de las crisis cibernéticas en las valoraciones de los activos depende, entre otras cosas, de cómo se gestiona la crisis. Como regla general, las crisis cibernéticas tienen un efecto temporal en las valoraciones de los activos, pero las organizaciones que las gestionan profesionalmente contienen los efectos y limitan el daño a largo plazo.

El equipo de gestión de crisis cibernéticas tiene el objetivo de minimizar el daño que una crisis cibernética causa a la organización. Para eso, opera en diversas esferas: comunicación, derecho, continuidad del negocio, tecnología, etcétera.

Por su parte, el propósito del equipo de respuesta a incidentes² es ayudar a las organizaciones a superar los incidentes cibernéticos a gran escala. Estos equipos están formados por expertos en contenido tecnológico que deben cumplir con los requisitos definidos en materia de procesos y recursos.

Los equipos de respuesta a incidentes pueden ser una parte integral de la organización o parte de un servicio externo, de acuerdo con el análisis de riesgos de la organización y su capacidad para contar

con los recursos y presupuestos necesarios para establecer y administrar el equipo. Sus miembros deben abordar los incidentes cibernéticos con conocimientos profesionales y herramientas para brindar apoyo y asistencia en materia de supervisión, identificación, investigación y respuesta a los eventos a medida que se producen.

Durante una crisis son de suma importancia las facultades del equipo de gestión de crisis y sus contactos cercanos con elementos dentro de la organización (por ejemplo, recursos humanos, operaciones, gestión de riesgos, asesoría jurídica, portavoces, etc.) y fuera de la organización (equipo nacional de respuesta ante emergencias informáticas [CERT, por sus siglas en inglés], reguladores, partes interesadas nacionales, expertos en contenido que brindan asistencia, etcétera).

2. El término *equipo de respuesta a incidentes* se usa de varias maneras en Israel y otros lugares. En esta publicación se refiere solo al equipo tecnológico de analistas de nivel 1, 2 y, a veces, a personas con capacidades de nivel 3, quienes brindan una respuesta para contener el incidente cibernético en la organización. El significado más amplio del *equipo de respuesta a incidentes*, como aquel que gestiona todos los aspectos legales, de medios de comunicación, de negocios y de otros aspectos de una crisis cibernética, se denomina aquí *equipo de gestión de crisis cibernéticas*. Varias empresas proporcionan lo que denominan servicios de respuesta a incidentes, que cubren diversas actividades: desde la gestión de los riesgos cibernéticos, pasando por el manejo de una crisis y los equipos de respuesta a incidentes, hasta la recuperación, la continuidad del negocio y el aumento de la inmunidad de la organización frente a nuevos ataques.

/02. Público destinatario

Organizaciones de la economía

Las organizaciones que desean establecer y operar equipos de gestión de crisis cibernéticas, encontrarán recomendaciones para la ejecución.

Las organizaciones que desean establecer y contratar servicios de equipo de respuesta a incidentes:

01

Obtendrán antecedentes y conocimientos sobre las herramientas de las que pueden disponer en este marco.

02

Comprenderán lo que necesita la organización para prepararse, en términos de procesos e información, para el funcionamiento óptimo del equipo de respuesta a incidentes.

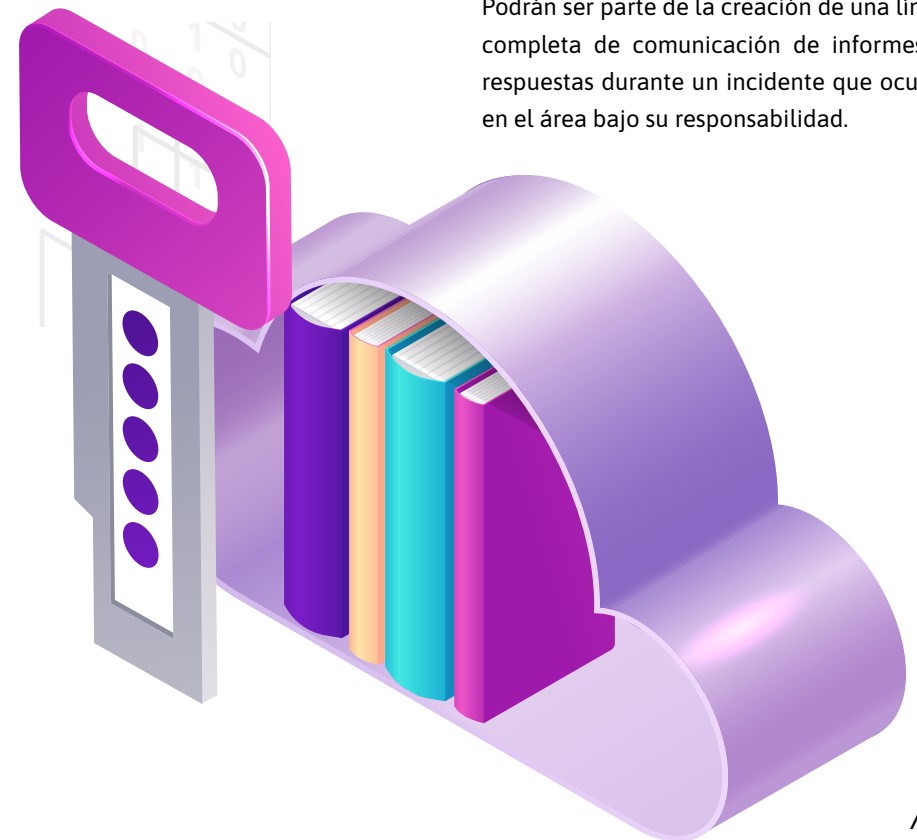
Empresas que prestan servicios de respuesta a incidentes

Encontrarán los requisitos para el cumplimiento de criterios definidos a fin de proporcionar un alto nivel de profesionalismo y capacidades y facilitar el manejo adecuado de las crisis.

Organismos nacionales con responsabilidades cibernéticas (para un sector, por ejemplo)

Comprenderán cómo facilitar la regulación de los servicios de respuesta a incidentes para infraestructuras críticas, para el gobierno y otras entidades supervisadas: requisitos mínimos para los proveedores de servicios.

Podrán ser parte de la creación de una línea completa de comunicación de informes y respuestas durante un incidente que ocurre en el área bajo su responsabilidad.



/03.

Equipos de gestión de crisis cibernéticas

De acuerdo con el documento de orientación nacional para la preparación para las crisis cibernéticas y su gestión, y la *Metodología de Ciberdefensa para Organizaciones*,³ cada organización debe prepararse para eventuales incidentes cibernéticos y definir un proceso estructurado a fin de manejar los incidentes que ocurran dentro de su esfera de responsabilidad.

Este proceso debe abarcar la política de la organización y su plan de acción para manejar incidentes cibernéticos. De acuerdo con

los requisitos de la *Metodología de Ciberdefensa* y con la forma en que se definen los controles, se determinará cómo responderá la organización. El plan de acción debe tener en cuenta las tareas, la cadena de informes y la capacidad de la organización para responder con las herramientas a su disposición, interfaces internas, recursos necesarios, etcétera.

Es aconsejable definir el proceso de notificación de incidentes cibernéticos significativos, tanto dentro como fuera de la organización:

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

01

Dentro de la organización, es importante notificar a alguien de la Dirección (ya sea el Director de Seguridad de la Información [CISO, por sus siglas en inglés], ejecutivos o asesor jurídico) o de relaciones públicas, quien decidirá si debe convocar al equipo de gestión de crisis cibernéticas (véase más adelante).

02

Fuera de la organización, se debe informar según lo exijan las leyes o reglamentos. Es aconsejable informar al CERT para obtener información preliminar y verificar si el incidente en la organización forma parte de uno más amplio.

La organización debe establecer un equipo interno para respaldar la gestión de crisis cibernéticas de antemano. Este equipo, encabezado por el Director de la organización, debe incluir a personas con conocimientos técnicos, jurídicos, de relaciones públicas, administrativos y con otro tipo de conocimientos especializados. Las organizaciones incapaces de gestionar una crisis de forma independiente pueden contratar servicios externos, pero deben mantener un nivel suficiente de control a nivel de la gestión interna.

En vista de la velocidad con la que puede desarrollarse un incidente cibernético y su enorme daño potencial para la organización, es aconsejable definir de antemano un procedimiento y un proceso de toma de decisiones para cuando ocurran los incidentes.

Para facilitar el manejo de incidentes cibernéticos, deben definirse de antemano todas las interfaces y métodos de comunicación que el equipo de gestión de crisis requiere en cada etapa, tanto internamente como con agentes externos (determinando los datos de contacto para vacaciones, celebraciones, etcétera). El gráfico 1 muestra estas interfaces.



Gráfico 1. Interfaces del equipo de gestión de crisis cibernéticas

Para minimizar el daño colateral de un incidente cibernético, es importante estar familiarizado con las partes interesadas externas con las que puede ser necesario contactar durante una crisis (por ejemplo, proveedores de servicios cibernéticos, ministerios y autoridades gubernamentales, agentes de relaciones públicas, miembros de la Dirección Nacional de Ciberseguridad, etcétera). Asegúrese de saber de antemano quiénes son estas partes interesadas y de contactar con ellos en caso de que se produzca un incidente:

01

Familiarícese con los organismos nacionales oficiales en el campo cibernético y sus áreas de responsabilidad, y notifique el incidente a quien corresponda (por ejemplo, al CERT, la policía, etcétera).

02

Para minimizar el daño causado por un incidente cibernético a otras entidades, es importante informarles lo antes posible en caso de que el incidente pudiera tener repercusiones más amplias (por ejemplo, si hay una estructura supraorganizacional o si la organización forma parte de una cadena de suministro conectada a otras entidades).

Es muy importante capacitar al equipo y realizar ejercicios anuales para mantener su grado de preparación.

Es importante definir procedimientos de trabajo para evitar errores (qué se puede eliminar, desconectar y cómo hacerlo). Estos procedimientos son vitales para evitar destruir pruebas legales (según lo define la ley) para varios propósitos:

01

En caso de sospecha de actos criminales, la policía debe realizar investigaciones (forenses) para identificar al atacante.

02

A fin de minimizar el daño a la organización después del incidente, los agentes jurídicos pueden emprender acciones legales contra el atacante o cualquier persona que haya sido negligente.

/04.

Integración de los expertos en respuesta a incidentes en la organización



El equipo de gestión de crisis cibernéticas necesita expertos para investigar un incidente cibernético desde una perspectiva técnica y ayudar a evaluar el daño. De eso se ocupa el equipo de respuesta a incidentes, que puede formar parte de la organización o ser un servicio contratado que realiza un organismo profesional externo.

La organización debe estar familiarizada con la defensa cibernética organizacional y poner en práctica una metodología para garantizar que se apliquen los principios básicos de protección de la organización y que exista una política de protección de la red y la información.

Es particularmente importante para la organización mapear sus procesos centrales y los activos cibernéticos esenciales que respaldan estos procesos y gestionan sus riesgos. Este requisito, que también es la base del documento de orientación nacional para la preparación y gestión de crisis cibernéticas, permite al equipo de respuesta a incidentes actuar de manera rápida, eficiente y efectiva para contener el incidente y evaluar el potencial daño.

Es importante definir las áreas o campos en los que puede actuar el equipo de respuesta a incidentes y determinar las áreas que podrían restringir su efectividad y definirlas como zonas externas.

Deben definirse de antemano los principios para las intervenciones del equipo de respuesta a incidentes y sus relaciones (tanto internas como externas). Se debe establecer una intervención por etapas del equipo de respuesta a incidentes.

Es muy importante designar a uno de los miembros del equipo como experto en contenido de red para la organización, el cual hará que el equipo proporcione los antecedentes tecnológicos necesarios a medida que se desarrolla el incidente. Esta persona de contacto debe tener un archivo operativo actualizado regularmente (en forma impresa), con toda la información y los datos requeridos por el equipo de respuesta a incidentes (como se especifica en la siguiente sección).



Durante las operaciones de rutina, la organización debe crear de antemano junto con el equipo de respuesta a incidentes un archivo operativo para el equipo designado. Ese archivo ha de contener la información más fundamental, que incluye: la arquitectura, la topología de red, los tipos de *hardware*, cortafuegos (*firewall*), enrutadores, sistemas de comunicación y, por supuesto, un mapa de los principales procesos organizacionales y la información de contacto de las personas cruciales durante un incidente.

En la medida de lo posible, las organizaciones deben preparar lógicamente sus respuestas a incidentes para ayudar al equipo de respuesta en su trabajo. Los ejemplos incluyen recopilar y guardar registros de los sistemas operativos y de seguridad de datos, grabar y guardar todo el tráfico de red, definir un puerto de escucha para conectarse al sistema de grabación del tráfico de red, tener la capacidad de distribuir “agentes” a estaciones de trabajo y servidores, etcétera.

Es importante definir procedimientos de trabajo internos para el personal de tecnologías de la información (TI) de la organización en caso de un incidente cibernético, a fin de evitar errores que puedan dificultar que los equipos de respuesta reaccionen de manera óptima (por ejemplo, si se deben desconectar las redes, ya sea para ejecutar herramientas de limpieza, antivirus, etcétera).

Es muy importante mantener el estado de funcionamiento básico del equipo de respuesta a incidentes durante las operaciones de rutina, con actualizaciones periódicas de inteligencia, conocimiento de nuevos ataques y capacidades tecnológicas, ejercicios y simulaciones regulares, y el estudio de situaciones en que casi se produjo un accidente, con el objetivo de extraer lecciones de los incidentes que no llegaron a materializarse.

Las organizaciones deben realizar un ejercicio general al menos una vez al año.

Asegúrese de que los procesos de gestión de la información estén en su lugar y que incluyan las lecciones extraídas de los incidentes.

Cabe destacar que el CERT está disponible para proporcionar asistencia telefónica en todas las etapas del incidente.

/05.

Requisitos para un equipo y un servicio de respuesta a incidentes calificado y profesional

Estas recomendaciones son los requisitos mínimos para un equipo de respuesta a incidentes de alta calidad. Las recomendaciones están clasificadas en las siguientes categorías: personal, herramientas y tecnología, metodología de trabajo y conocimiento de la organización. Todas incluyen reglas generales para el acuerdo de nivel de servicio y la interacción con los portavoces de la organización. Por supuesto, se requiere otro conocimiento especializado en áreas específicas para optimizar las capacidades del equipo de respuesta a incidentes.

Requisitos de personal

Designar un responsable en materia de incidentes para cada equipo a fin de recopilar todos los datos y tener una imagen de la situación para todas las partes interesadas, dentro y fuera de la organización.

Los miembros del equipo deben tener el conocimiento y las habilidades para:

01

Recopilar datos, como el registro del tráfico de red, clonación de unidades, volcado de memoria de acceso aleatorio (RAM, por sus siglas en inglés), recopilación de registros, etcétera.

02

Analizar y filtrar datos que puedan ayudar a decidir si el hecho en cuestión es un incidente cibernético.

03

Realizar cambios para bloquear o eliminar la actividad maliciosa de los sistemas.

Además, otros expertos en contenido deberían estar disponibles para unirse al equi-

po según sea necesario, dependiendo de la complejidad de la situación: expertos en ingeniería inversa y en análisis de código malicioso (*malware*).

Es importante tener en cuenta estos criterios para un proveedor de servicios de respuesta a incidentes:

01

¿Los miembros del equipo están calificados para realizar investigaciones cibernéticas u otras demandas internacionales?

02

¿Puede la empresa cumplir con el criterio del acuerdo de nivel de servicio de que el equipo preliminar se presente *in situ* en cuatro horas?

03

¿Cumple la empresa con la normativa sobre pruebas, según lo prescrito por las autoridades legales?

04

¿La empresa tiene expertos en análisis de código malicioso e ingeniería inversa?

Recomendaciones sobre herramientas y tecnologías

Los expertos del equipo necesitan un conjunto de herramientas tecnológicas para manejar el incidente, que ha de contener lo siguiente:

01

Herramientas técnicas específicas para el incidente:

- Para “detectar” el tráfico de red.
- A fin de clonar discos duros y copiar archivos.
- Para realizar un volcado de memoria.

02

Herramientas para localizar y analizar la actividad maliciosa mediante firmas, identificadores, comportamiento y anomalías, a nivel de tráfico de red y también en los procesos, la memoria y los archivos.

03

Herramientas para el análisis forense de sistemas operativos y la visualización de las acciones realizadas.

04

Herramientas para recuperar y reproducir datos eliminados.



Es importante tener en cuenta estos criterios para los proveedores de servicios de respuesta a incidentes:

- Capacidad de hacer un monitoreo en tiempo real las 24 horas del día durante los siete días de la semana de los sistemas de la organización (ya sea en las instalaciones o de forma remota).
- Compromiso de que las herramientas en uso son “seguras” y no dañarán las infraestructuras de la organización.
- Descripción del producto de detección y respuesta de puntos de conexión y las restricciones de aplicación.
- Descripción del producto de análisis de red y restricciones de aplicación.
- Asistencia para productos en sistemas operativos basados en Windows.
- Asistencia para productos en sistemas operativos basados en Linux.
- Capacidad para investigar entornos basados en Mac.
- Duplicaciones hechas según una norma legalmente aceptable.
- Equipo técnico para análisis en condiciones de campo y laboratorio móvil.
- Laboratorio del área de operaciones para el análisis avanzado de archivos.
- Capacidad para realizar ingeniería inversa en archivos.
- Modelo de informe para mostrar los resultados y resumir la actividad a nivel de gestión.
- Modelo de informe detallado y de alto nivel técnico que incluya todas las actividades realizadas, así como recomendaciones para la acción.



Requisitos metodológicos

Aunque cada ataque cibernético es diferente y los métodos de contención son distintos, el equipo debe tener una metodología de trabajo ordenada para garantizar la calidad y eficacia, a fin de limitar la duración del incidente, minimizar el daño a la organización y reducir al mínimo los problemas pendientes de resolución por parte del equipo de gestión de crisis.

Es importante tener en cuenta estos criterios para los proveedores de servicios de respuesta a incidentes:

01

Poseer experiencia en el manejo de incidentes cibernéticos significativos en organizaciones y pequeñas y medianas empresas (pymes).

02

Resumir los informes de respuesta a incidentes para que tengan una extensión adecuada para la organización.

03

Revisar el informe breve de la empresa a la Gerencia para que tenga una extensión adecuada para la organización.

04

Verificar la metodología de la empresa para el manejo de incidentes durante la respuesta a incidentes.

Requisitos relacionados con la experiencia previa de la organización

Los incidentes cibernéticos avanzan de manera rápida y pueden convertirse en crisis. La experiencia previa con una organización ayuda a un equipo de respuesta a incidentes a limitar la duración de un incidente, contenerlo rápidamente y reducir las posibilidades de que evolucione hacia una crisis o minimizar la gravedad de la misma si llega a producirse.

Es importante tener en cuenta estos criterios para un proveedor de servicios de respuesta a incidentes:

01

¿La empresa tiene experiencia previa con la red de la organización?

02

¿Dispone de una cartera de estaciones de trabajo?

03

¿Mantiene estaciones de trabajo de investigación en el sitio?

04

¿Con qué frecuencia el proveedor celebra reuniones de actualización con el cliente?

05

¿Realiza la empresa una evaluación en las instalaciones para localizar registros relevantes y optimizar productos a fin de prepararse para incidentes?

06

¿El presupuesto incluye un banco inicial de horas para manejar incidentes sospechosos de manera continua?



Acuerdo de nivel de servicio

El proveedor debe definir la manera y los tiempos de manejo de un incidente, desde la consulta inicial de la empresa hasta la llegada al sitio y el inicio del manejo en las instalaciones (por ejemplo, hasta media hora para una respuesta telefónica tras una solicitud).

La organización debe definir un tiempo para llegar al lugar tras una solicitud de la empresa o una decisión de que se requiere un equipo en el lugar (por ejemplo, hasta cuatro horas en un radio de 20 km de la empresa o hasta seis horas para una distancia más larga).

Debido a la naturaleza de las amenazas cibernéticas, es necesario definir la disponibilidad del equipo. En el caso de un incidente de alto riesgo, los equipos deben estar disponibles las 24 horas y los siete días de la semana, tanto en horarios normales como durante emergencias generales (hay que considerar posibles situaciones, como emergencias económicas, circunstancias de guerra, etcétera).

Interfaz entre los equipos de respuesta a incidentes y los portavoces

Cuando se maneja una crisis debido a un incidente cibernético, el tema de las relaciones públicas y la información sobre el incidente y sus implicaciones para las partes interesadas fuera de la organización es extremadamente importante. El equipo de relaciones públicas depende de la información que reciba del equipo de respuesta a incidentes. Esa información debe basarse en datos precisos y describir lo sucedido y de qué manera la organización está abordando el incidente, tanto en lenguaje técnico como corporativo.

Es esencial que los equipos de respuesta a incidentes sigan la política de relaciones públicas de la organización y se familiaricen con sus reglas y restricciones. Es vital preparar un procedimiento para trabajar e informar en los campos de relaciones con los medios y las relaciones públicas, incluida la presentación de informes a los accionistas, directores, autoridades gubernamentales, medios de comunicación, etcétera.

El equipo de respuesta a incidentes debe definir una sola persona de contacto que coordinará toda la información que se transmitirá a los interesados externos y portavoces.

Para ayudar a los portavoces, el equipo de respuesta a incidentes debe presentar un informe preliminar lo más rápido posible tras descubrir el incidente (como regla general, en 12 horas) y proporcionar informes posteriores de forma regular (como regla general, cada 24 horas hasta que se contenga el incidente).

A fin de prepararse para elaborar los informes, el equipo de respuesta a incidentes debe preparar de antemano una lista estructurada de información que se proporcionará periódicamente. Esta puede incluir lo siguiente:

01

¿Cuáles fueron los hallazgos iniciales (cómo ocurrió el ataque, cuál fue el escenario del ataque y penetración, si se conoce la identidad del atacante, qué sistemas se vieron afectados, cuál fue la naturaleza del daño)?

02

¿Qué ocurrió? ¿Cuándo? ¿Fallaron los sistemas de seguridad de datos? ¿Los sistemas de seguridad identificaron el ataque? ¿Cómo reaccionaron?

03

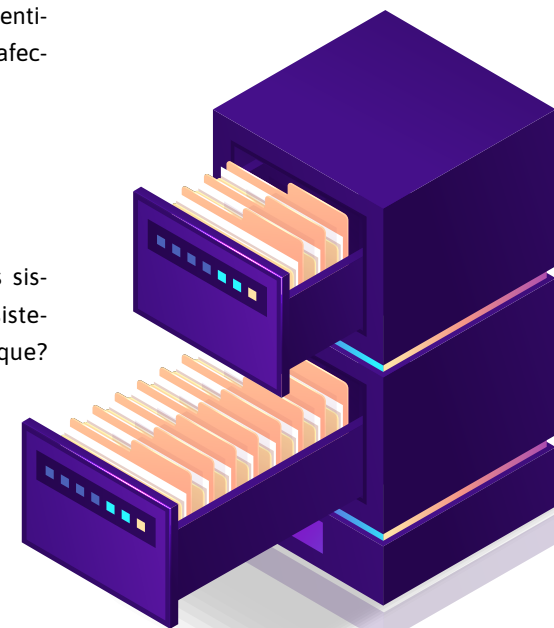
¿Qué medidas se han tomado para contener el incidente y evitar que se propague?

04

¿Cuánto tiempo pasará hasta que los servicios reanuden las operaciones?

05

¿Se ha visto afectada la información de la organización? ¿Qué información?





Esta publicación ofrece recomendaciones importantes a las organizaciones israelíes sobre la constitución de un equipo de gestión de crisis cibernéticas, sus relaciones de trabajo y los requisitos principales para un equipo de respuesta a incidentes cualificado y profesional, un campo que requiere conocimientos previos, capacitación, herramientas, procesos de trabajo específicos y un alto nivel tecnológico.

Además, supone una adición al documento de orientación nacional para la preparación y la gestión de crisis cibernéticas, elaborado por la Dirección Nacional de Ciberseguridad de Israel (INCD). El documento de orientación nacional sirve como base fundamental que define los principios y modos de acción sobre el tema de la preparación y la gestión de crisis en el ciberespacio civil.⁴

4. Puede leerse el documento de orientación en: <https://www.gov.il/en/departments/news/cybercrisispreparedness> (en inglés).

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

Volumen A: Un enfoque metodológico

- A.01** Metodología de Ciberdefensa para Organizaciones Versión 1.0
- A.02** Metodología de Ciberdefensa para Organizaciones Versión 2.0
- A.03** Uso de servicios en la nube: Adenda a la Metodología de Ciberdefensa para Organizaciones
- A.04** Recomendaciones de defensa: La amenaza interna
- **A.05** Preparación organizacional para una crisis cibernética
- A.06** Cadena de suministro
- A.07** Preguntas de orientación para formuladores de políticas cibernéticas
- A.08** Recomendaciones de ciberseguridad y reducción de riesgos cibernéticos para pequeñas empresas
- A.09** Práctica cibernética: creación y edición de ejercicios de ciberseguridad para organizaciones
- A.10** Gestión de riesgos cibernéticos en entornos de tecnologías operativas (OT)
- A.11** Plantilla de evaluación de riesgo en el sector minorista
- A.12** Práctica cibernética: creación de planes de concientización para organizaciones

Volumen B: Un enfoque técnico

Volumen C: Desarrollo seguro de *software*

