

# Cadena de suministro

Cuando todos  
los eslabones  
son fuertes, su  
organización está  
protegida

Mejores Prácticas en Ciberseguridad



## A.06

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 “Regulando la ciberdefensa de la cadena de suministro en la economía israelí”. © (2021) Dirección Nacional de Ciberseguridad de Israel.

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

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

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

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

El documento original se encuentra disponible en el siguiente enlace: <https://www.gov.il/en/Departments/General/expsupplychain>. Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

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

# Índice

## Prólogo

/Pág. 2

## 01. Introducción

/Pág. 8

## 02. Ámbito

/Pág. 16

## 03. Resultados de la iniciativa

/Pág. 20

## 04. Descripción del proceso desde la perspectiva de la organización

/Pág. 23

## 05. Descripción del proceso desde la perspectiva del proveedor

/Pág. 27

## 06. Descripción del proceso de regulación

/Pág. 29

## Anexos

/Pág. 32

# Prólogo

## La transformación digital y el reto de la ciberseguridad

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

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

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

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

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

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

## Israel, líder en ciberseguridad a nivel mundial

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

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

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

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

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

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

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

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

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

## ¿Qué hace el BID para apoyar a la región?

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



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

## El BID y la INCD: uniendo esfuerzos

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

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

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

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

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



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

# /01.

## Introducción

En la economía israelí, organizaciones grandes y pequeñas invierten en seguridad cibernética para minimizar el riesgo de ataques cibernéticos que podrían causarles pérdidas financieras sustanciales y provocar el robo de secretos comerciales, daños a su reputación, la interrupción de la continuidad funcional, etc. Algunas organizaciones son conscientes de que también podrían verse expuestas a una situación de riesgo a través de su cadena de suministro, en caso de que datos suyos almacenados por un proveedor sean robados y el sistema de su organización sea penetrado sirviéndose de las autorizaciones de acceso otorgadas al proveedor, etcétera.

La Dirección Nacional de Ciberseguridad de Israel (anteriormente Autoridad Nacional de Seguridad Cibernética) ha escrito y publicado las directrices nacionales llamadas *Metodología de Ciberdefensa para Organizaciones*, cuyo objetivo es ayudar a las organizaciones a gestionar sus riesgos cibernéticos.<sup>2</sup> En la *Metodología* se define, entre otras cosas, la necesidad de que las organizaciones se defiendan

de los ataques que lleguen a través de su cadena de suministro. Sin embargo, las organizaciones tienen una capacidad muy limitada para controlar las actividades de ciberdefensa de sus proveedores. Muchas carecen de los conocimientos profesionales necesarios para formular sus propios requisitos destinados a sus proveedores y no disponen de los recursos para verificar el grado de cumplimiento

de sus proveedores en materia de requisitos de ciberdefensa. Como resultado, el nivel de ciberdefensa con muchos proveedores es significativamente más bajo que el que la orga-

nización exige de sí misma. Por ese motivo, no ha de extrañar que muchos ataques cibernéticos contra organizaciones se lleven a cabo a través de su cadena de suministro.

### Recuadro 1. Datos acerca de incidentes de seguridad en cadenas de suministro

Un estudio de Bomgar<sup>3</sup> puso de manifiesto que solo el 35% de los expertos en seguridad de datos en organizaciones globales sabía con certeza cuántos proveedores tenían autorización de acceso a los sistemas de su organización.

Ese mismo estudio indicó que, en promedio, los proveedores acceden a la red de una organización 89 veces por semana.

Otro dato del estudio indica que el 69% de los encuestados creía que su organización había sufrido un incidente de seguridad de datos durante el año anterior como consecuencia de autorizaciones de acceso poco estrictas a los sistemas de la organización.

En 2016 las organizaciones que sufrieron un incidente de seguridad de datos que se originó en su cadena de suministro se vieron obligadas a gastar, en promedio, alrededor de US\$10 millones para responder al incidente y gestionarlo (fuente: CSO Online).

Alrededor del 63% de los ciberataques son resultado directo o indirecto de vulnerabilidades explotadas en la cadena de suministro (fuente: Soho Systems).

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

3. Más información disponible en: <https://blackmereconsulting.com/companies-suffering-from-supply-chain-risks/>

La Dirección Nacional de Ciberseguridad se reunió con proveedores, clientes, autoridades reguladoras y consultores a lo largo de 2018 y observó las siguientes deficiencias en la economía:

## 01

No existe una estandarización o lenguaje común entre las organizaciones y sus proveedores. La economía se caracteriza básicamente por organizaciones que no realizan actividades de ciberdefensa en relación con sus cadenas de suministro y organizaciones que han desarrollado sus propios cuestionarios (que en su mayor parte no están adaptados a los diversos tipos de riesgos). Esto crea complicaciones para las organizaciones y la necesidad de invertir recursos para desarrollar y actualizar sus cuestionarios.

## 02

Las organizaciones están teniendo dificultades para administrar el proceso de distribución del cuestionario, responder a las consultas de los proveedores y analizar los resultados. Están obligadas a distribuir el cuestionario a docenas, cientos y, a veces, miles de proveedores (principalmente por correo electrónico). Posteriormente, la organización verifica que cada proveedor haya recibido el cuestionario, que realmente entienda lo que

se espera de él y que sepa cómo responder al cuestionario específico de esa organización en particular. Finalmente, la organización analiza todos los cuestionarios y toma decisiones en función de las respuestas que haya recibido. Para todo esto, se necesita un experto en seguridad de datos y ciberseguridad, que debe dedicar una cantidad considerable de tiempo a estas operaciones.

## 03

Las organizaciones no logran mantenerse al día en relación con el número y alcance de las auditorías de sus proveedores.

## 04

Por su parte, los proveedores se ven obligados a nombrar expertos y asignar una cantidad considerable de recursos a la gestión de los requisitos de ciberdefensa de sus diversos clientes: completar numerosos cuestionarios diferentes, cumplir los distintos requisitos de cada organización, responder a todas las organizaciones que se ponen en contacto con ellos por cuestiones de ciberdefensa, prepararse para que los consultores de las organizaciones lleven a cabo auditorías en sus instalaciones, etcétera.

Esta falta de estandarización constituye una falla del mercado que debe ser corregida. La economía israelí considera que la Dirección Nacional de Ciberseguridad es un organismo gubernamental objetivo y profesional con una perspectiva integral de

la economía, por lo que goza de una buena posición para actuar en nombre del Estado a fin de hacer frente a esta falla del mercado. Además, en virtud de su responsabilidad en relación con la ciberdefensa del gobierno e infraestructura crítica del Estado de Israel, la Dirección tiene el deber de abordar esta falla ayudando a las organizaciones bajo su esfera.



## Recuadro 2. Ejemplos de riesgos potenciales originados en la cadena de suministro

Las organizaciones están expuestas a diversos riesgos potenciales en la gestión de sus cadenas de suministro, ya sea de proveedores o de subcontratistas que proporcionan bienes o servicios a la organización. Por ello, deben ser conscientes de los riesgos y gestionarlos de manera continua. La gestión de riesgos incluye realizar una cartografía de los riesgos, clasificarlos (en términos de criticidad), nombrar a un oficial de gestión de riesgos y definir los controles que deben adoptarse para mitigar el riesgo en la medida de lo posible o, de otra manera, asumir o transferir el riesgo.

Si un proveedor o subproveedor que proporciona un producto o servicio a la organización tiene medidas inadecuadas de seguridad de datos, esto podría poner en peligro a la empresa.

A continuación se presentan algunos ejemplos de riesgos potenciales (fallas) que se originan en las cadenas de suministro que las organizaciones deben gestionar:



Fugas de datos de la organización debido a un almacenamiento inadecuado en una nube (por ejemplo, por una configuración incorrecta).



Pérdida de información debido al extravío por parte de un proveedor de un equipo, como computadoras portátiles o dispositivos USB.



Daño a la reputación como consecuencia del daño a datos de la empresa almacenados en una nube.



Violación de la privacidad de los empleados de la empresa debido a una intrusión en un canal de comunicaciones utilizado por los proveedores para transferir productos a los clientes.



Deterioro de los objetivos comerciales como resultado del robo de patentes o planes comerciales guardados en los servidores de la compañía.



Vulnerabilidad de los datos por una codificación incorrecta por parte de un proveedor de *software*.



Desactivación de los objetivos de la organización debido a una denegación de servicio que paralice los recursos informáticos de un proveedor (por ejemplo, debido a un *software* de secuestro de datos [*ransomware*] en la red de un proveedor).



Filtrado de información comercial como consecuencia de procedimientos de gestión de personal negligentes por parte de un proveedor en relación con el despido de empleados.



Un *software* de código malicioso (*malware*) que infecta la red de la organización como resultado de conexiones no seguras entre la red de la organización y la de un proveedor.



En las reuniones con proveedores, clientes, autoridades reguladoras y consultores celebradas a lo largo de 2018 se concluyó que deben promoverse dos aspectos para ayudar a las organizaciones de la economía a gestionar de manera óptima el proceso:

# 01

Utilizar un lenguaje uniforme: la estandarización de los requisitos solicitados a los proveedores puede ayudar a las organizaciones (tanto proveedores como clientes) a ahorrar tiempo elaborando un documento de requisitos, respaldado por preguntas, etc. La situación actual en la que cada organización elabora su propio cuestionario es una carga tanto para los clientes como para los proveedores. Crear un lenguaje uniforme en la economía reducirá la carga en la etapa de planificación y en las etapas de control y auditoría.



# 02

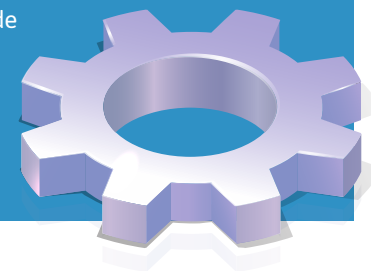
Construir un mecanismo de confianza fiable en el mercado: para ahorrar tiempo y dinero a las organizaciones, ambos lados del acuerdo (proveedor y cliente) deben garantizar que el modo de inspección y el nivel de verificación se realicen de manera profesional. En la situación actual, muchas organizaciones realizan inspecciones o revisiones del mismo proveedor, lo que supone una carga tanto para el proveedor como para el cliente. Para abordar esta situación, es posible fijar un denominador común más amplio que sea compatible con muchas organizaciones de la economía (por ejemplo, en relación con el mantenimiento de registros, cumplimiento con las normas de protección de la privacidad, copias de seguridad, herramientas de defensa para proteger las estaciones terminales y la red, etc.). Aunque los proveedores a veces pasan por el proceso para un cliente en particular, en ocasiones incluso recurriendo a un consultor independiente, a menudo se les exige que respondan al cuestionario completo varias veces para otros clientes. Debido a las dificultades que enfrentan las organizaciones para auditar a múltiples proveedores, con frecuencia los clientes “se las arreglan” enviando un cuestionario y usando un enfoque de “leer y firmar”.

## Recuadro 3. Ejemplo de mecanismo de confianza fiable

La organización A sabía que a un proveedor en particular se le hicieron preguntas sobre sus controles de seguridad cibernética que son importantes para ella, y que el proveedor probó incluso a través de un auditor certificado externo que cumplía tales controles.

Es posible que no se requiera que la organización A realice la auditoría de este mismo proveedor, si se considera que este proporcionó datos profesionales de sus medidas de ciberdefensa que deberían satisfacer a un sector sustancial de la economía. Incluso si la organización A desea inspeccionar problemas adicionales, debe poner el foco de atención exclusivamente en su riesgo residual.

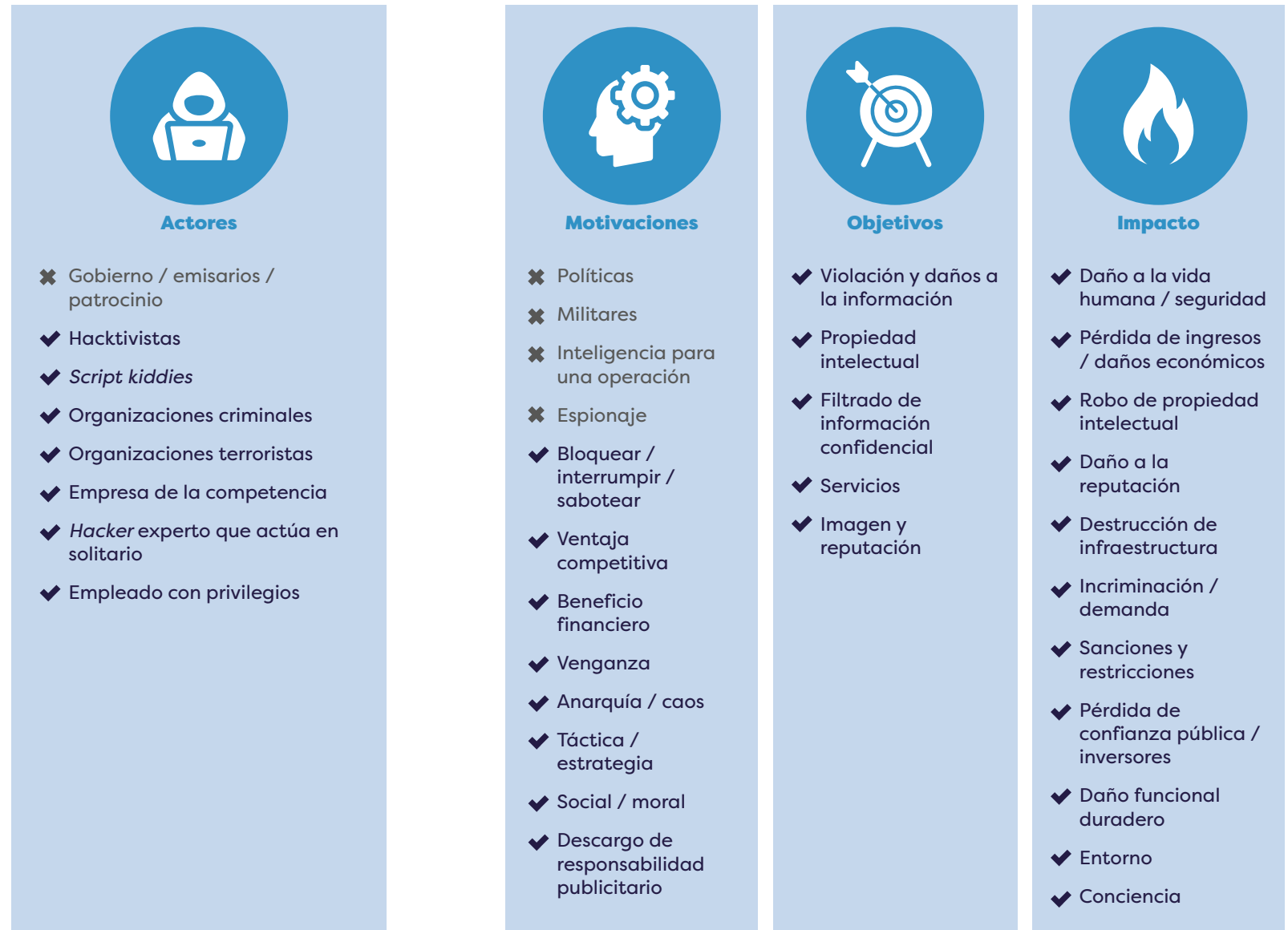
Por esa razón, la Dirección desarrolló la Metodología Nacional para la Protección de la Cadena de Suministro, que regula las actividades de ciberdefensa de la cadena de suministro en la economía israelí. En ella se aborda el nivel de servicios ofrecidos por el Estado y se ofrecen recomendaciones acerca de los procesos de gestión de los riesgos cibernéticos de la cadena de suministro para las organizaciones y de ciberdefensa para los proveedores.



# /02. Ámbito

El propósito de la iniciativa es aumentar las capacidades de ciberdefensa de los proveedores contra diversos tipos de ciberataques. Si bien no pretende prevenir un ataque de un atacante fuerte y determinado, como una amenaza persistente avanzada a nivel estatal, en la situación actual muchos atacantes no necesitan herramientas sofisticadas para piratear la red de una organización a través de una cadena de suministro que carezca de las medidas básicas de ciberseguridad. La iniciativa elevará el nivel de seguridad al mejorar los mecanismos de ciberdefensa de la economía contra atacantes poderosos.

**Gráfico 1.** Ámbito de aplicación de la iniciativa (marcado en azul)



Hay situaciones en las que se requieren actividades adicionales o distintas. Por ejemplo, las que se mencionan a continuación:

## 01

Algunos proveedores no pueden cumplir con los requisitos de ciberdefensa que se esperan de ellos, pese a lo cual las organizaciones desean contratarlos por razones particulares, como una obligación contractual existente, sus conocimientos y experiencia u otras razones. En estos casos, se debe llevar adelante un proceso de gestión de riesgos con respecto a ese proveedor específico y tomar decisiones de mitigación de riesgos, como implementar controles compensatorios, desarrollar un proceso de trabajo diferente con el proveedor, etcétera.

## 02

Hay proveedores sobre los cuales el cliente medio no tiene influencia en relación con su nivel de ciberdefensa. A veces esto se deriva de las “relaciones de poder” entre proveedor y cliente; en otras ocasiones, la fuente del problema es un proveedor extranjero dado que el cliente no puede realizar auditorías o exigir que cumpla con requisitos específicos en materia de ciberdefensa, etc. En estos casos, los clientes pueden intentar presionar

al proveedor a través de otros canales, por ejemplo, mediante una notificación a las autoridades reguladoras o un grupo organizado por varios clientes para ejercer presión sobre ese proveedor. Si no hay una forma efectiva de verificar el nivel de ciberdefensa de un proveedor, a veces también es posible confiar en la certificación internacional existente (como el control de organizaciones proveedoras de servicios 2 [SOC2, por sus siglas en inglés]) e incluir disposiciones contractuales que requieran auditorías o el envío de información. Con frecuencia, estos proveedores otorgan a sus clientes acceso a los resultados de encuestas de riesgos realizadas a través de un tercero independiente. La revisión de esas encuestas puede proporcionar a los clientes detalles significativos. En estos casos, es importante determinar el alcance de la auditoría, porque la certificación puede emitirse para un servicio o producto en particular y no para todas las operaciones del proveedor. Además, es fundamental comprender la división de responsabilidades entre el proveedor y el cliente en lo relativo a la ciberdefensa.

Por ejemplo, el hecho de que un proveedor internacional de servicios en la nube cumpla con los requisitos de la norma habitual en este campo (como la de Cloud Security Alliance [CSA2])<sup>4</sup> no certifica automáticamente la división de responsabilidades<sup>5</sup> en materia de gestión de actualizaciones de *software*, gestión de usuarios, soporte lógico inalterable (*firmware*), copias de seguridad, monitoreo, etc. El uso de una matriz RACI (responsable, aprobador, consultado, informado) ayudará a gestionar mejor el riesgo.

4. Para más información, visítese: <https://cloudsecurityalliance.org/>

5. Véase, por ejemplo, el siguiente enlace: <https://www.cloudsecurityalliance.no/2019/02/mapping-of-on-premises-security-controls-vs-major-cloud-providers-version-3-2-feb-2019/>

## 03

Algunos proveedores al ser atacados pueden causar graves daños a las operaciones centrales de una organización. En estos casos, además de realizar una revisión para evaluar el nivel de ciberdefensa de la organización de acuerdo con la Metodología para la Protección de la Cadena de Suministro, también se recomienda llevar a cabo encuestas de evaluación de riesgos individuales. Esas encuestas considerarán la información concreta, los procesos comerciales específicos, la cartografía de las amenazas específicas y de la imputación de amenazas, etcétera.



# /03. Resultados de la iniciativa

## 01

**Mejorar el nivel profesional en las organizaciones:** uso de la *Metodología de Ciberdefensa para Organizaciones* a fin de gestionar los riesgos cibernéticos que se originan en la ca-

dena de suministro. Este documento ayuda a las organizaciones a hacer una cartografía de los proveedores, priorizarlos de acuerdo con el grado de riesgo que representan para la organización, evaluar el riesgo específico que suponen para la organización y definir los requisitos de ciberdefensa de sus proveedores (véase el anexo 1).

## 02

**Cuestionario para proveedores:** conjunto modular de requisitos para proveedores. Estos requisitos se dividen según el grado de riesgo que el proveedor plantea a los procesos operacionales de una organización y sus sistemas (proveedor crítico o no crítico)<sup>6</sup> y según la naturaleza del acuerdo (proveedor de un servicio basado en la nube, proveedor que es desarrollador de software, proveedor que recibe acceso remoto, etc.) (véase el anexo 2).

## 03

**Módulo de la cadena de suministro en el sistema de objetivos y controles de la organización:** la Dirección Nacional de Ciberseguridad ha desarrollado este módulo de gestión de proveedores como servicio gratuito para las organizaciones. El módulo permite a los proveedores rellenar el cuestionario en línea de manera fácil e intuitiva. Una vez que el proveedor responde a todas las preguntas, se genera un informe

detallado que contiene análisis gráficos para ilustrar su situación de ciberdefensa e indica los controles en los que se requieren mejoras y aquellos necesarios para agilizar la construcción de un plan de trabajo (véase el anexo 3).

## 04

**Certificación de inspectores cualificados de la cadena de suministro:** acreditación estatal de expertos que hayan cumplido los criterios de nivel (en particular datos de nivel, un examen de ingreso y la aceptación por un comité de admisiones), que hayan completado una formación especializada en la inspección de las capacidades de ciberdefensa en las cadenas de suministro de la organización de acuerdo con la Metodología para la Protección de la Cadena de Suministro y hayan aprobado con éxito el examen de certificación. El certificado lo emite un organismo de certificación autorizado en nombre de la Dirección Nacional de Ciberseguridad, y los proveedores pasan a constar en la base de datos nacional (véase el anexo 4).

6. Proveedor crítico: es el proveedor que brinda servicios tales como asistencia o mantenimiento de sistemas de información, almacenamiento de información confidencial fuera de las instalaciones de la organización, servicios de externalización tecnológica, etc. (Prácticas bancarias adecuadas 363 - Gestión de riesgos cibernéticos en la cadena de suministro, cláusula 7), o aquel proveedor cuyo daño pueda causar daños importantes a la organización. La decisión de definir a un proveedor como crítico queda a discreción de la organización, con una excepción: cuando una autoridad reguladora haya definido de antemano para las organizaciones de la economía sobre las que es responsable que un proveedor en particular, o cualquier proveedor que cumpla con criterios definidos, constituye un proveedor crítico.

## 05

**Centro de asistencia telefónica “119”:** plataforma que brinda soporte y asistencia sobre temas relacionados con una cadena de suministro, incluidas las respuestas a cuestiones metodológicas y técnicas sobre el módulo de la cadena de suministro y el sitio web de la Dirección.

de proveedores lo realiza un organismo de certificación en nombre de la Dirección e incluye inspecciones por parte de un inspector certificado de la cadena de suministro, la aprobación del organismo de certificación, la emisión del certificado a los proveedores y el registro de proveedores certificados en la base de datos nacional (véase el anexo 4).

## 06

**Certificación de proveedor:** regulación estatal del proceso de certificación de proveedores aprobados. El proceso de certificación

## 07

**Base de datos nacional:** base de datos de escala nacional accesible en el sitio web de la Dirección, que incluye la lista de los inspectores certificados de la cadena de suministro y una función de consulta de la base de datos para encontrar a proveedores certificados (véase el anexo 4).



# /04. Descripción del proceso desde la perspectiva de la organización

La organización debe realizar una cartografía de los riesgos que se originan en su cadena de suministro y llevar a cabo operaciones en dos canales fundamentales para protegerse de los ataques cibernéticos que lleguen a través de la cadena de suministro:

## 01

**Operaciones realizadas por la propia organización:** incluyen medidas como cartografiar y clasificar a los proveedores, obtener firmas de los proveedores en declaraciones y contratos pertinentes, incorporar disposiciones de ciberdefensa en sus contratos, realizar controles y auditorías, adquirir e implementar herramientas de monitoreo, formular e implementar una política de conexión remota, desactivar y reconstruir contenido vinculado con los recursos que

se cargan en la red de la organización, bloquear soportes electrónicos hostiles, gestionar autorizaciones, realizar compartimentación, etcétera.

## 02

**Operaciones que la organización requiere que sus diversos proveedores implementen y/o que estos deben realizar en sus propias instalaciones antes de contratarlos.** Estas operaciones incluyen solicitar que el proveedor desarrolle software en una configuración particular y endurezca sus equipos de comunicación, dispositivos, servidores y estaciones terminales, requerir la protección del servicio que proporciona mediante tecnologías para la prevención de ataques de denegación de servicio (DoS, por sus siglas en inglés), exigir que se realicen copias de seguridad, etcétera.



Para este fin, la organización debe:

# 01

Cartografiar a sus proveedores según los siguientes aspectos:

- Categorías estructurales (derivadas de la naturaleza del riesgo): servicios generales, provisión de acceso remoto, servicios en la nube, desarrollo de software.
- La importancia o no del proveedor de acuerdo con las pérdidas potenciales que podrían ocasionarse en la organización si se produjera un ataque cibernético al proveedor (clasificación estructurada para la economía israelí).
- El nivel de pruebas requerido: declaración, certificación respaldada por datos probatorios o control por parte de un organismo de certificación independiente.

# 02

Remitir a sus proveedores al sitio web de la Dirección con el fin de que completen un cuestionario para proveedores basado en la naturaleza del riesgo, el daño potencial procedente del proveedor y el nivel de prueba requerido.

# 03

Analizar el cuestionario, los documentos de apoyo o la certificación requeridos (según lo indicado anteriormente) y determinar el nivel de riesgo residual del proveedor.

# 04

Incorporar la gestión de riesgos de proveedores en el sistema de gestión de riesgos cibernéticos de la organización.

# 05

Incorporar los controles necesarios en el proceso de contratación: aspectos de compra, política organizativa, contratos con proveedores e información para proveedores.

# 06

Incorporar los controles necesarios durante el plazo del contrato para proteger los datos confidenciales de las operaciones (y particularmente los datos de seguridad de las operaciones) y agregar controles compensatorios.

# 07

Incorporar los controles necesarios al concluir el acuerdo.

**Pueden verse más detalles en el anexo 1.**



**Gráfico 2.** Pasos y consideraciones desde la perspectiva de la organización

Nota: \*INCD: Dirección Nacional de Ciberseguridad de Israel (siglas en inglés).

# /05. Descripción del proceso desde la perspectiva del proveedor

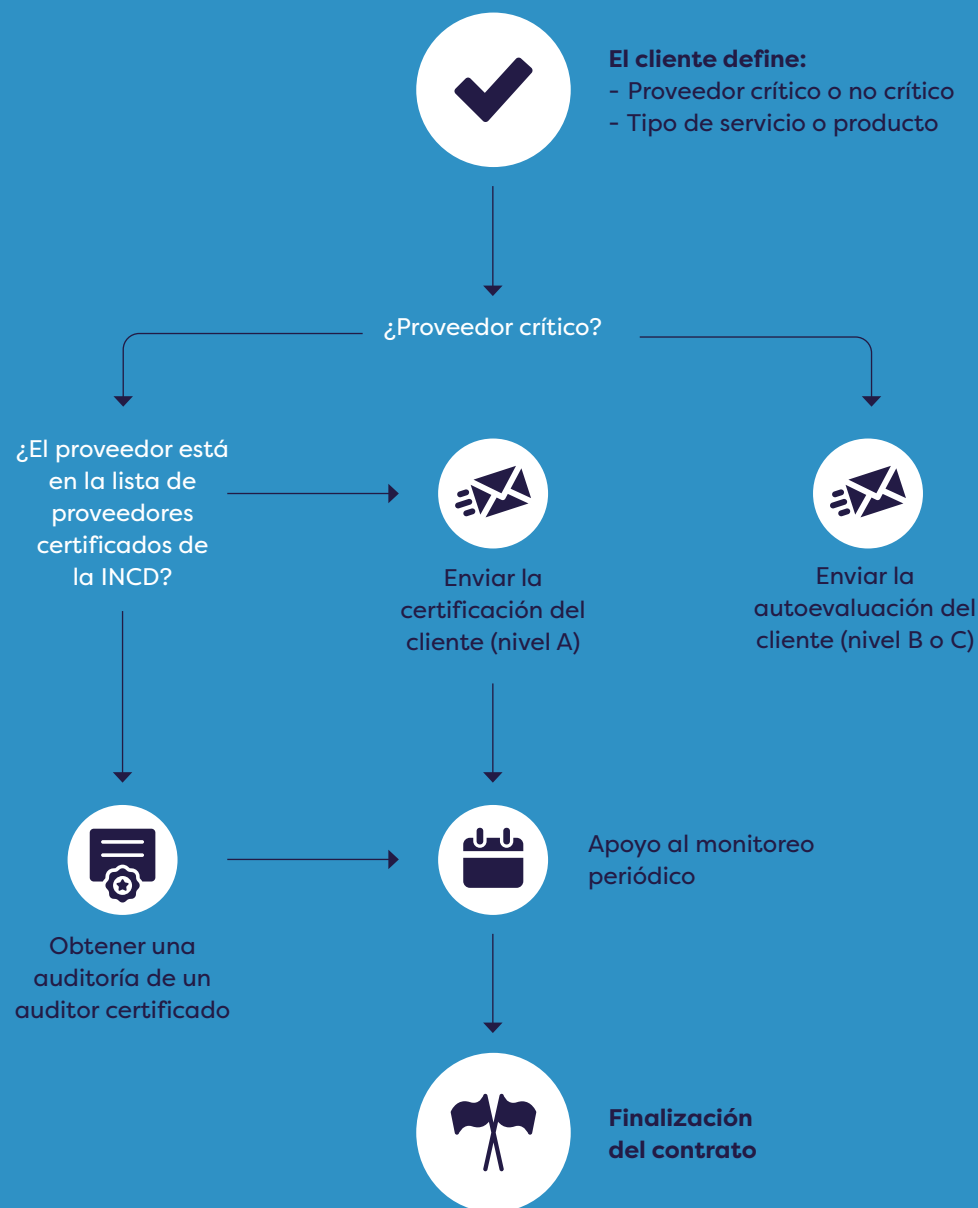
El proveedor completará el cuestionario disponible en el sitio web de la Dirección sobre el estado de sus medidas de ciberdefensa, en función de los servicios que preste a sus clientes, e incluirá la diferencia entre la situación real y la deseada (información dada de forma anónima).

Los proveedores clasificados en el nivel C deben enviar el cuestionario a la organización tras su firma por una persona autorizada.

Los proveedores clasificados en el nivel B deben enviar a la organización el cuestionario firmado por una persona autorizada y acompañado de los documentos de apoyo según se define en esta Metodología para la Protección de la Cadena de Suministro (con

el fin de determinar la efectividad de los controles de ciberdefensa requeridos).

Los proveedores clasificados en el nivel A deben completar el cuestionario junto con un inspector de la cadena de suministro certificado por la Dirección y enviar al organismo de certificación el cuestionario firmado por una persona autorizada junto con documentos de apoyo según lo definido en esta Metodología para la Protección de la Cadena de Suministro con el objeto de obtener un certificado oficial. El certificado y, de ser necesario, todos los demás materiales se enviarán a la organización. La certificación deberá renovarse periódicamente en función de lo establecido en esta Metodología para la Protección de la Cadena de Suministro. **Pueden verse más detalles en el anexo 2.**

**Gráfico 3.** Pasos y consideraciones desde la perspectiva del proveedor

# /06.

## Descripción del proceso de regulación

El proceso de regulación de la Dirección Nacional de Ciberseguridad incluye a dicha Dirección como el único organismo de acreditación, a organismos de certificación (como el Instituto Israelí de Normalización), a organismos de inspección que controlan la cadena de suministro y a los clientes en este proceso, es decir, los proveedores certificados (gráfico 4).

### Regulación por parte de los organismos de certificación en nombre de la Dirección Nacional de Ciberseguridad

Se ha definido un proceso piloto con el Instituto Israelí de Normalización como principal organismo de certificación:

## 01

Inspectores de la cadena de suministro que operan en nombre de la Dirección.

## 02

Proveedores certificados por la Dirección.

Este proceso define las interfaces entre la Dirección Nacional de Ciberseguridad y el organismo de certificación, y entre ellos y los organismos de inspección y proveedores. El organismo de certificación también debe proporcionar servicios de capacitación con el fin de cualificar a los inspectores de la cadena de suministro de acuerdo con la Metodología para la Protección de la Cadena de Suministro.

Se está realizando un llamamiento público a las organizaciones de la economía para establecer organismos de certificación adicionales.

### Regulación de los inspectores de la cadena de suministro (auditores certificados)

Se han definido los criterios de admisión a los cursos de certificación para inspectores de la cadena de suministro. Estos inspectores están

certificados en nombre de la Dirección con el fin de evaluar la calidad de las respuestas de los cuestionarios para proveedores y las pruebas requeridas para que el organismo de certificación emita un certificado. Los criterios de admisión son muy estrictos (comprenden una considerable experiencia en la realización de auditorías de ciberdefensa, un examen de ingreso profesional en ciberdefensa y una entrevista personal), y están destinados a encontrar inspectores de alto nivel, habida cuenta de que mantener la confianza de la

economía depende de inspectores profesionales independientes de alta calidad.

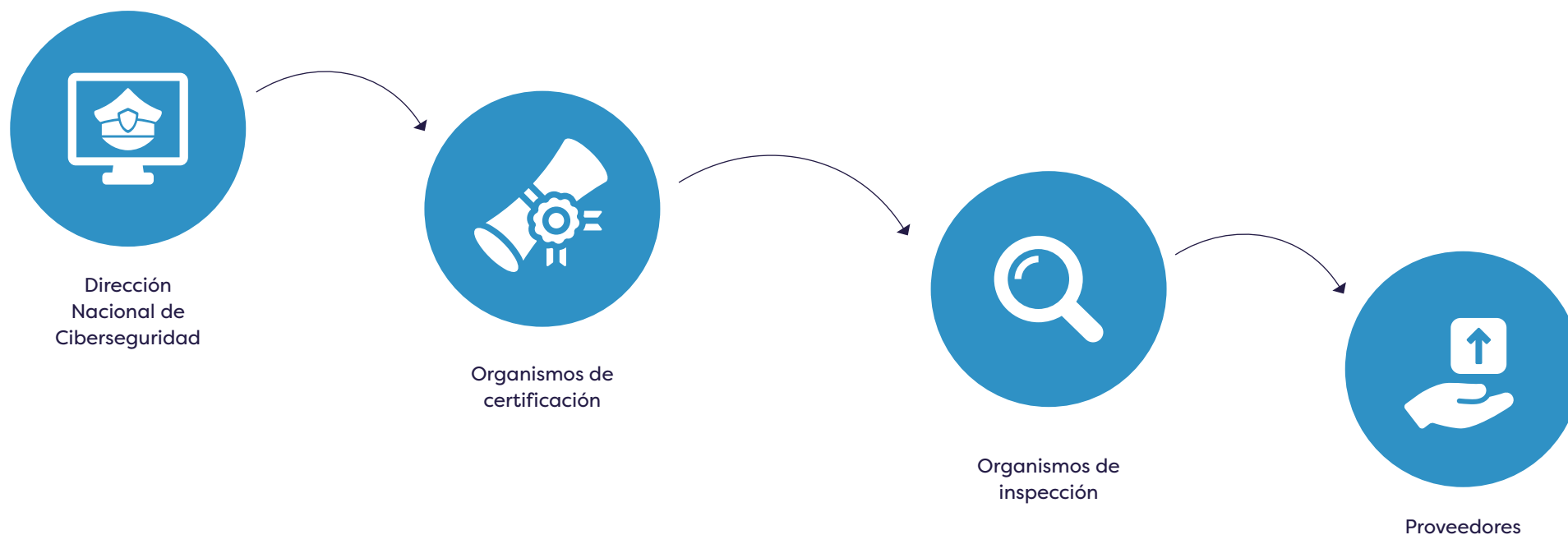
Un curso breve proporciona instrucción sobre la Metodología para la Protección de la Cadena de Suministro de la Dirección Nacional de Ciberseguridad y sobre el proceso de certificación de proveedores.

### Regulación de proveedores certificados

Se ha definido el proceso de certificación del proveedor, desde la presentación de una solicitud de certificación hasta la emisión de un certificado, la validez del certificado, etc. El objetivo de este proceso es minimizar la carga sobre los proveedores al tiempo que se mantiene una alta calidad en el proceso y sus resultados a fin de garantizar que la certificación sea confiable.

**Pueden verse más detalles en el anexo 4.**

**Gráfico 4.** Participantes en el proceso de regulación



# Anexos

## Anexo 1. El proceso desde la perspectiva de la organización

Se presenta ahora el proceso de protección contra riesgos cibernéticos de la cadena de suministro desde la perspectiva de una organización de la economía israelí (particularmente desde el punto de vista del Director de Ciberdefensa y del CISO de la organización).

Esta es una metodología ordenada y práctica para gestionar la ciberdefensa de la cadena de suministro, que está acompañada por un conjunto de controles detallados que se recomienda que todas las organizaciones de la economía israelí implanten con el fin de contar con una gestión continua y efectiva de la cadena de suministro.

La gestión de la cadena de suministro abarca el ciclo de las actividades de la organización con respecto a los proveedores de bienes y servicios, que comienza en la etapa preliminar de cartografía y clasificación de los activos de información de la organización, seguido por el mapeo de los proveedores que la organización contratará. Los proveedores

deben ser inspeccionados periódicamente a lo largo del tiempo, utilizando un conjunto de criterios y mediciones predefinidos. Durante sus acuerdos con los proveedores, las organizaciones deben realizar evaluaciones de riesgos constantemente y tomar las medidas que resulten necesarias.

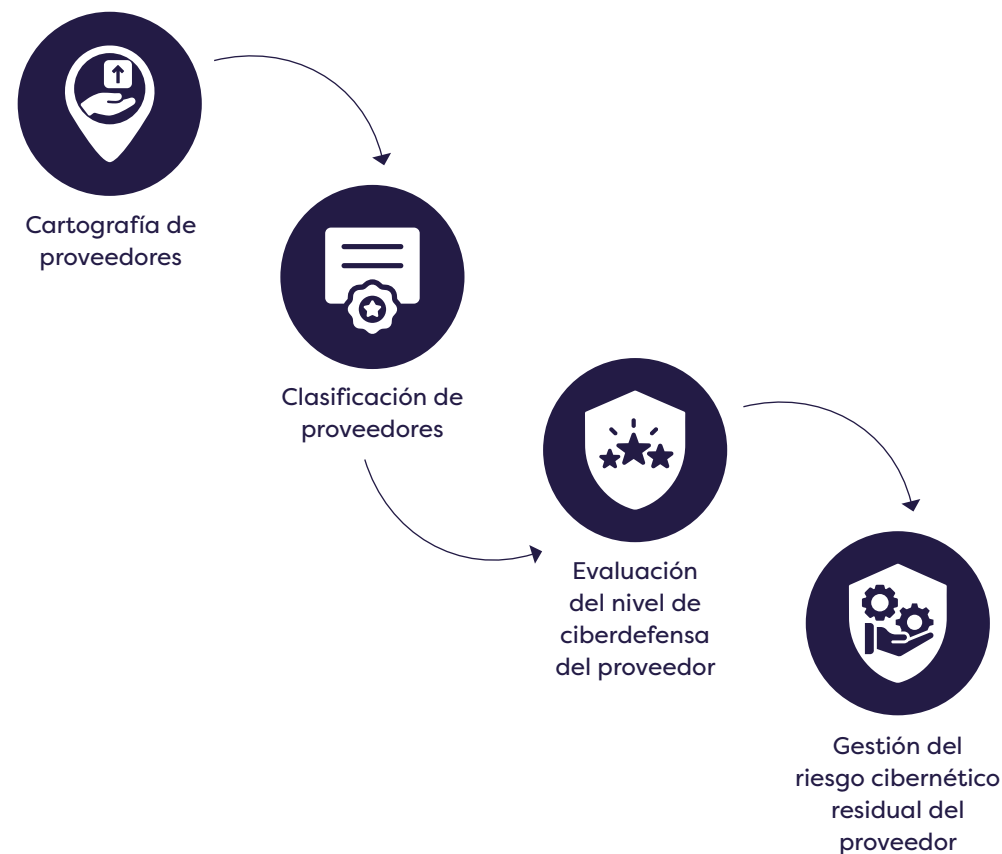
Es importante hacer hincapié en la necesidad de incorporar en los acuerdos integrales con los proveedores todos los criterios y niveles de servicio requeridos para cumplir con los estándares necesarios en materia de seguridad de datos para cada bien o servicio. Las organizaciones deben instituir procedimientos ordenados y documentar el proceso de selección de proveedores y los procedimientos para gestionar sus acuerdos con ellos. Además, las organizaciones deben proporcionar una capacitación general sobre aspectos de seguridad de datos a todos los empleados del proveedor que se espera que participen en las labores que engloba el acuerdo con la organización. Otra cuestión fundamental es el proceso de rescisión de un acuerdo con un proveedor. Las organizaciones tienen que velar por la correcta ejecución de todas las disposiciones de sus acuerdos con proveedores relacionadas con la eliminación de los datos de la organización y cancelación de las autorizaciones de acceso del proveedor.

El conjunto de controles y los aspectos de especial importancia que se presentan a continuación constituyen una metodología ordenada para administrar la cadena de suministro de una organización. Las activida-

des de ciberdefensa de las organizaciones contra los riesgos de la cadena de suministro se pueden dividir en las etapas que se mencionan a continuación.

### Operaciones en relación con proveedores

**Gráfico A1.1.** Operaciones en relación con proveedores para la ciberdefensa en la cadena de suministro





## Cartografía de proveedores

Se debe preparar una lista de los proveedores de la organización que prevea los diversos tipos de prestadores de servicios, como proveedores de desarrollo de *software*, *hardware* y comunicaciones, empresas que implantan e integran sistemas en la organización, empresas de consultoría y encuestas sobre riesgos, y proveedores de servicios tales como contadores, abogados, impresores, editores, profesionales de imagen de marca, soporte técnico, integración, etcétera.

La lista debe ser validada por los profesionales de la organización que estén familiarizados con las actividades que se llevan a cabo con esos proveedores. Se recomienda involucrar al personal de compras en este proceso y en la preparación de la lista, así como al personal del departamento de sistemas de tecnologías de la información (TI) (para identificar *software* externo, proveedores de servicios de TI, proveedores con acceso remoto a la organización, etc.).

Además, se debe instituir un proceso organizativo para garantizar que el personal de ciberdefensa sepa cuándo se agrega un nuevo proveedor y cuándo se firma un nuevo acuerdo. Podría implantarse en el marco de un procedimiento de trabajo en la organización e involucrando al departamento de seguridad de datos o ciberdefensa en el proceso de abrir una nueva cuenta de proveedor en el departamento financiero y en el sistema de información, etcétera.

La cartografía de proveedores debe incluir referencias al tipo de servicio que preste cada proveedor y a las siguientes categorías:

# 01

**Acceso remoto:** se refiere a los proveedores que necesitan conectarse a los recursos de la organización en el marco del acuerdo para proporcionar el producto o servicio. En tales casos, se espera que el proveedor trabaje de conformidad con la política de seguridad de la organización en materia de conectividad remota. No obstante, hay situaciones en las que el proveedor define su modo de conexión remota con sus clientes. En estos casos, la organización debe verificar que el modo de conexión se realice de forma segura. Tales proveedores suelen ser empresas de informática, TI, comunicaciones o desarrollo que podrían causar daños importantes a la organización. En el cuestionario para proveedores se definen los controles y requisitos de defensa específicos para estos servicios.



# 02

**Servicios en la nube:** se trata de proveedores que proporcionan *software* como servicio (SaaS, por sus siglas en inglés) o plataforma como servicio (PaaS, por sus siglas en inglés) dentro del alcance del contrato. Estos proveedores incluyen los servicios habituales en la nube, como SaaS, PaaS e infraestructura como servicio (IaaS, por sus siglas en inglés). Entre ellos se cuentan empresas de almacenamiento de webs, sistemas de información que tienen acceso a la organización a través de una nube, servicios en línea que utiliza la organización, etc. También pueden ser proveedores cuya disponibilidad es esencial para la organización y aquellos para los cuales el grado de confidencialidad y confiabilidad de la información es particularmente sensible. En el cuestionario para proveedores se definen los controles y requisitos de defensa específicos para estos servicios. Ha de tenerse en cuenta que esta categoría no prevé casos en los que la información se almacena fuera de línea (como el almacenamiento de cintas de respaldo, documentos, etc.).

# 03

**Desarrollo de *software*:** hace referencia a proveedores que desarrollan *software* que se instala en la organización. Estos pueden suponer una posible violación de seguridad. El nivel de ciberdefensa de la

organización depende en gran medida del nivel de ciberdefensa en los procesos de desarrollo y gestión del ciclo de vida del proveedor que desarrolla el *software*. En el cuestionario para proveedores se definen los controles y requisitos de defensa específicos para estos servicios.

# 04

**Requisitos generales:** se precisa que cada proveedor mantenga un nivel básico de ciberdefensa con respecto a diversos problemas, independientemente del tipo de servicio prestado. Estos requisitos representan el mínimo exigido de cada proveedor que la organización contrata, de acuerdo con el nivel de riesgo derivado de él (proveedor crítico o no crítico). Los proveedores de esta categoría pueden incluir empresas de imagen de marca, empresas de encuestas, diversos tipos de empresas de consultoría (asesoramiento cibernético, asesoramiento operativo, asesoramiento estratégico, etc.), abogados, contadores, empresas que prestan servicios de traducción, empresas de impresión y otros proveedores si un ciberataque contra ellos pone en peligro a sus clientes debido a la exposición de información y otros riesgos.

Al final de esta etapa, las organizaciones obtendrán un cuadro que recogerá la cartografía de proveedores, el cual contendrá al menos los aspectos que figuran en el cuadro A1.1.

**Cuadro A1.1.** Cartografía de los proveedores

## Cartografía de proveedores

Nombre del proveedor	Tipo de servicio o producto que proporciona	Contacto de la organización con el proveedor	Datos de contacto del representante del proveedor encargado de la ciberdefensa	Tipo de servicios prestados (basados en la nube, desarrollo de software, acceso remoto, requisitos generales)
----------------------	---	--	--	---



Clasificación de proveedores

Los proveedores deben clasificarse según tres niveles de riesgo, los cuales se presentan en el cuadro A1.2. La clasificación de los proveedores debe tener en cuenta las repercusiones o daños potenciales que se pueden causar a la organización como resultado de un incidente cibernético en el sistema de un proveedor. Se pueden usar varios criterios para calcular el daño potencial, como los que se indican en el cuadro A1.2.

Trabajar con el cuadro A1.2 ayudará a clasificar a los proveedores de acuerdo con los diversos criterios. La clasificación final de un proveedor (en los niveles A, B o C) se basará en el daño potencial máximo. Por ejemplo, un proveedor clasificado en el nivel A en un criterio se considerará que posee un nivel de daño potencial A aunque se incluya en el nivel C para el resto de los criterios.

Cuadro A1.2. Ejemplos de criterios para calcular el daño potencial

Rango de proveedor	Nivel previsible de daño a la organización procedente del proveedor	Daño económico a la organización (incluidos los costos resultantes de la pérdida de ingresos, reputación, regulaciones, etc.)	Daño a la continuidad del negocio	Sensibilidad de los datos a los que tiene acceso el proveedor	Probabilidad de la ocurrencia de un incidente cibernético en el marco de un acuerdo
C	Bajo	Más de US\$3.000	La recuperación de un incidente cibernético en un proveedor llevará varias horas	La información no es muy sensible	<b>Baja dependencia cibernética.</b> Ejemplos: proveedor de equipos de oficina, servicios especializados que no involucren la información de la organización y que no cuenten con autorizaciones de acceso a los sistemas de la organización, etc.
B	Moderado	Más de US\$30.000	La recuperación de un incidente cibernético en un proveedor llevará varios días	La información es moderadamente sensible	<b>Dependencia cibernética moderada durante el acuerdo con el proveedor</b>
A	Alto	Más de US\$300.000	La recuperación de un incidente cibernético en un proveedor llevará varias semanas	Información organizacional confidencial, como patentes, secretos comerciales, etc.	<b>Alta dependencia cibernética.</b> Ejemplos: proveedores de servicios de TI, con autorizaciones de acceso remoto; proveedores de equipos de software; proveedores que tienen material sensible en una nube o en sistemas en las instalaciones del proveedor

# 01

Los proveedores clasificados en el nivel A deberán demostrar su nivel de ciberdefensa en los requisitos del cuestionario para proveedores mediante un inspector certificado de la cadena de suministro. Puede consultarse la lista de inspectores certificados en el sitio web de la Dirección y en el módulo de regulación.

# 02

Los proveedores clasificados en el nivel B deberán completar el cuestionario para proveedores y adjuntar las pruebas en función de lo requerido en el cuestionario. El proveedor enviará la prueba al cliente a través del canal seguro que acuerden las partes.

# 03

Los proveedores clasificados en el nivel C completarán el cuestionario para proveedores y harán firmar a un abogado o al presidente de la compañía una declaración del proveedor con respecto al nivel de cumplimiento de los requisitos de ciberdefensa en el cuestionario.

Al final de esta etapa, las organizaciones contarán con una cartografía de los proveedores con la clasificación de su nivel de riesgo y el grado de criticidad de cada uno de ellos (cuadro A1.3).

**Cuadro A1.3.** Cartografía de los proveedores con clasificación de nivel de riesgo

Cartografía de proveedores					Categoría de proveedores
Nombre del proveedor	Características del acuerdo	Contacto de la organización con el proveedor	Datos de contacto del representante del proveedor para cuestiones relacionadas con la ciberdefensa	Categoría de servicio que se proporciona (servicio basado en la nube, desarrollo de software, acceso remoto, servicio que implica la exposición de información del cliente)	Nivel de riesgo del proveedor (proveedor crítico o no crítico)
<b>Ejemplo A</b> Consultoría estratégica	Asistir a la Dirección de la organización en la construcción de un plan estratégico	Anat	XYZ	Requisitos generales: redacción de documentos sensibles para la organización. El proveedor tiene planes de gestión sensibles con respecto a nuevas esferas de negocio a las que la organización planea expandirse en los próximos años	Sí
<b>Ejemplo B</b> Implementador de un sistema de planificación de recursos empresariales	Implantar el sistema junto con el departamento de operaciones	Israel	ABC	Desarrollo de software: ayuda al departamento de sistemas de TI con la implementación del sistema	No
<b>Ejemplo C</b> Desarrollo y almacenamiento de sitios web	Almacenar el sitio web de la empresa (incluidas actualizaciones, mantenimiento, etc.)	Or	AAA	Almacenamiento en la nube y mantenimiento del sitio web de la compañía	Sí
<b>Ejemplo D</b> Integración	Soporte de equipos y comunicaciones	Eli	BBB	Requisitos generales: el proveedor no tiene acceso remoto y su trabajo se centra en ayudar al personal de comunicaciones de la empresa	No
<b>Ejemplo E</b> Despacho de abogados	Redacción de patentes	Israel	CCC	Requisitos generales: el proveedor tiene información confidencial sobre la compañía en su computadora personal y en un dispositivo USB	Sí

## Evaluación del nivel de ciberdefensa del proveedor

Con el objeto de evaluar el nivel de ciberdefensa de un proveedor, las organizaciones deben exigir a sus proveedores que cumplan con los requisitos de ciberdefensa que se exponen en esta Metodología para la Protección de la Cadena de Suministro. Para este fin, las organizaciones definirán los siguientes parámetros para los proveedores:

# 01

**Definir si el proveedor es crítico para la organización:** con el fin de adaptar la ciberdefensa al riesgo derivado de la contratación con el proveedor específico, las organizaciones deben definir si se trata o no de un proveedor crítico. Eso afecta la cantidad y alcance de los controles que se requieren. Por ejemplo, un proveedor no considerado crítico deberá mantener copias de seguridad básicas, mientras que un proveedor crítico deberá mantener e implementar controles más

avanzados. Nota: algunas normas y reglamentos contienen una definición de lo que se considera un proveedor crítico.

# 02

**Determinar la categoría de servicio pertinente:** las organizaciones deben informar a sus proveedores sobre lo que se espera de ellos dentro del alcance del acuerdo en materia de acceso remoto, desarrollo de software, etc. Aunque existen requisitos generales mínimos en cada acuerdo, en los casos en que el acuerdo incluya tareas especiales, como procesos de desarrollo, el proveedor debe cumplir con los aspectos adicionales de ciberdefensa que se especifican en el cuestionario para proveedores de esta Metodología para la Protección de la Cadena de Suministro.

# 03

**Establecer el tipo de respuesta esperada:** las organizaciones deben informar a sus proveedores si deben completar el informe utilizando un formulario de autodeclaración que generan a partir del sistema, si deben adjuntar documentos de apoyo de acuerdo con los requisitos del cuestionario o si tienen que demostrar el cumplimiento de los requisitos de la Metodología para la Protección de la Cadena de Suministro mediante un tercero independiente (como un inspector certificado).

Si un proveedor ya está certificado, podría ser suficiente para una organización recibir los resultados del estudio o agregar algunos requisitos específicos. Se recomienda elaborar un plan de trabajo anual que defina el cronograma para enviar los requisitos de ciberdefensa y a qué proveedores hacerlo, incluido un modelo de carta de requisitos de ciberdefensa estándar, lo cual agilizará el proceso en la organización y permitirá verificar que se ha entrado en contacto con todos los proveedores pertinentes (de acuerdo con el plan de gestión de riesgos de la organización).

**El nivel de riesgo de algunos proveedores puede verse afectado por aspectos regulatorios, o el proveedor podría estar listado como proveedor en tiempos de emergencia nacional.**

## Gestión del riesgo cibernético residual del proveedor

En algunos casos, a pesar de la necesidad de contratar a proveedores que mantengan un nivel adecuado de ciberdefensa, la dirección de una organización puede estar obligada a firmar un acuerdo bajo cualquier circunstancia. Para gestionar los riesgos de manera efectiva, se recomienda tener en cuenta las cuatro alternativas en la gestión de riesgos:

# 01

**Aceptar el riesgo:** en este caso, el riesgo potencial debe presentarse a la Dirección de la organización, junto con la decisión de no adoptar medidas especiales en el acuerdo con ese proveedor. Puede tratarse de un proveedor no crítico, por lo que la organización decide no exigirle requisitos de ciberdefensa, o de casos de dependencia importante de un proveedor que, aunque no está preparado para cumplir con los requisitos de ciberdefensa, la organización contrata debido a otras limitaciones o motivos.

# 02

**Transferir el riesgo,** por ejemplo, comprando un seguro para cubrir pérdidas de este tipo.

# 03

**Mitigar el riesgo,** por ejemplo, agregando controles de compensación en relación con el proveedor.

# 04

**Rechazar el riesgo,** por ejemplo, si la Dirección recomienda no renovar el acuerdo con el proveedor o rescindirlo inmediatamente.





## Operaciones intraorganizacionales

**Gráfico A1.2.** Operaciones intraorganizacionales para la ciberdefensa en la cadena de suministro



### Cartografía de riesgos

Tras completar los procedimientos para los contratos que la organización tenga con sus proveedores –cartografía, clasificación, evaluación del nivel de ciberdefensa de los proveedores y gestión del riesgo residual de los proveedores, tal como se describe previamente–, se debe elaborar un mapa de riesgos, que el Director de Ciberdefensa de la organización debe mantener y actualizar de manera regular y debe ser aprobado periódicamente por la Dirección de la organización.

### Aspectos de compras

La definición del acuerdo de la organización debe tener en cuenta los aspectos de ciberdefensa presentados en este documento a través de un proceso estructurado.

## 01

Al contratar un nuevo proveedor, debe informarse automáticamente al Director de Ciberdefensa. Si es posible, el sistema de gestión de proveedores debe automatizar este proceso y agregar campos para definir los detalles del proveedor en relación con la ciberdefensa (persona de contacto, clasificación de proveedores, servicios que proporciona, etc.). Si se puede, el proceso de creación de un nuevo proveedor en el

sistema debe supeditarse a la aprobación del Director de Ciberdefensa o del CISO de la organización.

## 02

Al renovar un acuerdo con un proveedor existente, las organizaciones deben asegurarse de que la renovación tenga en cuenta el nivel actual de ciberdefensa del proveedor y los procedimientos para cumplir con las recomendaciones destinadas a remediar las deficiencias que la organización haya detectado en el proveedor.

## 03

Periódicamente se debe hacer una comparación entre los proveedores de una organización y la lista de proveedores certificados en el módulo de certificación de los objetivos y el sistema de controles de la organización.

## 04

La Dirección de la organización debe asignar los recursos necesarios para realizar auditorías de proveedores críticos, según la definición del funcionario pertinente de la organización, y de las posibles pérdidas que podrían causar.

### Política de evaluación de riesgos en la cadena de suministro

La Dirección debe redactar un procedimiento de trabajo y validarlo periódicamente. La política de una organización debe incorporar referencias a controles compensatorios en aquellos acuerdos en los que no sea posible llevar al proveedor al nivel requerido de ciberdefensa. Estos controles pueden incluir, por ejemplo, el establecimiento de un entorno de proveedores en la organización, el suministro de computadoras y equipos reforzados a los proveedores, la decisión de que determinados tipos de tareas de un proveedor solo podrán ser realizadas en las instalaciones de la organización, etcétera.

Esa política debe incluir referencias a herramientas de gestión para controlar el proceso. Estas herramientas pueden ser útiles para la organización tanto durante la etapa de cartografía y evaluación de proveedores como durante el seguimiento para garantizar que se aplican las recomendaciones y tareas con respecto a los diversos proveedores. Se trata de herramientas comunes, tales como gobierno, gestión de riesgos y cumplimiento (GRC, por sus siglas en inglés) o gestión de riesgos en relación con los proveedores (VRM, por sus siglas en inglés). La ventaja de estas herramientas radica en la capacidad de obtener una imagen completa del estado de los proveedores, así como alertas, presentación de un informe de situación de referencia, automatización de las comunicaciones con ellos y

una evaluación del nivel de ciberdefensa del proveedor, etcétera.

La política también debe incluir referencias a los siguientes aspectos: cambios en el tipo de acuerdo con un proveedor y en la estructura organizativa o tecnológica del proveedor, aspectos de control y auditoría, modo de acceso remoto de los proveedores, aspectos sobre la subida de información a una nube, manejo de incidentes de seguridad de datos en un proveedor, procedimientos para rescindir acuerdos con proveedores, y la frecuencia y el modo de las consultas sobre ciberdefensa a los distintos proveedores de acuerdo con los requisitos de esta Metodología para la Protección de la Cadena de Suministro.

Finalmente, la política de la organización debe definir la parte responsable de proteger la información que posee un proveedor (a lo largo de toda la cadena de custodia, incluidos los proveedores y los subcontratistas de los proveedores).

### Acuerdo

Se debe firmar un acuerdo con el proveedor en el que se reflejen todos los aspectos de la gestión de los riesgos cibernéticos en la cadena de suministro. En el anexo 5 puede verse un modelo de acuerdo. La incorporación de aspectos de ciberdefensa en los contratos y acuerdos debe seguir un procedimiento de trabajo coordinado con el departamento de

compras de la organización. Se debe prestar especial atención a los contratos a largo plazo ya existentes. En estos casos, a menudo es más difícil convencer al proveedor para que mejore su nivel de ciberdefensa. Se recomienda que el departamento de compras de la organización analice formas de motivar a los proveedores para que cumplan con los requisitos de ciberdefensa que se esperan de ellos.

### Reunión para informar al proveedor

Antes de que un proveedor comience a trabajar o tenga acceso al sistema de la organización, ya sea física o electrónicamente, cada uno de los empleados del proveedor que participa en el acuerdo debe recibir información sobre los siguientes temas:

# 01

Las amenazas pertinentes para el sistema.

# 02

Las pérdidas potenciales resultantes de un ataque cibernético en el sistema.

# 03

Detalles de las directivas que deberán cumplir e implementar.

La sesión informativa debe ser presentada por un profesional de la organización experto en los requisitos de ciberdefensa que deben cumplirse para minimizar en la medida de lo posible la exposición de la organización a los riesgos.

Tras la sesión informativa, todos los empleados del proveedor deben firmar una declaración en la que se comprometen a implementar los requisitos de seguridad.

**Una vez que haya finalizado el acuerdo con el proveedor, la organización debe conservar tales documentos de declaración durante un mínimo de dos años o lo que resulte necesario.**



**Controles que han de implementarse durante la vigencia del acuerdo**

Si un proveedor trabaja en las instalaciones de la organización, esta debe asegurarse de que las actividades se realicen de acuerdo con las directivas impuestas a los empleados de la organización.

En cambio, si un proveedor trabaja desde sus propias instalaciones, la organización debe enviarle un documento sobre requisitos de seguridad cibernética antes de que comience a operar o acceda al sistema de la organización, ya sea de manera física o electrónica.

# 01

En el caso de los proveedores críticos, la organización debe realizar auditorías al menos una vez al año en las instalaciones del proveedor a fin de verificar que esté implementando las directivas de seguridad cibernética.

# 02

Para los proveedores críticos, se recomienda considerar el uso de herramientas de monitoreo capaces de proporcionar indicaciones

en tiempo real y monitoreo continuo del nivel de defensa del proveedor (monitoreo de control continuo).

La organización debe definir aquellas actividades para las que se requiere que el proveedor utilice medios de identificación robustos.

También debe estar preparada para operar durante un incidente de seguridad de datos, contractualmente, tecnológicamente y a través de procesos.

Debido a los riesgos incurridos en razón del acceso remoto de un proveedor a los sistemas de la organización durante sus actividades (si se diera el caso), es esencial que las organizaciones mantengan mecanismos de seguridad y control para ayudar a minimizar tales riesgos, como por ejemplo:

# 01

El uso de un entorno específico separado con una configuración virtual.

# 02

Las conexiones de Internet a los sistemas de la organización se realizarán mediante un protocolo de sesión que difiera del utilizado al conectar el entorno separado a los sistemas de la organización.

# 03

El acceso a este entorno estará en un formato de lista blanca y debe limitar las estaciones de trabajo y direcciones que tienen autorización de acceso, los protocolos, los tiempos de conexión, la duración de una conexión activa y la desconexión en caso de inactividad, y limitar las aplicaciones con acceso autorizado.

# 04

El entorno volverá a un estado estable seguro al final del uso.

# 05

La duración de una conexión activa se limitará y desconectará si se observa inactividad.

# 06

La cuenta de usuario para el acceso desde el exterior será diferente de la utilizada para el acceso interno y debe tener diferentes datos de identificación y autenticación.

# 07

La autenticación se basará en dos factores diferentes considerando las siguientes alternativas: un componente de contraseña de un solo uso (OTP, por sus siglas en inglés) específico que no esté conectado a medios, una tarjeta inteligente, datos biométricos o una contraseña.

# 08

La cuenta y autorizaciones a nivel de aplicación para el acceso remoto serán diferentes de las utilizadas para el acceso interno.

# 09

Se evitará que los usuarios se conecten simultáneamente a redes o sistemas de forma local y remota. Se instaurará una alerta para esos casos.

# 10

Todas las aplicaciones en una estación de trabajo operarán utilizando un formato de lista blanca y se evitará abrir aplicaciones no autorizadas.

# 11

Los datos de identificación y autenticación de una cuenta de administración remota diferirán de las cuentas de administración interna y deben gestionarse en un grupo específico.

# 12

La organización determinará que cualquier usuario con acceso remoto solo recibirá las autorizaciones de acceso necesarias para las operaciones de administración permitidas a través del acceso remoto, según lo definido por el profesional correspondiente en nombre de la organización.



# 13

Se realizará el registro y monitoreo del tráfico durante toda la conexión; se identificará cualquier anomalía y desviación de las operaciones de gestión autorizadas, así como cualquier incumplimiento de la política de ciberseguridad (los proveedores deben ser informados de que todas sus operaciones en los sistemas de la organización serán grabadas).

# 14

Se evitará que los proveedores obtengan acceso no autorizado a los sistemas de la organización, en particular al entorno de producción.

# 15

La organización garantizará un acceso seguro y el aislamiento de sus operaciones de todos los entornos de trabajo de sus proveedores.

# 16

La organización redactará un procedimiento escrito que describa el proceso de conexión del proveedor con el propósito de administrar o mantener los componentes del sistema en la red, que haga referencia a lo siguiente:

- Conexión y aprobación de operaciones, únicamente por parte del profesional competente en nombre de la organización.
- Modo de monitoreo y grabación.
- Recepción de alertas y manejo de anomalías.
- Interrupción de operaciones y cierre de conexiones.
- Verificación de desconexiones de los sistemas de la organización.

# 17

Se creará la capacidad de interrumpir inmediatamente una conexión en caso de que se detecte un incidente anómalo. Además, se evitará la posibilidad de añadir o eliminar archivos en este canal, algo que solo se habilitará en un canal separado para desactivar y reconstruir contenido, prevenir la pérdida de datos y para el oscurecimiento (*blackening*) de soportes electrónicos.

Debido a los riesgos incurridos cuando un proveedor externo tiene acceso a las instalaciones de la organización, es esencial que esta mantenga mecanismos de seguridad y control para ayudar a minimizar esos riesgos:

## 01

Para las actividades de un proveedor permanente, se debe asignar una computadora específica de la organización que contenga todas las aplicaciones necesarias para las actividades del proveedor.

## 02

Para las actividades *ad hoc*, como pruebas de penetración, exámenes de vulnerabilidad, etc., el volumen de las actividades del proveedor debe estar predefinido de manera clara y precisa, junto con indicadores de éxito y fracaso, incidentes y respuestas en caso de mal funcionamiento. Se debe designar a un miembro del personal interno para supervisar activamente a los empleados del proveedor.

## 03

Las contraseñas de administración no se divulgarán a los proveedores. Si es necesario, se abrirá una cuenta temporal únicamente con las autorizaciones necesarias para la actividad que se vaya a llevar a cabo.

## 04

Si las contraseñas de administración se divulgan para realizar una actividad, se cambiarán inmediatamente después.

## 05

El personal pertinente será informado sobre el comienzo y el final de la actividad para que esté más alerta y aumente el umbral de sensibilidad frente a incidentes anómalos.

## 06

Cualquier actividad realizada por un proveedor en los sistemas de la organización (como pruebas de penetración o exámenes de vulnerabilidad) debe llevarse a cabo de manera tal que no afecte al nivel de ciberseguridad y tras analizar las implicaciones de los riesgos derivados de tales actividades.

## 07

Al final de la actividad, se realizará una prueba para determinar qué operaciones se llevaron a cabo realmente, se cerrarán las cuentas temporales y se retirarán las autorizaciones asignadas para la actividad.

### Protección de datos operacionales confidenciales

Los datos operacionales confidenciales son aquellos relacionados con la operación, mantenimiento, medidas de seguridad y administración de los sistemas, que en caso de ser atacados pueden permitir que se tomen atajos hacia sistemas críticos o robos de información confidencial:

- Nombres de usuario y contraseñas.
- Topología de red (como diagramas de red con direcciones IP).
- Parámetros de equipos de seguridad de datos y comunicaciones (como reglas de cortafuegos y definiciones de comunicaciones).
- Datos técnicos u operacionales sobre el sistema (como manuales de operación o código fuente).
- Fotografías de áreas y componentes particularmente sensibles (como salas de servidores y equipos de comunicaciones).

- Copias de seguridad que contienen archivos de datos y bases de datos.
- Información sobre la reducción temporal de las medidas de seguridad de datos en el sistema con el fin de realizar operaciones de mantenimiento y actualización.

La información confidencial debe almacenarse de forma segura y encriptada, y únicamente el personal autorizado debe poder acceder a ella. Además, se llevará a cabo un seguimiento a fin de detectar cualquier intento de acceso y uso de la información, incluso de los intentos fallidos.

También se impedirá que el personal no autorizado envíe información clasificada fuera de la red de la organización utilizando medios específicos para ello (como la prevención de pérdida de datos). Se verificará que la identificación de información confidencial o privilegiada también incluya referencias a información operacional confidencial.

Toda información operacional confidencial se enviará a una parte externa únicamente a través de una configuración segura (correo electrónico cifrado) o un mecanismo seguro de transferencia de archivos (como cajas fuertes).

Asimismo, el disco duro y el sistema básico de entrada y salida (BIOS, por sus siglas en inglés) de las computadoras portátiles que contienen dicha información estarán encriptados.

### Protección de la información en los sistemas de control industrial (tecnología operativa)

La mayoría de los sistemas de control industrial se diseñaron hace mucho tiempo, antes de que se conocieran las amenazas cibernéticas. Por ello, estos sistemas carecen de controles de seguridad de datos. Debido al aumento de las amenazas internas y externas contra las infraestructuras industriales y críticas, se necesitan controles que proporcionen detección y defensa en tiempo real, al tiempo que cumplan con los requisitos técnicos y operativos especiales de los sistemas de control industrial. Puede consultarse el documento de la Dirección Nacional de Cibernética sobre controles específicos relacionados con los sistemas de control industrial<sup>7</sup> o los documentos pertinentes publicados por las principales organizaciones de normalización en este ámbito.

### Controles compensatorios y sanciones

Cuando la organización no puede confiar en el nivel de seguridad de datos del proveedor, a veces se necesitan controles compensatorios durante un acuerdo con un proveedor. He aquí algunos ejemplos de controles compensatorios que pueden preverse en un acuerdo:

7. El documento *Reducción de riesgos cibernéticos para los sistemas de control industrial (ICS)* se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad.



# 01

La organización debe proporcionar una computadora portátil o estación de trabajo reforzada de uso exclusivo para las actividades del proveedor.

# 02

En la medida de lo posible, la organización exigirá al proveedor que realice su trabajo *in situ* en la organización.

# 03

Si el proveedor no trabaja en entornos separados, la organización debe proporcionar un entorno seguro a través del cual el proveedor proporcionará sus servicios.<sup>8</sup>

# 04

La organización debe probar el sistema o servicio del proveedor utilizando herramientas internas y

realizar pruebas de penetración antes de pasar el sistema o servicio a la etapa de producción.<sup>9</sup>

A veces es necesario imponer sanciones en relación con las actividades de un proveedor. He aquí algunos ejemplos:

## 01

Si un proveedor no cumple con los criterios que la organización haya definido como críticos para el propósito del acuerdo. Los acuerdos deben estar supeditados a la realización de un examen al proveedor durante el cual la organización (u otra parte en su nombre) hará una evaluación de su naturaleza y conducta antes de firmar el acuerdo.<sup>10</sup>

## 02

Si un proveedor no sigue las directivas de ciberseguridad de la organización, se debe valorar la situación y, en caso necesario, rescindir el acuerdo.

## 03

Si durante la vigencia de un acuerdo surge una sospecha de que un proveedor crítico está exponiendo a la organización a graves riesgos cibernéticos, la organización debería considerar rescindir el acuerdo de inmediato.

## Finalizar un acuerdo con un proveedor

La organización debe verificar que se estén cumpliendo las disposiciones definidas en el acuerdo con el proveedor. Es particularmente importante asegurarse de que el proveedor cumpla con todas las disposiciones relacionadas con la eliminación de los datos de la organización almacenados en el sitio del proveedor al concluir el acuerdo entre las partes. Entre otras cosas, se verificarán los siguientes elementos:

## 01

Comprobar que se hayan devuelto todos los registros, soportes físicos, equipos y componentes propiedad de la organización que se utilizaron para los fines del trabajo del proveedor, incluidos los artículos en poder de todos los empleados y subcontractistas del proveedor.

## 02

Solicitar al proveedor que firme una declaración de compromiso de no retener en su poder ningún componente relacionado con un sistema o información acerca de la organización, y que no hará ningún uso de la información sobre la organización a la que tuvo acceso durante el acuerdo.

# 03

Verificar que los soportes magnéticos de cualquier equipo utilizados por el proveedor durante su acuerdo con la organización hayan sido destruidos (por ejemplo, si las computadoras del proveedor se usaron para procesar o almacenar información sobre la organización). Asimismo, la organización corroborará que se hayan eliminado las copias de archivos e información sobre la organización de los sistemas de información del proveedor y el equipo de TI una vez que ya no haya ninguna necesidad de mantenerlas.

# 04

Comprobar que el proveedor ya no tenga autorizaciones de acceso, medios de identificación o acceso físico o electrónico a la información de la organización.

# 05

Asegurarse de que se haya definido una directiva sobre lo que está permitido y lo que está prohibido en relación con la divulgación a terceros de detalles del proyecto o acuerdo.

8. Control 16.4 de la *Metodología de Ciberdefensa para Organizaciones*.

9. Control 16.5 de la *Metodología de Ciberdefensa para Organizaciones*.

10. Control 16.3 de la *Metodología de Ciberdefensa para Organizaciones*.

## Anexo 2.

### Cuestionario para proveedores

El cuestionario para proveedores constituye el elemento fundamental que se requiere de los proveedores en relación con los acuerdos. Este cuestionario refleja el umbral profesional mínimo, dependiendo del tipo de acuerdo (como almacenamiento de información en una nube, desarrollo, acceso remoto, etc.) y del grado de confidencialidad del acuerdo (proveedor crítico o no crítico). El cuestionario aborda la

gestión de riesgos, crea transparencia y uniformidad en la economía con respecto a los controles de ciberdefensa e infunde confianza acerca de la respuesta de ciberdefensa de la organización, su nivel de controles y de protección.

El cuestionario incluye varios requisitos de ciberdefensa, de acuerdo con la estructura que figura en el gráfico A2.1.

**Puede encontrarse el modelo de cuestionario completo siguiendo este enlace:**  
<http://www.iadb.org/document.cfm?id=EZHARE-37811622-6>.



Gráfico A2.1. Requisitos de ciberdefensa incluidos en el cuestionario



## 01

**Tipo de acuerdo:** hay diversos tipos de acuerdos, como servicios basados en la nube, desarrollo de *software*, etc.

## 02

**Carácter crítico:** definir si el requisito específico de ciberdefensa se espera de cualquier tipo de proveedor o solo de los proveedores críticos. La respuesta a esta pregunta es sí o no, donde “sí” significa que se espera que el requisito sea implementado solo por proveedores críticos.

## 03

**Código de tema:** número asignado a las diversas cuestiones en materia de requisitos.

## 04

**Tema:** descripción del tema general y sus requisitos de ciberdefensa (como protección perimetral, copias de seguridad y recuperaciones, protección de estaciones de trabajo terminales, etc.).

## 05

**Código de control:** número de código asignado a los diversos requisitos de control.

## 06

**Control:** descripción del requisito específico que se espera que el proveedor implemente.

## 07

**Énfasis en la implementación del control:** enfoque general que ayuda a coordinar las expectativas entre el proveedor y la organización, y explicar por medio de ejemplos y un énfasis adicional cuáles son las expectativas en relación con el nivel de ciberdefensa.

## 08

**Alcance de la implementación de un control:** detalles sobre las diversas formas de implementar el control, con una respuesta que va desde “no está implementado” hasta “implementado de manera total y eficaz” (y todo el abanico entre ambas opciones). El propósito de esta columna es coordinar las expectativas con respecto al alcance de la implementación real del control o requisito por parte del proveedor. Por ejemplo, no se espera que el

proveedor responda a la pregunta “¿Tiene registros?”/“¿Realiza copias de seguridad?” con un sí o un no, sino que se le da la oportunidad de explicar en qué medida se implementa el control en relación con la organización.

## 09

**Prueba requerida:** una explicación de cómo la organización debe demostrar que los requisitos definidos se están implementando realmente. Dicha prueba debe hacerse llegar a la organización de acuerdo con lo acordado entre las partes.

## 10

**Énfasis en la inspección externa:** énfasis en un organismo de inspección que verificará el cumplimiento antes de emitir una “calificación” para el grado de asimilación de los requisitos de control de ciberdefensa. Esta columna es obligatoria para las inspecciones de inspectores certificados.

## 11

**Umbral:** definición del grado mínimo de asimilación requerido para cada control, diferenciando entre un proveedor crítico o no crítico. Por ejemplo, las copias de seguridad, la extensión mínima del control requerido por un proveedor

no crítico podría ser 1, mientras que para un proveedor crítico el mínimo requerido podría ser 3. Cualquier proveedor que no alcance el umbral de implementación del control no cumple con las expectativas de la organización en relación con esa cuestión específica.

## 12

**Compatibilidad con normas:** normas y reglamentos que se aplican al proveedor.



## Anexo 3.

### Módulo de la cadena de suministro

Los objetivos organizacionales y el sistema de controles conforman una plataforma nacional que consta de varios módulos. Uno de ellos es un módulo de la cadena de suministro que se desarrolló con el fin de proporcionar una respuesta a varios desafíos relacionados con la gestión de los riesgos cibernéticos en la cadena de suministro que surgieron durante la iniciativa. Los diversos desafíos encontrados son los siguientes:

# 01

**Escasez de recursos para respaldar la etapa de difusión del cuestionario a un gran número de proveedores:** actualmente las organizaciones deben enviar sus cuestionarios a todos los proveedores, en general por correo electrónico. Este proceso requiere que las organizaciones mantengan una lista actualizada de las personas de contacto de sus diversos proveedores, verifiquen la recepción del cuestionario y los requisitos de ciberdefensa por parte de sus proveedores, gestionen versiones del cuestionario e informen a los proveedores en caso de revisión del cuestionario, etc. Una vez que se digitalice el cuestionario, cada organización podrá remitir a sus proveedores al sistema donde encontrarán la última versión.

# 02

**Escasez de recursos para contar con personal de apoyo que responda a las preguntas de los proveedores sobre cómo rellenarlo:** al utilizar el sistema los proveedores podrán obtener respuestas completas a sus preguntas sobre los requisitos de ciberdefensa, los documentos asociados y las herramientas, todo en una sola plataforma.

# 03

**Falta de uniformidad en la estructura de los productos del proceso de revisión:** con el fin de brindar apoyo a los procesos de control y auditoría de los inspectores y organismos de certificación, el sistema guía a la persona que completa el cuestionario a través de un proceso estructurado hasta que se elabora un informe final al terminar del proceso. Este informe puede constituir un formulario de autodeclaración si el proceso se lleva a cabo sin la intervención de un inspector certificado y también puede conformar la base que el inspector aporta al organismo de certificación si un proveedor desea solicitar la certificación.

# 04

**Dificultades de los proveedores para gestionar las conclusiones que surgen durante la revisión:** trabajar con varias aplicaciones y correspondencia dificulta el proceso de subsanar las deficiencias y presentar la situación actualizada a los clientes. El sistema permi-

te a los proveedores obtener su informe de situación en forma de gráficos fácilmente exportables y profundizar en un tema en particular, actualizar el nivel de defensa y producir un informe actualizado en consecuencia.

# 05

**Mantener el principio de irrefutabilidad:** en la actualidad, el proceso de responder a los requisitos de ciberdefensa a menudo se lleva a cabo utilizando diversas aplicaciones, como correspondencia por correo electrónico, Excel, etc. Trabajar con un sistema estructurado ayuda al destinatario del informe a conocer quién respondió al informe y cuándo se elaboró, y a saber que el informe no se envió como un archivo abierto (por ejemplo un Excel, ya que es no es fácil determinar si los valores fueron alterados, cuándo, por quién, cuál era el valor original, dónde está la última versión, etc.).

**El módulo de la cadena de suministro ayuda a:**

# 01

Hacer que el cuestionario para proveedores sobre el nivel de ciberdefensa en la economía esté accesible en línea en el sitio web de la Dirección: <https://grc.cyber.gov.il>.<sup>11</sup>

11. Nota de los editores: Al momento de la publicación, el cuestionario para proveedores en línea se encuentra disponible solo en idioma hebreo.

# 02

Constituir una plataforma para que los proveedores produzcan informes a fin de declarar su nivel de cumplimiento con los requisitos de ciberdefensa de esta Metodología para la Protección de la Cadena de Suministro, así como su capacidad de gestionar las deficiencias que surgen para los proveedores durante el proceso de corrección. Además, los proveedores pueden actualizar sus datos en el sistema en cualquier momento, con lo que se genera una nueva clasificación para el producto o servicio.

# 03

Facilitar una lista de proveedores que han completado el proceso de certificación de conformidad con la metodología nacional a este respecto (proveedores e inspectores certificados). Todas las organizaciones de la economía podrán realizar una búsqueda en el sistema y recibir un desglose adecuado de proveedores que cumplan con el umbral de riesgo definido por la organización. Con base en esta información, las organizaciones pueden elegir el proveedor más adecuado y firmar un acuerdo con él para garantizar su adhesión al nivel de riesgo definido.

# 04

Hacer accesible el soporte técnico y metodológico a través del sitio web del centro de soporte de la Dirección y llamando al 119.

## Anexo 4.

### Modelo de Regulación

**Gráfico A4.1.** Participantes en el proceso de regulación



#### Organismo de acreditación

El modelo de regulación y certificación adoptado por la Dirección Nacional de Ciberseguridad, tras analizar modelos en Israel y a escala internacional, coloca a esta Dirección como principal organismo de acreditación. En consecuencia, es responsable de establecer y mantener estándares profesionales apropiados. Por este motivo, servi-

rará como organismo de acreditación con la función de garantizar que los organismos de certificación estén tomando medidas para capacitar a los inspectores y certificar a los proveedores en relación con los requisitos. La Dirección también actuará como organismo de supervisión y control, para asegurarse ocasionalmente de que sus requisitos estén siendo cumplidos. Las regulaciones cambiarán periódicamente.

#### Organismos de certificación

Estos organismos actualmente operan de conformidad con las normas internacionales aceptadas, realizan revisiones, capacitación y certificación utilizando las diversas normas de gestión de la Organización Internacional de Normalización (ISO, por sus siglas en inglés). En estas circunstancias, se requerirá que los organismos de certificación cumplan con los requisitos particulares del organismo de acreditación y posteriormente recibirán autorización expresa para operar en nombre del organismo de acreditación dentro del ámbito solicitado; en este caso, por ejemplo, en la cadena de suministro.

#### Organismos de inspección

Se trata de organismos que realizan inspecciones en nombre del organismo de certificación. Un organismo de inspección puede ser toda una organización o una parte de ella, como un profesional específico en una organización. En el presente caso, se refiere a un inspector de la compatibilidad de las medidas de ciberdefensa de un proveedor en la cadena de suministro de una organización, que verifica el cumplimiento de las condiciones definidas por la Dirección, las cuales se especificarán más adelante (en adelante, "el inspector").

#### Proveedores

Los proveedores que así lo desean completan el proceso de certificación y reciben la

certificación de que cumplen con los requisitos y procesos dentro del ámbito de su solicitud de certificación, de acuerdo con los requisitos definidos por la Dirección.

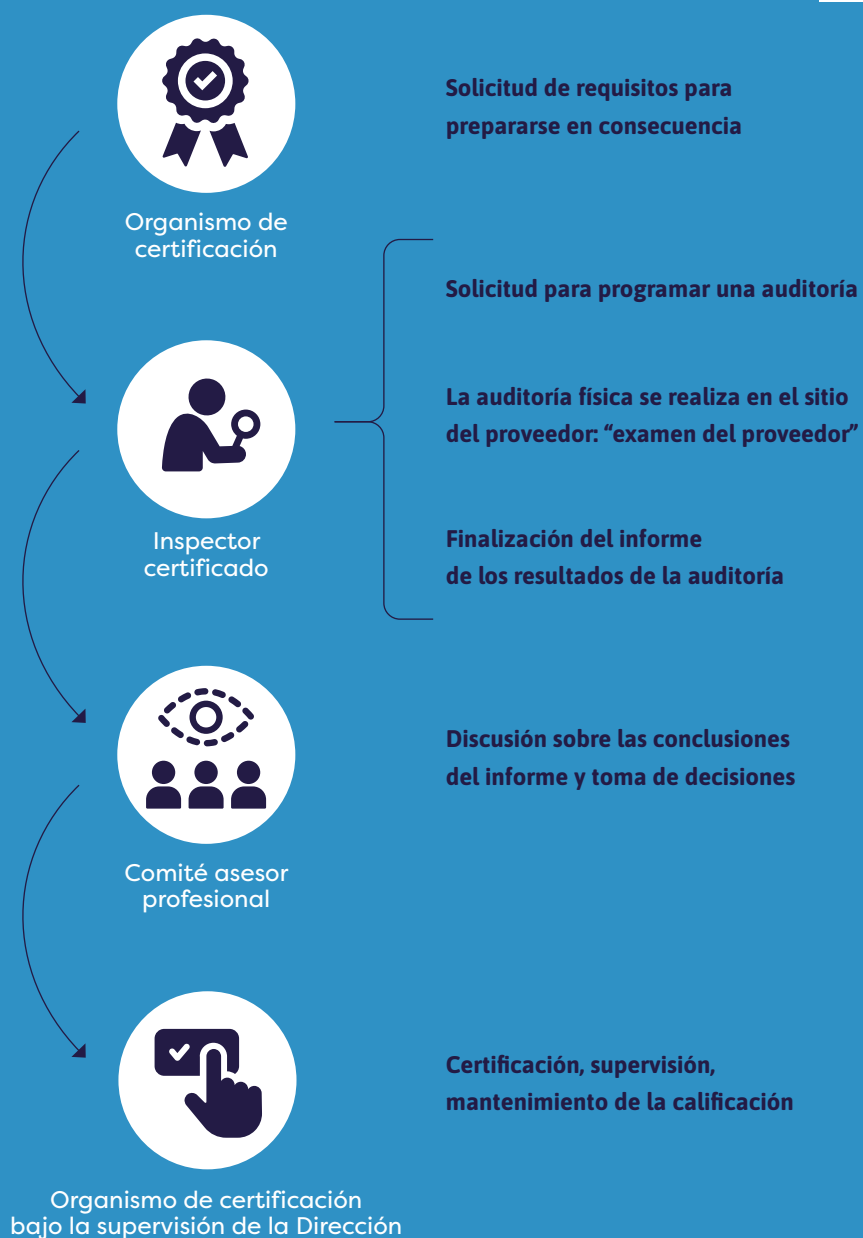
#### Niveles de regulación

La inspección de la compatibilidad de la ciberdefensa en una cadena de suministro organizacional pasa por una regulación que tiene un alcance relativamente estrecho y está en relación directa con los proveedores que actúan en la cadena de suministro de las organizaciones de la economía.

Esta regulación fue formulada dada la percepción de que los proveedores sufren numerosos incidentes cibernéticos que pueden afectar a los consumidores de los servicios que prestan (entre ellos importantes organizaciones industriales, bancos, etc.), principalmente debido a que las capacidades de ciberdefensa de los proveedores no son iguales a las de las organizaciones que contratan sus servicios.

Teniendo en cuenta las ventajas descritas en la introducción de esta publicación, la Dirección espera que las organizaciones instruyan a sus diversos proveedores para que participen en el proceso, que incluye recibir una respuesta del proveedor, o inspector en su nombre, al cuestionario para proveedores de acuerdo con uno de los tres niveles de regulación y nivel de riesgo que el proveedor plantea a una organización.



**Gráfico A4.2.** Competencias y etapas en el proceso de certificación

Antes de explicar los niveles de regulación, conviene aclarar que el nivel más alto de regulación (A) se asigna a los proveedores críticos. Puede verse una definición del nivel A en un documento elaborado por la Dirección titulado *Doctrina de defensa: la cadena de suministro*.

**Proveedor crítico:** es un proveedor que brinda servicios tales como soporte o mantenimiento de sistemas de información, almacenamiento de información confidencial fuera de las instalaciones de la organización, servicios de externalización tecnológica, etc. (Prácticas bancarias adecuadas 363 - Gestión de riesgos cibernéticos en la cadena de suministro, cláusula 7), o aquel proveedor cuyo daño pueda causar perjuicios importantes al cliente. La decisión de definir a un proveedor como crítico queda a discreción de la organización, con una excepción: cuando una autoridad reguladora haya definido de antemano para las organizaciones de la economía sobre las que es responsable que un proveedor en particular, o cualquier proveedor que cumpla con los criterios definidos, constituye un proveedor crítico en cualquier caso.

A continuación se muestran los niveles de regulación desde el nivel más bajo (C) hasta el más alto (A) (véase el gráfico A4.3):

01

**Nivel de autoevaluación C:** el proveedor o cualquier parte que actúe en su nombre completa un cuestionario de autoevaluación y luego firma una declaración. El informe obtenido se puede exportar a organizaciones con las cuales el proveedor desea contratar, para que puedan recibir una indicación del cumplimiento del proveedor en relación con los estándares de control pertinentes.

02

**Nivel de autoevaluación B:** completar un cuestionario y presentar pruebas de aplicación del control. También en este caso el proveedor obtiene un informe que puede exportarse, junto con las pruebas requeridas para corroborar su cumplimiento en relación con los controles pertinentes.

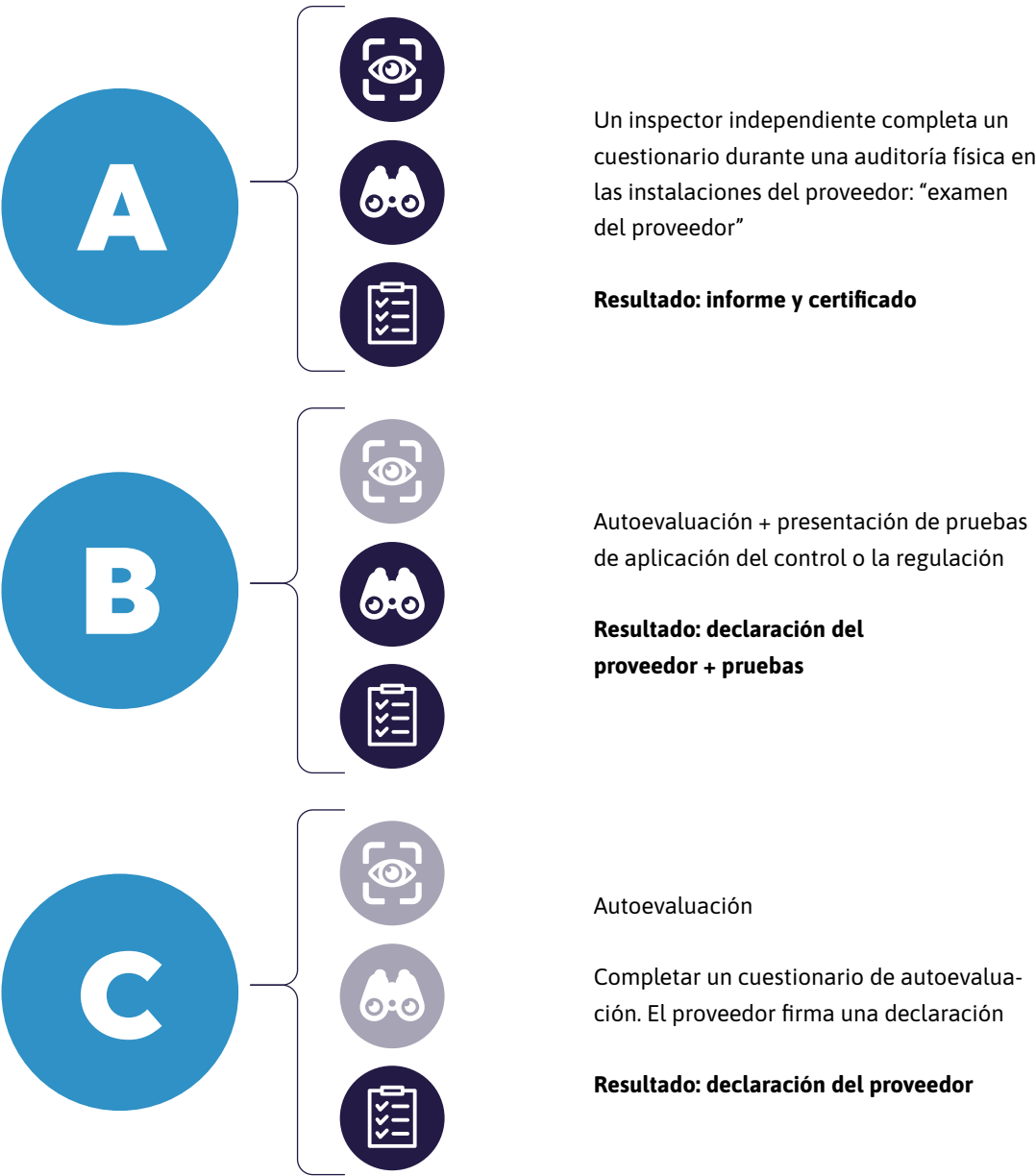


# 03

**Nivel A:** destinado a proveedores definidos como críticos para una organización. Este nivel de regulación incluye las dos etapas anteriores, que se llevan a cabo durante una auditoría física realizada por un inspector en las instalaciones del proveedor. Este proceso se denomina “revisión del proveedor” y constituye un control adecuado por parte de un profesional externo objetivo que examina personalmente el cumplimiento de dichos requisitos por parte del proveedor.

Al finalizar esta etapa, el inspector presentará un informe al comité de certificación con las conclusiones obtenidas durante la inspección realizada al proveedor, como se especifica a continuación, y si el informe indica el cumplimiento, se emitirá un certificado adecuado al proveedor y este será incluido en el sitio web de la Dirección y en el del organismo de certificación como “proveedor certificado” (previo consentimiento del proveedor) o, alternatively, se emitirá un informe acerca de las deficiencias que se hará llegar al proveedor. La corrección de esas deficiencias es una precondition para recibir la certificación solicitada.

Gráfico A4.3. Niveles de regulación



## Gestión de los requisitos de los organismos profesionales en el modelo de regulación

La Dirección Nacional de Ciberseguridad gestionará el proceso de regulación controlada y supervisará los procesos que ha establecido con el objetivo de mantener un nivel de ciberdefensa muy elevado.

**Organismos de certificación:** las actividades de capacitación y certificación definidas por los organismos de certificación requieren el cumplimiento de los criterios definidos por la Dirección a este respecto:

# 01

Los organismos de formación:

- Demostrarán un compromiso activo y continuo en la gestión de un centro de capacitación, incluidos todo su personal, edificios, instrumentación, laboratorio de computación, desarrollo y gestión de la plataforma y el proceso de capacitación y cualquier otro elemento con el que cuenten con el propósito de la gestión actual.
- Evidenciarán un compromiso centrado en la capacitación tecnológica.

- Se considerarán en ventaja si cuentan con más de cinco años de experiencia en la capacitación en temas de ciberdefensa.

## 02

Los organismos de certificación mantendrán las siguientes certificaciones y capacidades:

- Certificación válida con respecto a la norma ISO 17021: Requisitos para organismos de certificación.
- Certificación válida respecto de la norma ISO 27001: Gestión de seguridad de la información.
- Compromiso comprobado en materia de normalización de más de cinco años.

## 03

Los inspectores mantendrán las siguientes certificaciones y capacidades:

- Experiencia acumulada de al menos cinco años en ciberdefensa en empresas comerciales.
- Certificado de finalización del curso en seguridad de datos o ciberdefensa de al menos 250 horas o certificación internacional reconocida, tales como Certified

Information Systems Security Professional (CISSP), Certified Chief Information Security Officer (CCISO), Certified Information Systems Auditor (CISA) o Certified Information Security Manager (CISM).

- Familiaridad con tecnologías y productos de ciberdefensa y con topologías de red seguras.
- Conocimientos y experiencia en análisis y gestión de riesgos.
- Habilidades de comunicación escrita y oral.
- Habilidades de presentación significativas, que incluirá el manejo de objeciones.
- Hebreo como lengua materna y dominio del inglés.
- Aceptación por un comité de admisiones.
- Aprendizaje independiente previo al curso.
- Se considerará una ventaja contar con una experiencia práctica en ciberdefensa de más de tres años en una organización empresarial establecida.



## Gestión de las funciones de los profesionales en el modelo de regulación

### Funciones de los organismos de capacitación

# 01

Se requerirá que los organismos de capacitación que cumplan con los requisitos antes mencionados y que respondan al llamado público que anuncie la Dirección Nacional de Ciberseguridad brinden un conjunto de servicios de capacitación y constituyan un organismo examinador de acuerdo con los requisitos profesionales de la Dirección, la cual emite un certificado de finalización dirigido a los participantes para la función para la que recibieron capacitación y para mantener sus calificaciones, mediante seminarios, etcétera.

# 02

Los representantes de la Dirección Nacional de Ciberseguridad serán participantes activos en los cursos de capacitación para ofrecer información sobre el proceso, mejorar la metodología, enriquecer el programa y el contenido proporcionado por la Dirección, evaluar a los profesores, personalizar las tareas de los cursos encargadas a los participantes, actuar como asesores de los procesos y operaciones

de los organismos de capacitación, y proporcionar respuestas inmediatas relacionadas con la nueva metodología. Luego entregarán a los profesionales pertinentes de la Dirección una lista de recomendaciones sobre adiciones, enmiendas, revisiones y mejoras, y analizarán y establecerán relaciones entre el material que se enseña y el comienzo real del trabajo, como un inspector de la compatibilidad de una cadena de suministro organizacional.

# 03

Los siguientes son algunos de los requisitos de la Dirección con respecto a las funciones de un cuerpo de capacitación:

- Difundir y publicitar los cursos de capacitación, seminarios web, fechas de reuniones del comité de admisiones y todas las publicaciones relacionadas.
- Seleccionar candidatos de acuerdo con los requisitos relativos a los umbrales definidos por la Dirección.
- Realizar exámenes de ingreso y reuniones del comité de admisiones.
- Capacitar instructores profesionales de acuerdo con los requisitos de la Dirección y elaborar cursos en consonancia con las especificaciones y metodología de la Dirección para la regulación requerida.
- Realizar cursos de formación y exámenes intermedios y finales (exámenes y simulaciones teóricas y prácticas de laboratorio).
- Cobrar pagos por cursos de capacitación o exámenes.
- Proporcionar instalaciones para los cursos de capacitación (incluido un laboratorio de computación) y el examen de certificación (definición de una ubicación física específica para realizar los exámenes).
- Preparar exámenes (administrar un equipo de preparadores de exámenes), programar los exámenes, administrarlos, asignar supervisores para los exámenes, gestionar las solicitudes de revisión y los casos excepcionales, y ocuparse de una base de datos de preguntas actualizada.
- Elaborar informes periódicos.
- Emitir certificados de calificación (sujeta a la aprobación del comité de aprobación de la Dirección).
- Realizar una revisión periódica de las actividades de los graduados.
- Mantener la cualificación de los graduados, en particular mediante los cursos de actualización requeridos.

### Funciones de los inspectores

# 01

Los candidatos que cumplan con los criterios de admisión, completen con éxito el curso de capacitación requerido y aprueben el examen final recibirán un certificado del organismo de capacitación y la Dirección Nacional de Ciberseguridad, sujeto a la aprobación del comité de aprobación de la Dirección. Ese certificado debe especificar la versión del cuestionario para proveedores para el fortalecimiento de la cadena de suministro de la que trató la capacitación.

# 02

Los datos del inspector se publicarán en el sitio web de la Dirección, previo consentimiento por escrito por parte del inspector. En el sitio web figurará como inspector que cumple con los requisitos de la Dirección para la inspección de la compatibilidad de la ciberdefensa para una cadena de suministro de la organización.

## 03

Los inspectores deben mantener sus cualificaciones para dicha función participando en seminarios y cursos de educación continua, ya que la metodología que se enseña en los cursos de capacitación (la versión del cuestionario) se actualiza periódicamente. Esto resulta esencial para desempeñar esa función y será una condición para que los datos del inspector sigan publicándose en el sitio web de la Dirección.

## 04

La organización de dichos seminarios es responsabilidad de los organismos de capacitación de acuerdo con los requisitos y directivas de la Dirección con respecto al contenido profesional que se impartirá en ellos.

## 05

La función de un inspector es analizar la presencia de elementos críticos en las instalaciones del proveedor que entró en contacto con él y desea recibir el reconocimiento de la Dirección como proveedor crítico en el nivel A dentro de un ámbito particular.

## 06

El análisis de la presencia de elementos críticos supone: realizar consultas e investigaciones, efectuar evaluaciones independientes de los sistemas del proveedor, recibir pruebas que deban ser examinadas durante la auditoría, llevar a cabo exámenes en los diversos departamentos, mantener conversaciones con empleados profesionales sobre los controles pertinentes, examinar las medidas de seguridad en la sala de servidores, inspeccionar las medidas de seguridad física, revisar las reglas de los cortafuegos, realizar consultas sobre los controles de acceso, examinar las políticas y procedimientos, las autorizaciones del Directorio Ejecutivo y la Dirección, etcétera.

## 07

Hay seis posibles temas de inspección en el cuestionario para proveedores:

- General, que incluye todos los controles del cuestionario para proveedores.
- Manejo de la información.
- Acceso remoto.
- Trabajo realizado en las instalaciones de un cliente.

- Desarrollo de software seguro.
- Almacenamiento de información en la nube.

## 08

El cliente que requiere el trabajo del inspector definirá el tema de la auditoría en las instalaciones del proveedor que lo solicita.

## 09

Entre las materias enseñadas en el curso de capacitación que los inspectores deben aprobar antes de comenzar a trabajar, se incluyen los detalles de la auditoría de cada control, el alcance de su implementación en los sistemas del proveedor, las pruebas que deben adjuntarse para corroborar el cumplimiento del proveedor en relación con el control en cuestión, el trabajo del inspector en el sistema en línea de la Dirección, los objetivos de la organización y el sistema de controles (el módulo de la cadena de suministro), el modo de completar el informe sobre las conclusiones, el manejo de las objeciones, los aspectos legales, el mundo de la auditoría, etcétera.

## 10

El inspector elaborará un informe con los resultados obtenidos durante la inspección del proveedor y adjuntará en cada caso las pruebas requeridas.

## 11

El inspector introducirá todos los detalles sobre cada control en el campo apropiado y para cada caso que indique como “irrelevante” se le requerirá la máxima cantidad de detalles que satisfagan al comité de certificación de que el control específico es realmente irrelevante para el proveedor o sector de actividad inspeccionado.

## 12

El modo de presentación del expediente de un proveedor al comité de certificación se especifica más adelante en el apartado sobre Funciones de los organismos de certificación.



# 13

Los inspectores no pueden tener conflictos de intereses y han de presentar informes confiables. Al enviar los archivos del proveedor al comité de certificación, los inspectores deben incluir las declaraciones de cumplimiento de lo mencionado anteriormente en relación con cada proveedor inspeccionado.

# 14

Los inspectores regularán sus acuerdos con los proveedores que contrataron sus servicios de inspección por medio de un documento legal que garantice la confidencialidad de los aspectos a los que están expuestos durante las inspecciones.

# 15

La Dirección recomienda que todos los inspectores se protejan durante el plazo de sus acuerdos con los proveedores mediante la adquisición de un seguro de responsabilidad profesional con la cobertura adecuada para la prestación de servicios de este tipo.

## Funciones de los organismos de certificación

# 01

Los organismos de certificación que cumplan con los requisitos antes mencionados y que respondan al llamado público de la Dirección deberán proporcionar servicios de certificación de extremo a extremo: desde la

etapa de contratación de funciones de certificación adecuadas que abarquen todos los requisitos profesionales de la Dirección hasta la emisión de la certificación a los proveedores aprobados, la supervisión detallada de los proveedores, la verificación de la confiabilidad de los datos y el aseguramiento de que los proveedores continúen cumpliendo los requisitos para la certificación.

# 02

El gerente de certificación tendrá las siguientes funciones y características:

- Será responsable de examinar los archivos de los proveedores, entre ellos, un informe de las conclusiones del inspector y las pruebas requeridas, y de determinar si cumplen con los estándares establecidos en las especificaciones o metodología de la Dirección en cuanto organismo profesional.
- Será contratado por el organismo de certificación y no dará a entender en ningún momento que es empleado/a de la Dirección.

- Será un profesional individual que posea certificados y pruebas fidedignas de su conocimiento, experiencia y cualificaciones de acuerdo con los siguientes requisitos:

1. Una formación tecnológica evidente, con un título en ingeniería de software o informática.
2. Certificación internacional (CCISO/CISSP).
3. Una cualificación tecnológica evidente y una experiencia práctica en ciberdefensa reflejadas por la antigüedad profesional y una experiencia de más de cinco años.
4. Familiaridad con herramientas y productos tecnológicos.
5. Familiaridad con los aspectos de la auditoría del ámbito cibernético.
6. Experiencia en certificación y amplia familiaridad con la acreditación internacional y las actividades vinculadas.

- El porcentaje de nombramientos de gerentes de certificación será definido por el organismo de certificación, siempre que este no comprometa la duración del examen y que la fecha del examen no exceda los 14 días hábiles desde la presentación de una solicitud para certificar a un proveedor.





## 03

También puede convocarse a un experto en contenido:

- En los casos en que el proveedor que se somete a la certificación se dedique a ámbitos de negocios particularmente técnicos, como un proveedor de equipos e instrumentos de tecnología financiera o un proveedor especializado para entidades de defensa, etc., y que se necesite la participación de un experto en contenido específico para examinar el informe de las conclusiones y pruebas presentadas, se añadirá un experto en contenido al comité de certificación de acuerdo con la recomendación de la Dirección o, alternativamente, un experto propuesto por el organismo de certificación, siempre que el experto sea aceptable para la Dirección Nacional de Ciberseguridad.
- El experto en contenido, que será invitado a asesorar al oficial de certificación, será seleccionado de acuerdo con una lista de categorías de servicios y expertos en contenido específicos que la Dirección deberá presentar al organismo de certificación, y que se actualizará periódicamente.

- El plazo para la toma de decisiones con respecto al proveedor pertinente, en caso de que también se requiera un experto en contenido, es de 21 días hábiles a partir de la fecha de presentación de la solicitud de certificación del proveedor. El plazo para emitir un certificado a un proveedor es de un máximo de siete días hábiles tras la toma de la decisión con respecto al proveedor.
- En relación con la toma de decisiones deben considerarse los siguientes aspectos:
  1. En caso de acuerdo entre el Gerente de certificación y el experto en contenido, el juicio del representante de la Dirección será opcional.
  2. En caso de desacuerdo entre el oficial de certificación y el experto en contenido, la decisión con respecto a la certificación del proveedor recaerá en el representante de la Dirección.
  3. Para disipar cualquier duda, el representante de la Dirección tendrá un derecho de veto y su decisión será definitiva en relación con la certificación del proveedor.



## 04

Para la presentación del expediente de un proveedor para certificación debe considerarse lo siguiente:

- Criterios de presentación: un inspector certificado que realiza una inspección con el permiso del proveedor y llega a la conclusión de que el proveedor cumple completamente con los controles requeridos de acuerdo con el alcance deseado de la inspección del proveedor, debe presentar el expediente del proveedor al organismo de certificación.
- El expediente de certificación del proveedor debe contener los siguientes documentos:
  1. Un formulario de consentimiento firmado por el proveedor, por el cual acepta someterse a una inspección por parte del inspector certificado, afirma que el expediente del proveedor se presenta con su consentimiento, y consiente en ser incluido en la base de datos de proveedores certificados, si cumple con los requisitos de la declaración del inspector sobre la confiabilidad de la información indicada en el informe de hallazgos, y sobre la ausencia de conflictos de intereses entre el inspector y el proveedor que es sujeto del expediente presentado.

2. El informe de las conclusiones acerca del proveedor, completado por el inspector certificado en el Sistema de Controles y Metas Organizacionales en formato PDF, que debe ser firmado (a mano o digitalmente) por un representante autorizado del proveedor.
3. Portada que enumere la evidencia requerida para probar el cumplimiento de los controles.
4. Cuadro informativo sobre el alcance de la inspección realizada al proveedor que es sujeto del informe, el cual incluirá las horas mínimas requeridas para el alcance de cada inspección.
5. Confirmación del pago del costo de la inspección y certificación del proveedor, de acuerdo con las tasas del organismo de certificación.

## 05

El expediente puede presentarse como copia impresa al organismo de certificación o en un medio físico o, alternativamente, por correo electrónico a una bandeja de entrada designada del organismo de certificación en un archivo PDF que contenga el expediente completo del proveedor.

# 06

Los proveedores que no deseen enviar el expediente completo de las pruebas al comité de certificación tienen una alternativa, por la cual el examen por parte del comité de certificación del cumplimiento del proveedor del alcance de inspección deseado se llevará a cabo en las instalaciones del proveedor o en su dirección de servicio.

- El proveedor es responsable de presentar al comité todas las pruebas requeridas que se presentaron al inspector y sirvieron para convencerlo, de acuerdo con el informe de conclusiones presentado al comité.
- La visita del gerente de certificación y, si fuera necesario, del experto en contenido a las instalaciones del proveedor para obtener una impresión independiente de las pruebas especificadas en el informe de conclusiones, en virtud de las cuales el inspector llegó a sus conclusiones, implica un costo adicional resultante de los gastos de viaje y otros gastos de acuerdo con las tarifas que publicará el organismo de certificación.

# 07

En la medida en que sea necesario presentar pruebas adicionales o explicaciones

detalladas, se invitará al inspector a una reunión presencial o telefónica con el organismo de certificación y se le pedirá que ofrezca respuestas adecuadas al gerente de certificación o al experto en contenido hasta que estén convencidos de que el proveedor cumple los requisitos para ser certificado como proveedor aprobado o, en caso contrario, sobre el rechazo inmediato de la solicitud del proveedor.

# 08

Si el examen del gerente de certificación revela deficiencias excesivas relacionadas con la clasificación del proveedor como proveedor crítico, la implementación de un control que no sea proporcional al nivel de seguridad requerido en razón de la esfera de negocios del proveedor, la elaboración de un informe insatisfactorio como consecuencia de la ausencia de medios tecnológicos requeridos para ese proveedor o debido a una preocupación sobre la confiabilidad, etc., el expediente del proveedor se devolverá al inspector, sin certificación y con la especificación de las deficiencias que requieren rectificación, con un plazo para volver a presentarlo que no exceda los 90 días. El nuevo examen del expediente de un proveedor implica un pago adicional con una tarifa reducida, de acuerdo con el arancel que publicará el organismo de certificación.

## Certificados

# 01

La aprobación por parte del gerente de certificación del informe de resultados presentado por el inspector de acuerdo con las pruebas requeridas presentadas equivale a la aprobación de la certificación del proveedor para el alcance indicado en la solicitud.

# 02

La certificación del proveedor como proveedor certificado estará vigente durante dos años a partir de la fecha de su aprobación por parte del gerente de certificación. Al final del primer año de la certificación del proveedor, se requiere que el proveedor o cualquier delegado en su nombre presente una declaración firmada por un representante autorizado de que no se han producido cambios críticos en el alcance del examen que dio lugar a su certificación y que se compromete a notificar cualquier cambio para que la certificación emitida permanezca vigente por un año adicional y su nombre siga constanding en la base de datos de proveedores aprobados.

# 03

Los certificados serán emitidos a los proveedores por el organismo de certificación, con sujeción a la aprobación de sus contenidos por la Dirección y de acuerdo con la cláusula de patrocinio en las regulaciones acordadas.

## Resumen del acuerdo de nivel de servicio sobre los aspectos de la certificación

# 01

El porcentaje de nombramientos de gerentes de certificación será definido por el organismo de certificación, siempre que este no comprometa la duración del examen y que la fecha del examen no exceda los 14 días hábiles desde la presentación de una solicitud para certificar a un proveedor.

# 02

El plazo requerido para la toma de decisiones con respecto al proveedor pertinente es de 21 días hábiles a partir de la fecha de presentación de la solicitud de certificación del proveedor; en caso de que también se requiera la opinión de un experto en contenido, deberán transcurrir 28 días hábiles a partir de la presentación de la solicitud de certificación.

# 03

El período para la rectificación de las deficiencias de un proveedor no excederá los 90 días naturales desde la fecha de la notificación al proveedor y hasta la nueva presentación de su solicitud.

# 04

El plazo requerido para entregar un certificado a un proveedor desde la fecha de la decisión sobre su expediente será de un máximo de siete días hábiles.

# 05

El recurso de un proveedor con respecto al rechazo de su solicitud o al rechazo parcial se discutirá con un representante de la Dirección dentro de los 14 días hábiles de la fecha de presentación del recurso del proveedor.

## Tasas de certificación (resumen)

# 01

La tasa de certificación será fijada por el organismo de certificación y deberá ser aprobada por la Dirección con el fin de proporcionar un servicio completo y profesional, por un lado, y mantener un costo razonable y proporcionado que no imponga una carga sobre la economía, por otro lado.

# 02

La tasa de certificación básica consistirá en una tarifa de examen por parte del gerente

de certificación, calculada en función del alcance del examen realizado para el proveedor, y un costo separado para emitir y entregar el certificado al proveedor.

# 03

Una tarifa separada para el examen del expediente del proveedor por un experto en contenido, si fuera necesario.

# 04

Una tarifa reducida para volver a examinar o realizar un examen adicional después de que el proveedor presente nuevamente su expediente tras rectificar las deficiencias identificadas como resultado de la inspección original.

# 05

Se prevé una tasa para una inspección física con el permiso del proveedor, para los proveedores que no permitan que se saquen las pruebas de sus instalaciones y soliciten al gerente de certificación que visite las instalaciones del proveedor.

## Anexo 5. Modelo de acuerdo<sup>12</sup>

El proveedor cumplirá con las disposiciones de las reglamentaciones, leyes y normas vigentes para su sector de actividad durante todo el término del contrato.

El proveedor se compromete a cumplir con los requisitos en materia de cadena de suministro establecidos por la Dirección Nacional de Ciberseguridad en el cuestionario para proveedores (anexo 2). El alcance de la inspección y el modo de probar el cumplimiento de estos requisitos serán acordes a la definición de la organización (uno de los tres niveles especificados previamente en esta publicación: A, B o C).

El proveedor designará a una persona de contacto que actuará como enlace de ciberdefensa en relación a las actividades pertinentes de la organización, cuya identidad, datos y detalles de contacto deberán ser aprobados por la organización.

Todos los costos relacionados con la seguridad de la información de los sistemas, soluciones de seguridad de la información y bases de datos se aplicarán únicamente al proveedor.



El proveedor informará por escrito sobre las operaciones destinadas a satisfacer diversas necesidades pero que constituyen una vulnerabilidad en materia de seguridad de la conexión, como el nombre de usuario y la contraseña de la puerta trasera utilizada para abrir una cuenta bloqueada de la organización en caso de olvido de la contraseña. Si no existen operaciones de este tipo, el proveedor presentará una declaración de que a su leal saber y entender no existen tales operaciones.

Los sistemas de seguridad de la información, como las bases de datos y los sistemas conectados a Internet o a redes públicas de comunicación, están expuestos a una amplia variedad de riesgos internos y externos. La información confidencial contenida en la base de datos del proyecto requiere que el proveedor mantenga mecanismos estrictos de ciberdefensa.

12. Control 16.2 de la Metodología de Ciberdefensa para Organizaciones.

El proveedor hará uso de todos los medios tecnológicos y procedimientos necesarios para evitar, como mínimo, la creación de los siguientes riesgos:

- Fugas y exposición de información: una fuga de información se define como un reenvío de información del sistema del proveedor a un tercero no autorizado. El proveedor implementará un sistema de prevención de pérdida de datos<sup>13</sup> para evitar fugas de información. El sistema cubrirá todos los canales utilizados para enviar información desde la organización.
- Denegación de servicio:<sup>14</sup> el proveedor se compromete a implantar las medidas necesarias para detectar y neutralizar los incidentes de denegación de servicio.

### Protección de la privacidad, confidencialidad y garantía

- La organización es propietaria de las bases de datos. Está terminantemente prohibido que el proveedor venda, transfiera o copie total o parcialmente (ya sea

una copia impresa o digital) cualquier información que pertenezca a la organización sin el consentimiento previo y por escrito de la organización.

- El proveedor se compromete a utilizar la información únicamente para las actividades definidas en el acuerdo y a no hacerlo para ninguna otra actividad.
- El proveedor firmará un acuerdo de confidencialidad según lo solicite la organización y requerirá que cada uno de sus empleados involucrados en el desempeño de los servicios lo firme.
- El proveedor reenviará la información en un formato seguro utilizando los medios de transferencia de información seguros aprobados por la organización.
- Cifrado de datos:<sup>15</sup>

1. Datos en reposo: los datos almacenados en el sistema se cifrarán con la potencia mínima del estándar de cifrado avanzado (AES, por sus siglas en inglés) 256.
2. Datos en tránsito: toda la información en tránsito se cifrará utilizando seguridad de la capa de transporte (TLS, por sus siglas en inglés) o seguridad de protocolo de Internet (IPsec, por sus siglas en inglés) con una clave de una longitud mínima de 128 bits.

- Desarrollo seguro.<sup>16</sup> El proveedor se compromete a que, en caso de que se desarrolle *software*, todos los desarrollos cumplirán con los principios habituales para el “desarrollo seguro”. El proveedor de la clave del sistema o aplicación para la organización presentará un informe sobre el desempeño de un examen de código y una prueba de penetración por parte de una compañía externa.

### Protección física<sup>17</sup>

- Cualquier ubicación física en la que se gestione la información relacionada con la organización se asegurará mediante medios físicos de protección (sistema de control de entrada, cámaras y medios de control existentes en el mercado). La entrada a las instalaciones solo estará permitida para el personal autorizado cuando sea necesario que acceda a información.
- El proveedor definirá por separado los procedimientos de seguridad en sus diversas instalaciones en las que la información se utiliza dentro del alcance de este acuerdo.
- El proveedor almacenará todo el material procedente del sistema de \_\_\_\_\_ (a defi-

nir según la naturaleza del sistema crítico o sensible tratado) en una sala filmada y monitoreada las 24 horas del día los siete días de la semana, que presentará una capacidad de investigación retrospectiva de al menos dos semanas.

### Documentación<sup>18</sup>

A los fines de investigar incidentes y para las capacidades de control, el proveedor dispondrá de documentación técnica de los sistemas de telefonía y componentes de la red. El canal de control (como los archivos de registro) se conservará durante un período de tiempo que definirán conjuntamente el proveedor y la organización y que será, como mínimo, el exigido por la ley y las normas habituales en el campo.

### Monitoreo<sup>19</sup>

El proveedor documentará las operaciones de los usuarios en un sistema y el acceso a las bases de datos, registrando la identidad del usuario, la fecha de la operación, los detalles de la operación, etc. El proveedor monitoreará y detectará patrones anormales de actividad en el sistema y por parte de los usuarios, en particular en relación con el consumo de recursos, extracción de datos y actividad en horas anormales.

13. Control 5.1 de la *Metodología de Ciberdefensa para Organizaciones*.

14. Control 9.3 de la *Metodología de Ciberdefensa para Organizaciones*.

15. Control 8 de la *Metodología de Ciberdefensa para Organizaciones*.

16. Control 17.6 de la *Metodología de Ciberdefensa para Organizaciones*.

17. Control 18 de la *Metodología de Ciberdefensa para Organizaciones*.

18. Control 21 de la *Metodología de Ciberdefensa para Organizaciones*.

19. Control 21 de la *Metodología de Ciberdefensa para Organizaciones*.

### Grabación

El proveedor registrará las actividades que se realizan en un sistema. Esa grabación se conservará en los sistemas durante al menos 30 días. La grabación se realizará a nivel de \_\_\_\_\_ (a definir según la naturaleza del acuerdo).

### Copias de seguridad<sup>20</sup>

El proveedor realizará copias de seguridad diarias/semanales/mensuales/trimestrales (seleccionar la frecuencia deseada). El proveedor pondrá en marcha procedimientos para la recuperación y restauración de datos ante situaciones de falla operativa o falla de seguridad de datos y realizará simulacros trimestrales de restauración de datos de respaldo a fin de verificar el buen funcionamiento de las copias de seguridad.

### Bastionado de componentes<sup>21</sup>

El proveedor fortalecerá el equipo de comunicaciones, infraestructura y aplicaciones (servidores, enrutadores, conmutadores, estaciones de trabajo terminales, bases de datos, sus instalaciones, etc.) de acuerdo con los documentos de mejores prácticas de cada fabricante de software y hardware.

### Conexión de estación de trabajo y conexión remota a la red de la organización

- Se realizará una prueba de salud para las estaciones de trabajo como condición previa para conectarlas a la red de la organización (que debe incluir verificaciones de que un programa antivirus autorizado y el sistema operativo se han actualizado con las actualizaciones críticas de seguridad).
- La conexión usará un canal de comunicaciones seguro, como IPsec o capa de conexiones seguras/red privada virtual (SSL/VPN, por sus siglas en inglés), y la dirección IP externa legal que haya sido aprobada por la organización.
- Se prohibirá la conexión remota a componentes que el fabricante considere en fin de vida útil.

### Recursos humanos<sup>22</sup>

Los usuarios y las autorizaciones de usuarios en el sistema se administrarán de acuerdo con los siguientes principios:

- Gestión de las autorizaciones de acceso de usuarios determinada de acuerdo con la definición del trabajo a realizar.
- Compartimentación de los usuarios del sistema y visualización exclusivamente de la información pertinente.
- Mantenimiento de una lista actualizada de empleados y autorizaciones de acceso definidas.
- Evaluación y verificación de los empleados.
- Capacitación de los empleados y aumento de su conciencia sobre los riesgos informáticos, particularmente a aquellos que tengan acceso a información sobre \_\_\_\_\_ (un sistema crítico o sensible). La capacitación será una precondition para la asignación del empleado para el trabajo relacionado con la organización por parte del proveedor.



20. Control 25.10 de la Metodología de Ciberdefensa para Organizaciones.

21. Control 6.1 de la Metodología de Ciberdefensa para Organizaciones.

22. Control 19 de la Metodología de Ciberdefensa para Organizaciones.



### Presentación de informes, control y alertas<sup>23</sup>

- Notificación de cualquier indicación de compromiso o anomalía detectada durante el acuerdo al personal autorizado para actuar en nombre de la organización.
  - Notificación inmediata (el mismo día hábil) de incidentes anormales.
  - Control de incidentes y notificación a la organización.
1. El proveedor pondrá en marcha procedimientos para manejar incidentes de seguridad de datos: alertas, registro y gestión del incidente, proceso de remisión a una instancia superior y notificación a un representante de la organización. Además, el proveedor se compromete a informar a la organización de mane-

ra inmediata, tanto por escrito como verbalmente, en el momento en el que ocurra el incidente.

2. Durante estos incidentes, el proveedor permitirá actividades de investigación, como el reenvío de archivos de registro pertinentes, la duplicación de servidores y estaciones de trabajo, la apertura de canales de comunicaciones cifrados con el fin de revisarlos, etcétera.

- Garantizar el derecho de auditar. La organización o cualquier parte que actúe en su nombre pueden realizar una auditoría de seguridad de datos en cualquier momento sin previo aviso y sin coordinación anticipada con el proveedor.

### Gestión de contraseñas<sup>24</sup>

El proveedor implementará un sistema de identificación mediante contraseñas que cumplan con los siguientes requisitos:

- Tendrán ocho caracteres compuestos por al menos tres variables diferentes: mayúscula, minúscula, número, carácter especial.
- Las contraseñas usadas previamente no podrán reutilizarse.

- Después de tres intentos fallidos, el usuario será bloqueado.
- Las contraseñas se cambiarán como mínimo una vez cada tres meses.

### Externalización<sup>25</sup>

- El proveedor no hará uso de los servicios de ningún tercero para operaciones de servicio esenciales que sean parte de la prestación del servicio que proporciona dentro del alcance de este acuerdo, sin la autorización previa por escrito de la organización.
- El proveedor analizará los riesgos de seguridad de datos incurridos en la contratación con partes externas y presentará un informe de sus conclusiones a la organización y un plan para subsanar las deficiencias.
- Si fuera necesaria la externalización y la organización la aprueba, el proveedor será responsable de garantizar que todas las disposiciones de seguridad de datos especificadas en este documento sean también implementadas por la parte externa.

### Finalización del servicio y eliminación de datos

- El proveedor se compromete a permitir que la organización rescinda el servicio en cualquier momento sin restricciones contractuales injustificadas y se compromete a exportar la información para que pueda restaurarse a otro sistema dentro de los cinco días posteriores a la notificación de la organización.
- El proveedor se compromete a bloquear las cuentas de usuario y autorizaciones de acceso tras finalizar su uso.
- El proveedor se compromete a eliminar todos los componentes del sistema y toda la información almacenada (copias impresas, copias electrónicas, hardware, medios de almacenamiento, documentación, etc.) tras la finalización del servicio, y a proporcionar pruebas a la organización del modo en que se haya realizado dicha eliminación.

23. Control 24.4 de la Metodología de Ciberdefensa para Organizaciones.

24. Control 4.35 de la Metodología de Ciberdefensa para Organizaciones.

25. Control 16 de la Metodología de Ciberdefensa para Organizaciones.





Las organizaciones grandes y pequeñas invierten en seguridad cibernética para minimizar el riesgo de ciberataques capaces de ocasionar pérdidas financieras sustanciales y provocar el robo de sus secretos comerciales, daños a su reputación y la interrupción de la continuidad funcional. Sin embargo, muchos ataques cibernéticos contra organizaciones también se llevan a cabo a través de su cadena de suministro, como en casos donde los datos almacenados por un proveedor han sido robados y el sistema de la organización ha sido penetrado sirviéndose de las autorizaciones de acceso otorgadas a dicho proveedor, entre otros factores.

En este sentido, las industrias deben ser capaces de defenderse de los ataques que lleguen a través de su cadena de suministro. No obstante, las organizaciones tienen una capacidad muy limitada para controlar las actividades de ciberdefensa de sus proveedores y generalmente no disponen de los recursos para verificar su grado de cumplimiento en materia de defensa cibernética. Como resultado, el nivel de ciberdefensa de muchos proveedores puede ser significativamente más bajo que el que la organización exige de sí misma.

El presente documento ofrece una metodología ordenada y práctica para gestionar la ciberdefensa de la cadena de proveedores de cualquier organización, por medio del mapeo y clasificación de los riesgos que se originan en la cadena de suministros. Esto permite al lector incorporar en los acuerdos integrales con los proveedores todos aquellos criterios y niveles de servicio requeridos para cumplir con los estándares necesarios en materia de seguridad de datos para cada bien o servicio de la organización, de manera de evitar el robo de información sensible almacenada por un proveedor externo y prevenir los ataques de penetración que puedan utilizar las autorizaciones de acceso otorgadas a terceros.

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*

