

# Metodología de Ciberdefensa para Organizaciones Versión 2.0

Mejores Prácticas en Ciberseguridad



## A.02

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 “Doctrina de ciberdefensa 2.0”. © (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/cyber\\_security\\_methodology\\_2](https://www.gov.il/en/Departments/General/cyber_security_methodology_2). 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

## Resumen ejecutivo

/Pág. 8

## 01. Introducción

/Pág. 10

## 02. Principios de la Metodología de Ciberdefensa

/Pág. 12

## 03. Estructura de la Metodología de Ciberdefensa

/Pág. 14

## 04. Proceso de planificación desde la perspectiva de la organización

/Pág. 20

## Anexos

/Pág. 69

# 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>.

# Resumen ejecutivo

La finalidad de la Metodología de Ciberdefensa es presentar a la economía israelí un método profesional y organizado para la gestión de riesgos cibernéticos en las organizaciones. Por medio del método que se presenta en esta publicación, la organización podrá reconocer sus riesgos, formular una respuesta de defensa e implementar un plan de reducción de riesgos en función de ello.

## Fase A.

### La organización debe comprender a qué categoría pertenece

**Categoría A:** las organizaciones con un potencial de daños medio-bajo como resultado de un incidente cibernético.

**Categoría B:** las organizaciones con un potencial de daños alto como resultado de un incidente cibernético.

En la página 19 se incluye un cuestionario que sirve para determinar la categoría a la que pertenece la organización.

## Fase B.

### Realización del proceso de evaluación y gestión de riesgos

Las actividades de ciberprotección se llevan a cabo debido al deseo de la organización de gestionar los riesgos cibernéticos a los que está expuesta.

Para este fin, en primer lugar, la organización deberá definir cuáles son sus principales **objetivos de protección** (por lo general, procesos comerciales o activos digitales), cuál es el nivel de protección requerido, cuáles son las brechas de defensa en relación con la situación deseada y, luego, deberá elaborar un plan de trabajo para reducir dichas brechas.

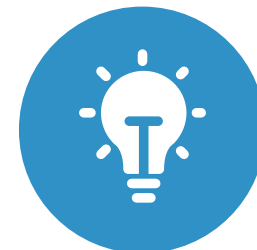
Este proceso se llevará a cabo de forma diferente en las distintas organizaciones, dependiendo de su tamaño, su grado de cumplimiento de los distintos requerimientos y reglamentos legales, y otros parámetros.

Esta publicación presenta una serie de métodos para efectuar la evaluación y gestión de riesgos, y diferencia entre organizaciones con un potencial de daños relativamente bajo (hasta US\$1,5 millones) y organizaciones con un potencial de daños superior, para las cuales se ha desarrollado una metodología más extensa.

## El producto final después de trabajar con esta publicación

La organización comprenderá el mapa de riesgos existentes y cuáles son los controles necesarios para reducirlos, incluyendo el orden de prioridad adecuado para poner en práctica el plan de trabajo.

Estos controles constituirán la base para la elaboración del plan de trabajo, la asignación de recursos y la preparación de la organización para todo lo anterior.



# /01. Introducción

El ciberespacio es ya una parte integral de nuestras vidas. A nivel personal, las personas buscan información en Internet, encuentran el camino correcto en la carretera utilizando un *software* de navegación, hablan por teléfono móvil y algunas también tienen un marcapasos o un dispositivo de insulina conectados a Internet. Y todo esto es parte del ciberespacio. A nivel comercial, se utilizan tarjetas de crédito, se gestionan bases de datos de clientes, se administran organizaciones globales por medio de redes informáticas, se realizan operaciones comerciales, se compra y vende; todo ello, con base en el ciberespacio.

Para muchas personas, disponer de un ciberespacio funcional, accesible y fiable es una condición necesaria para la vida diaria, particularmente en lo relativo a los negocios. Es fácil entender esto cuando no es posible hacer uso de él de manera temporal. ¿Cómo se puede gestionar un negocio sin un teléfono móvil? ¿Sin la información almacenada en la red de la organización? ¿Sin la capacidad de liquidar tarjetas de crédito?

El ciberespacio presenta oportunidades por un lado, y amenazas y riesgos por el otro. En este espacio tienen lugar a gran escala actividades de espionaje estatal e industrial, crimen organizado y delitos ocasionales. Todo ello puede tener un impacto en la seguridad nacional (por ejemplo, debido a daños al ciberespacio de estructuras nacionales fundamentales, tales como el sistema de agua o electricidad) o en la conducta empresarial

(por ejemplo, debido a espionaje comercial o extorsión de naturaleza económica).

En la actualidad, diferentes organizaciones se protegen ante estas amenazas de distintas maneras. Internet ofrece mucha información sobre formas de protegerse contra los riesgos cibernéticos, incluyendo metodologías organizadas, mejores prácticas, normas de “qué hacer y qué no hacer”, etcétera.

Numerosas organizaciones en Israel y en todo el mundo deben abordar cuestiones como: “¿Se está invirtiendo lo suficiente en ciberprotección?”, “¿se está invirtiendo correctamente en ciberprotección?” o “¿se está invirtiendo en ciberprotección de manera adecuada para la economía de la organización o su sector?”.

Esta Metodología de Ciberdefensa busca ayudar a las organizaciones a mapear los distintos riesgos cibernéticos, comprender la importancia de su materialización para cada organización y definir medios de protección adecuados para reducir los principales riesgos.

La Metodología va acompañada de diferentes apoyos para ayudar a la organización a la hora de implementarla. Esto incluye documentos de ampliación profesional, procedimientos de protección y recomendaciones para su implementación en distintos ámbitos, cuadros relativos a la legislación y las normativas israelíes y a estándares internacionales,

la mecanización de la Metodología por medio de una plataforma tecnológica que resulte cómoda a la organización, y mucho más.

**Puede encontrarse la información más reciente en el sitio web del Plan Cibernético:**  
[https://www.gov.il/en/departments/topics/organization\\_cyber\\_protection/govil-landing-page](https://www.gov.il/en/departments/topics/organization_cyber_protection/govil-landing-page)



# /02.

## Principios de la Metodología de Ciberdefensa

El principio fundamental de la Metodología de Ciberdefensa es la defensa contra las amenazas pertinentes a cada organización; es decir, reconocer que a la hora de proteger la continuidad operativa de la organización y sus activos deben comprenderse las amenazas de referencia, la inteligencia y las tendencias cambiantes en el campo en cuestión. Este principio se expresa por medio de los siguientes subprincipios:



### 01

**Responsabilidad de la gestión:** la responsabilidad de proteger la información recae principalmente en la Dirección de la organización.

### 02

**Protección desde la perspectiva del oponente:** el peso de las recomendaciones en materia de protección, y el concepto presentado para definir las prioridades en su implementación, deben derivarse directamente de una comprensión de los escenarios de ataque habituales y del grado de efectividad de dichas recomendaciones ante estos escenarios. Las recomendaciones de protección son los medios para conseguir un nivel de resiliencia organizacional acorde a las amenazas y el *modus operandi* del atacante que sean pertinentes para la organización.

### 03

**Protección basada en los conocimientos y la experiencia israelíes:** la Metodología de Ciberdefensa permite centrarse en los riesgos pertinentes para cada organización de forma individual. En el marco de las actividades del Plan Cibernético Nacional, se llevan a cabo periódicamente auditorías y evalua-

ciones de inteligencia de la economía. Estas actividades permiten a las organizaciones centrarse en ámbitos específicos de los distintos círculos de protección.

### 04

**Protección en función del potencial de daños:** la inversión en protección por cada uno de los objetivos de protección debe ser acorde a su grado de importancia para el funcionamiento de la organización.

### 05

**Protección basada en la profundidad de implementación:** los controles de la Metodología de Ciberdefensa permiten a la organización una implementación en diferentes niveles de madurez, por lo que se pasa de observar los controles desde punto de vista del cumplimiento (*compliance*) en aspectos como la prevención de pérdida de datos (DLP, por sus siglas en inglés), controles para organizaciones y sistemas (SOC, por sus siglas en inglés), estudios de riesgo, etc., al punto de vista de la efectividad de su implementación. Esto se refleja en la definición de “profundidad de implementación” para cada una de las recomendaciones en materia de protección (control) y la definición de “evidencia requerida” correspondiente.

# /03.

## Estructura de la Metodología de Ciberdefensa

La Metodología consta de dos rutas diferentes para la evaluación y gestión de riesgos, las cuales se derivan principalmente del potencial de daños para la organización como resultado de un incidente cibernético:

### 01

**Ruta para las organizaciones de la categoría A:** está destinada a las organizaciones en las que los daños sufridos por un incidente cibernético no superarían los US\$1,5 millones. Esta ruta comprende un proceso simple y rápido de mapeo de los objetivos de protección y la respuesta a un número reducido de preguntas adaptadas a las organizaciones pertenecientes a esta categoría. En la mayoría de los casos, este proceso será realizado por una parte externa que asesore sobre los aspectos de ciberprotección de la organización.

### 02

**Ruta para las organizaciones de la categoría B:** está destinada a las organizaciones en las que los daños sufridos por un incidente cibernético puedan superar los US\$1,5 millones. Esta ruta incluye un proceso de evaluación de riesgos (*risk assessment*), la comprensión de la respuesta de protección requerida en relación con la matriz de riesgos (*risk matrix*), el apetito de riesgo (*risk appetite*), el examen de la situación actual en relación con las recomendaciones de protección aceptadas en la industria (*gap analysis*) y la elaboración de un plan de trabajo para reducir los riesgos (*mitigation plan*) o tratarlos de otra manera. En la mayoría de los casos, los procesos de evaluación y de análisis de sus conclusiones serán gestionados por el responsable de ciberprotección de la organización (como parte de su cargo o como un campo de responsabilidad

**¿Los daños resultantes de un incidente cibernético en su organización pueden exceder los US\$1,5 millones?** A fin de calcular el impacto económico, se recomienda ponderar, entre otros, los siguientes parámetros:

- La pérdida de ingresos resultante de los daños a la continuidad del negocio.
- El costo de hacer frente al incidente (incluyendo equipos de respuesta, expertos en contenido, etc.).
- El costo de rehabilitar los sistemas de información hasta que vuelvan a la normalidad (incluyendo licencias, *hardware* y *software*).
- El costo directo resultante de la violación de leyes/regulaciones y de posibles demandas comerciales.
- Los daños indirectos, por ejemplo a la reputación, incluyendo el posible impacto de la pérdida de clientes nuevos y existentes.



adicional). En algunas ocasiones, el responsable será una parte externa.

A fin de evaluar los daños con mayor precisión, pueden utilizarse calculadoras y estudios profesionales que ponderen parámetros tales como el sector en el que opere la organización, el tipo de información y la cantidad de expedientes que tenga.

No obstante, es recomendable que la organización examine el potencial de daños desde una perspectiva más amplia, que incluya aspectos de responsabilidad corporativa. La visión en la base del enfoque es que el fundamento de una organización comercial no es solo la creación de beneficios para los accionistas (*shareholders*), sino también la creación de valor para todas las partes interesadas (*stakeholders*), como

clientes, empleados, proveedores, inversores, comunidad y medio ambiente.

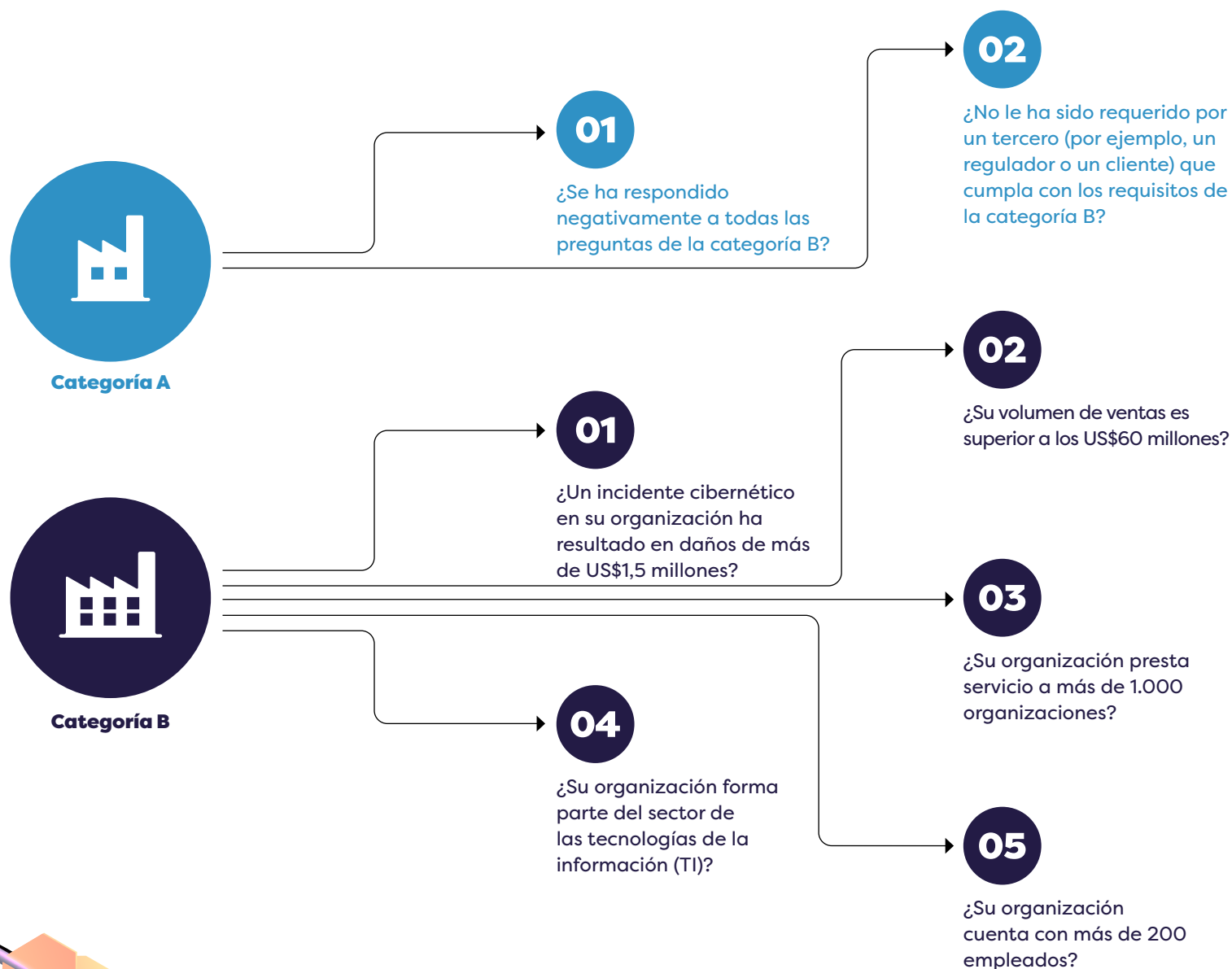
Al aplicarse este enfoque, se ponderan los efectos de un incidente cibernético para las partes interesadas de la organización, se refuerza la relación de confianza entre ellas y se consigue una mejora del rendimiento económico a largo plazo. El enfoque también aborda los daños potenciales a la vida humana, a la confianza de los ciudadanos, a terceros y una visión amplia e integral de los posibles daños agregados no solo a la organización, sino también a círculos de impacto más amplios.

Para comprender rápidamente a cuál de estas categorías pertenece su organización, puede ayudarse con las reglas prácticas que se presentan a continuación.

## Árbol de clasificación de organizaciones

En el gráfico 1 se ponderan parámetros tales como el tamaño de la organización, el número de clientes, el volumen de negocios y el grado de dependencia de los medios digitales. Este árbol no reemplaza al estudio del potencial de daños, pero puede ayudar a dirigir a la organización hacia el camino correcto.

**Gráfico 1.** Árbol de clasificación de organizaciones



# Organizaciones representativas de cada categoría

En el cuadro 1 se muestra un ejemplo general de una posible división de los tipos de organizaciones en la categoría recomendada para estas. Esta división es superficial y está destinada a proporcionar una regla práctica preliminar para clasificar las organizaciones en diferentes categorías.

**Cuadro 1.** Organizaciones representativas de cada categoría

Categoría A	Categoría B
Despacho de abogados pequeño	Ayuntamiento
Despacho contable pequeño	Hospital
Imprenta pequeña	Institución académica
Empresa de traducción pequeña	Oficina estatal
Fábrica pequeña	Compañía de software
	Proveedor de servicios informáticos

## Cuestionario

Responder a estas preguntas específicas ayudará a decidir a qué categoría pertenece la organización.

### ¿Cuál es el grado de motivación para atacar a la organización?

- ¿Qué tipo de información existe en la organización? Por ejemplo, información personal, datos financieros (como datos de créditos), información de carácter médico, patentes o información de seguridad.
- ¿Cuál es el alcance de la información sensible existente en la organización? Por ejemplo, ¿hay cientos, miles o cientos de miles de registros?
- ¿Cuál es la naturaleza de la organización? Por ejemplo, ¿es una compañía de software que proporcionaría una ruta de acceso a otros clientes?, ¿es una organización que almacena datos de muchos clientes?, ¿es un símbolo nacional?

### ¿Cuál es la superficie de ataque de la organización?

Por ejemplo, la cantidad de interfaces abiertas de la organización y el tipo de interfaces, el despliegue y la accesibilidad

globales a los activos digitales de la organización, o la cantidad y el tipo de proveedores de la organización.

### ¿Cuáles son los recursos dedicados por la organización a la ciberprotección?

Por ejemplo, ¿hay un encargado de ciberprotección y protección de la información en la organización?, ¿el gerente de sistemas de información asigna recursos a la gestión de la ciberprotección?, ¿el presupuesto para ciberprotección de la organización se adecua al esquema de amenazas de su sector y ha sido definido por la Dirección como un porcentaje de la facturación anual o del presupuesto de TI?

**Si la organización está sujeta a obligaciones adicionales de legislaciones y/o regulaciones que debe cumplir, requerimientos contractuales o necesidades comerciales distintas, esto podría resultar en su transferencia de la categoría A a la B.** Por otra parte, las organizaciones que tengan una gran dependencia tecnológica y que puedan sufrir daños importantes debido a un incidente cibernético, deben considerar llevar a cabo este proceso según los requisitos de la categoría B.

# /04.

## Proceso de planificación desde la perspectiva de la organización

En esta sección se presenta el trabajo en función de la categoría de la organización.



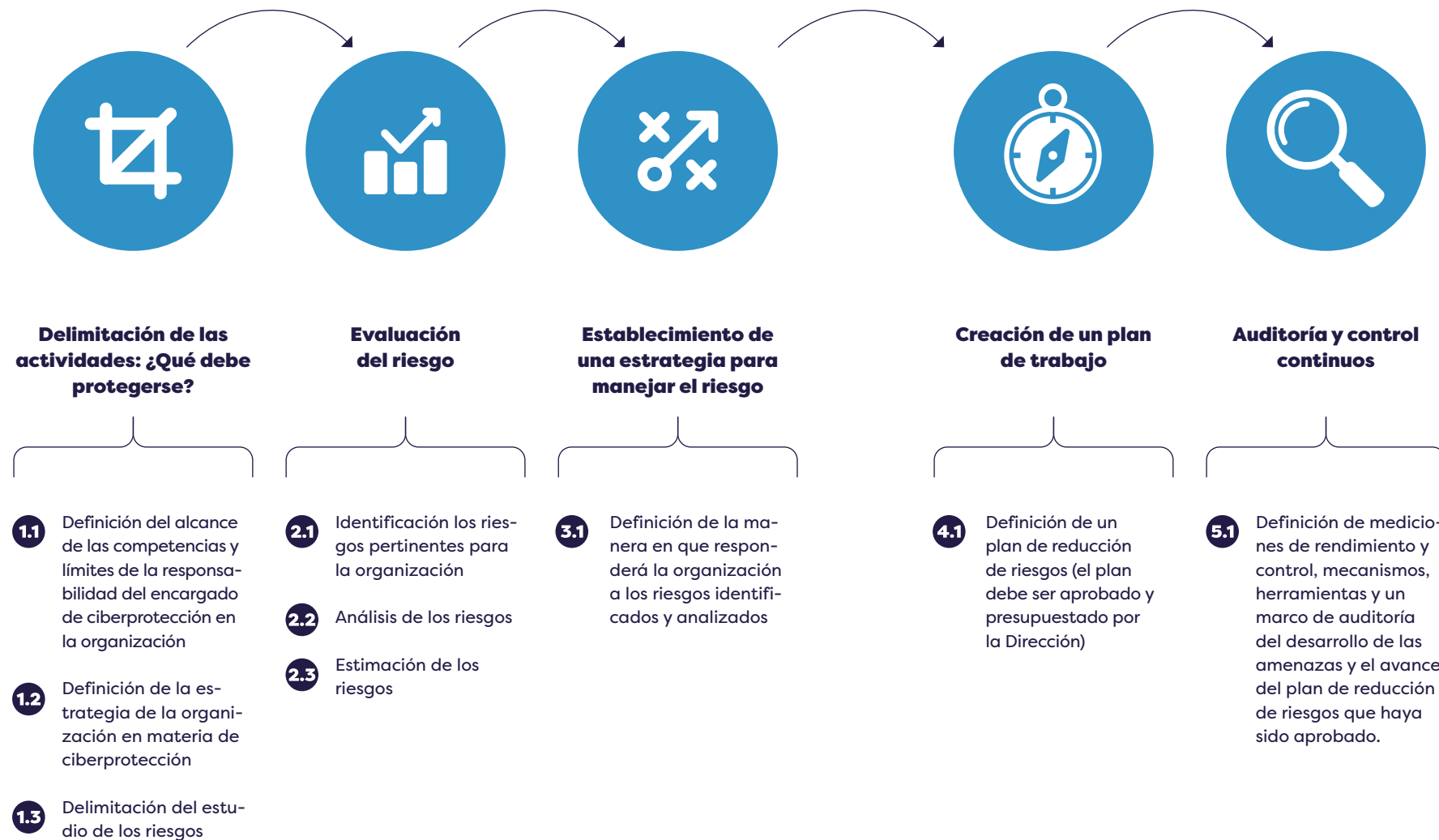
## Para una organización de categoría A

**Gráfico 2.** Proceso de planificación para una organización de categoría A



## Para una organización de categoría B

**Gráfico 3.** Proceso de planificación para una organización de categoría B



## Implementación de la Metodología de Ciberdefensa para una organización de categoría A

### Fase 1: delimitación de las actividades

Se debe consultar con el encargado de soporte técnico cuáles son los tipos de equipos y activos informáticos utilizados por la organización. Además, es necesario comprender cuáles son los activos digitales de la organiza-

ción y dónde están almacenados. La finalidad de esta fase es identificar cuáles son los objetivos de protección contra las ciberamenazas. Como parte de esta fase de delimitación, debe entenderse si la organización dispone de bases de datos, activos digitales como redes sociales, sistemas organizacionales y software como un sistema para los salarios, un sistema de asistencia laboral o estaciones de pago y liquidación.

Al final de esta fase, la organización tendrá una lista de activos. Así deberá examinarse el nivel de protección de estos activos frente a riesgos cibernéticos de acuerdo con la lista de controles recomendados.

**Gráfico 4.** Ejemplo de mapeo de los objetivos de protección en una organización de la categoría A



### Fases 2-3: evaluación y tratamiento de riesgos. Los 10 mandamientos para una organización de la categoría A

Una organización de la categoría A necesita defenderse de forma acorde al potencial de daños. Por consiguiente, deberá utilizar controles con una efectividad especialmente alta.

En numerosos incidentes cibernéticos, los atacantes no tienen en cuenta el tamaño de la organización o los daños potenciales que puedan causarse. Muchos negocios pequeños han sufrido ataques de secuestro de datos (*ransomware*), fugas de la base de clientes, robos de información de los clientes, etcétera.

A fin de reducir la probabilidad de sufrir daños en este tipo de incidentes e incrementar la capacidad de supervivencia y continuidad del negocio en caso de producirse un ataque, se recomienda que todas las organizaciones adopten los requisitos de protección transversal que figuran en el anexo 1. Estos controles se dividen en las 10 categorías de protección que se presentan en el recuadro 1.



**Recuadro 1.** Diez categorías de protección para organizaciones de categoría A

**1. Responsabilidad de gestión:** comprender los riesgos a los que se enfrenta la organización en el ciberespacio y crear un plan de trabajo destinado a cerrar las brechas de protección en este ámbito.

**2. Evitar código malicioso:** utilizar tecnologías para manejar *software* malicioso (*malware*) y realizar actualizaciones de seguridad en los sistemas de su organización. En particular, debe prestarse atención a la protección contra *malware* que llega por correo electrónico y al navegar por sitios web.

**3. Cifrado:** cifrar la conexión remota de los empleados y proveedores de la organización, utilizando mecanismos de cifrado sencillos y comerciales. Cifrar el acceso a la información sensible utilizando un medio de comunicación cifrado (tanto al navegar a la organización desde una red doméstica inalámbrica como desde la organización a clientes y proveedores).

**4. Computación en la nube y adquisición de *software*:** celebrar un contrato con el proveedor que requiera el cumplimiento de los estándares aceptados para la protección de *software* y la información, como el método de la cadena de suministro del Plan Cibernético. En particular, al subir datos a la nube, debe asegurarse una división de responsabilidad de la ciberprotección entre el proveedor de la nube y la organización.

**5. Protección de la información:** establecer mecanismos de protección sobre cómo debe sacarse información fuera de la organización.

**6. Protección de computadoras y equipos periféricos:** establecer el nivel de protección requerido para las computadoras. Este nivel debe incluir el cambio de las contraseñas predeterminadas, la eliminación de *software* innecesario, la securización de las interfaces externas y la eliminación de usuarios fuertes (*Admin account*) que no sean necesarios.

**7. Recursos humanos:** instruir a los empleados en el momento de su contratación, incrementar su concienciación y hacerles firmar acuerdos que eviten que revelen información de la organización cuando termine la relación laboral. Establecer políticas para el uso de equipos informáticos privados y su conexión a la organización, y formular procedimientos de trabajo para la red y las computadoras. Establecer políticas para el personal de informática y ciberprotección (examinando la forma de contratación, ya sea como empleados internos o externos), que incluya su concienciación y el control de sus actividades.

**8. Documentación y monitoreo:** con vistas a una investigación en el futuro, monitorear y documentar los registros de actividades inusuales que la organización desee saber si se han producido y que indiquen una amenaza cibernética.

**9. Seguridad de la red:** asegurarse de que el acceso a la red esté bajo control de la organización (los proveedores y los empleados no deben poder conectarse a la red de forma remota cuando y como quieran) y que la red esté preparada frente ataques de denegación de servicio (DoS, por sus siglas en inglés). En particular, debe reducirse la superficie de exposición y comprobar si la organización está expuesta al mundo a través de interfaces innecesarias y/o no seguras.

**10. Continuidad del negocio:** asegurarse de que exista capacidad de recuperación en caso de una caída del sitio web, eliminación de información o bloqueo de archivos. En particular, debe garantizarse que exista una copia de seguridad eficaz. Además, debe llevarse a cabo una restauración activa de forma periódica y establecerse la frecuencia y el tipo de copia de seguridad que se requiere.

## Tras examinar el estado de implementación de los controles, debe decidirse qué respuesta se requiere para los riesgos derivados de las brechas en la puesta en práctica de dichos controles.

Por lo general, estos riesgos se dividen en violaciones de la confidencialidad de los datos, de la continuidad del negocio y de la integridad de la información. Estos riesgos pueden tener numerosas consecuencias, tales como daños a la reputación del negocio, incapacidad para recibir a clientes y brindarles un servicio, exposición a demandas por incumplimiento de una legislación y/o normativa, o fugas de la información de los clientes que podrían denunciar a la organización. Es importante examinar estos riesgos frente a los objetivos de protección definidos en la fase 1.

### Fase 4: elaboración de un plan de trabajo

Luego de que la organización haya definido los riesgos para sus objetivos de protección, debe elaborarse un plan anual para reducirlos y/o transferirlos, de acuerdo con lo decidido en la fase 3. Dicho plan puede incluir la implementación de procesos y adquisición de

soluciones, como la comprobación periódica de las copias de seguridad en la compañía, la protección de computadoras portátiles, la instalación de *software* de protección de las estaciones finales y la formación de los empleados de la organización.

Al elaborarse el plan de trabajo para cerrar las brechas en los controles, deben tenerse en cuenta las siguientes consideraciones:

# 01

**Efectividad del control:** su contribución a la reducción del riesgo para la organización.

# 02

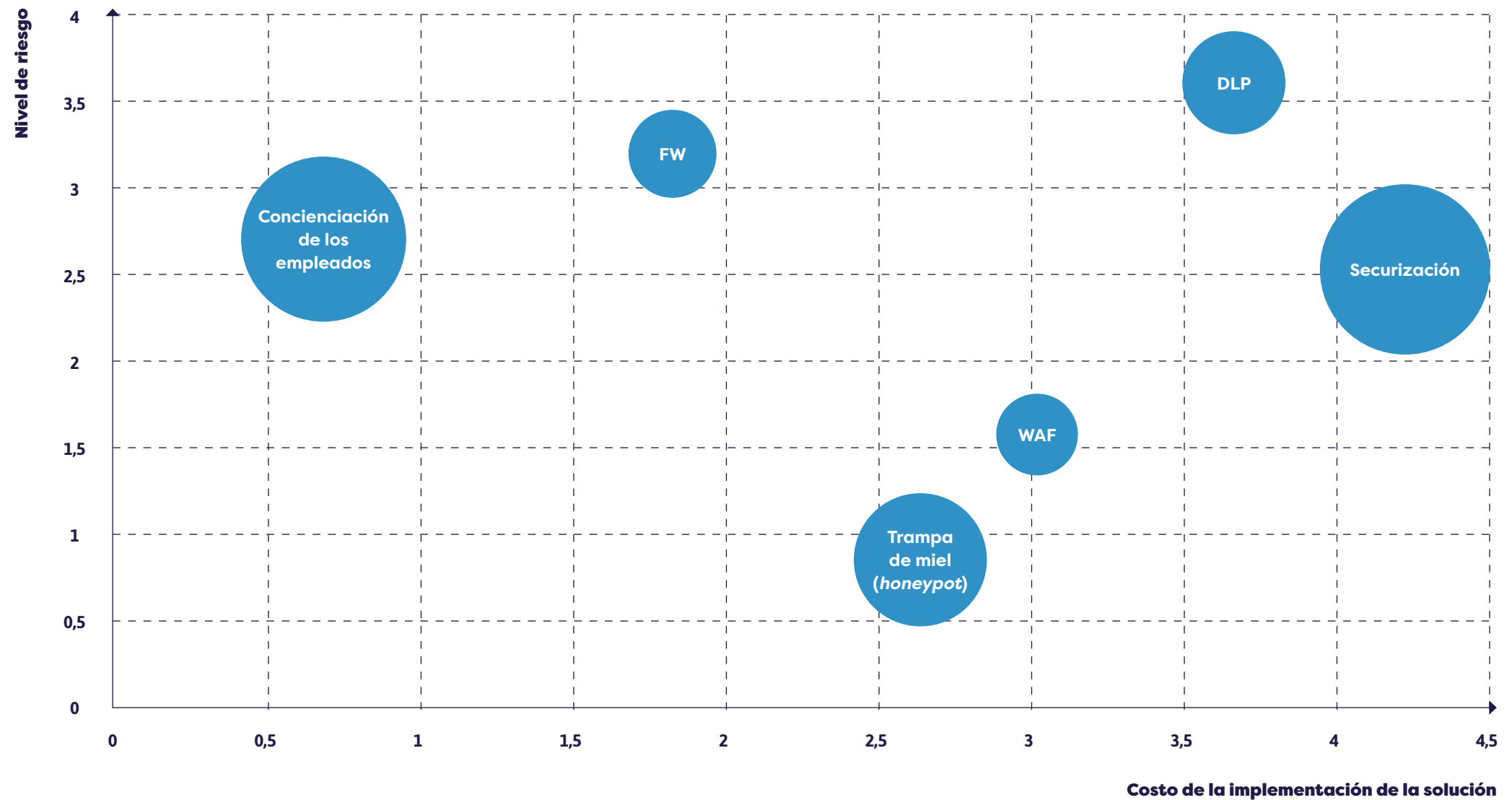
**Costo de la implementación de la solución:** se representa en el gráfico 5, mediante el eje costo de la solución (duración y complejidad de la implementación, mano de obra y equipo requerido).

# 03

**Velocidad de la implementación:** se representa en el gráfico 5, mediante el tamaño del círculo.

**Gráfico 5.** Ejemplo de la ponderación de parámetros para determinar las prioridades del plan de trabajo para una organización de la categoría A

**Nota:** FW: cortafuegos (firewall); WAF: cortafuegos de aplicaciones web (siglas en inglés);  
DLP: prevención de pérdida de datos (siglas en inglés).



**Cuadro 2.** Apoyo para completar los datos del plan de trabajo

Objetivos de protección mapeados en la organización	Por ejemplo: sitio web, base de clientes, estaciones finales, servidor de correo electrónico, servidor de copia de seguridad, etc.			
Familia de control	Existe / no existe	Efectividad del control	Costo de la implementación	Ponderación de datos/priorización
Responsabilidad de gestión				
Evitar código malicioso				
Cifrado				
Computación en la nube y adquisición de software				
Protección de información				
Protección de computadoras				
Recursos humanos				
Documentación y monitoreo				
Seguridad de la red				
Continuidad del negocio				

El cuadro 2 sirve de ayuda para completar los datos. Debe tenerse en cuenta que el plan de trabajo propuesto debe ser aprobado por el director de la organización.

**Fase 5:** auditoría y control continuos

Deben examinarse periódicamente el ritmo de la puesta en práctica del plan de trabajo y su grado de pertinencia. La finalidad de esta fase es comprobar si existen nuevos activos de información, qué controles han sido implementados hasta el momento y qué recursos y aportaciones se requieren de parte de la Dirección de la organización a ese respecto.

La auditoría puede realizarse paralelamente a una inspección periódica (por ejemplo, anualmente o cada dos meses) o en relación con incidentes cibernéticos que hayan tenido lugar en los últimos años en negocios pequeños en Israel y en el extranjero. Esta auditoría ayudará a la organización a centrar sus esfuerzos y priorizar los recursos en función de los riesgos que sean más pertinentes para la organización.

Aquí termina la lectura para las organizaciones de categoría A.

## Implementación de la Metodología de Ciberdefensa para una organización de categoría B

### Fase 0: gobernanza corporativa y estrategia de gestión de riesgos de la organización

Antes de identificar las amenazas y respuestas de la organización, debe examinarse la gobernanza corporativa que apoya el proceso (llamado a veces sistema de gestión de seguridad de la información [ISMS, por sus siglas en inglés]): su finalidad, definición de jerarquía, funcionarios, rutinas de protección y procedimientos de control efectuados. El objetivo es mapear los riesgos cibernéticos y la respuesta a estos, de manera de presentar una mejora continua.

**En el marco de la definición de la gobernanza corporativa, la organización debe hacer referencia a los siguientes puntos:**

# 01

¿Cuál es la parte que realiza la evaluación del riesgo en la organización? ¿Cuál es su formación y su experiencia en este ámbito?

¿Qué recursos tiene a su disposición? ¿Ante quién rinde cuentas en la organización?

# 02

¿Existe en la organización un mapeo de procesos sensibles como parte del plan de continuidad del negocio (BIA, por sus siglas en inglés) que pueda utilizarse para efectuar la evaluación de riesgos? ¿Cómo se integra la evaluación de riesgos con los objetivos de la organización?

# 03

¿Con qué método se identificarán los nuevos riesgos y qué herramientas están a disposición de la organización para identificarlos de forma eficaz?

# 04

¿Con qué frecuencia se efectúa la evaluación de riesgos? ¿La evaluación de riesgos se realizará a la vista de escenarios de ataque y amenazas de referencia, o según la metodología de gestión de riesgos (ERM, por sus siglas en inglés) general de la organización?

# 05

¿Cuál es la parte autorizada para decidir si se acepta un riesgo? ¿Quién está autorizado para aprobar las actividades destinadas a la reducción de riesgos? ¿Quién está autorizado para modificar un riesgo a un valor menor, a la vista de la implementación de controles de protección y actividades correctivas/compensatorias?

# 06

¿Existe un comité de gestión en materia de ciberprotección y protección de la información? En tal caso, ¿quiénes forman parte de él? ¿Existe un comité de dirección en materia de continuidad del negocio? En tal caso, ¿quiénes forman parte de él?

### Fase 1: delimitación de la actividad y estudio de la evaluación de riesgos

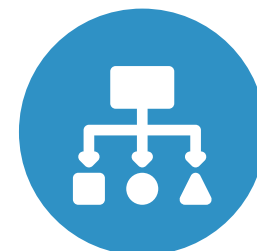
La delimitación de los objetivos de protección es una fase inicial y necesaria a fin de comprender el entorno en el que la organización opera y definir los límites del sector y los ámbitos de responsabilidad. **En esta fase, la organización debe abordar, entre otros, los siguientes puntos:**

# 01

**Límites entre el encargado de ciberprotección y protección de la información y otros funcionarios en la organización:** debe establecerse una división de competencias y responsabilidades con las partes interesadas internas, como el oficial de seguridad, el responsable de operaciones, el responsable de sistemas de información, el responsable de riesgos, el asesor jurídico y el director general. Si la organización recibe servicios cibernéticos y/o informáticos (MSSP, por sus siglas en inglés), es importante definir la interacción y división de responsabilidades entre las partes.

# 02

**Conocimiento profundo de la estrategia de la organización** (incluyendo visión, objetivos, características del mercado en cuestión y de los competidores) y cómo se integra la ciberprotección y la protección de la información.



# 03

**Establecimiento de la delimitación del estudio de riesgos:** el estudio debe abordar aspectos como las cámaras de seguridad, el sistema de aire acondicionado, la línea de producción y el entorno operativo, informatización privada de los empleados, la cadena de suministro y sucursales fuera de las fronteras del país.

**Al final de esta fase, la organización tendrá un documento que describe su entorno comercial, sus características y la delimitación de las actividades del estudio.**

Esta fase puede tener consecuencias para los documentos de continuidad del negocio, el plan de respuesta a incidentes de la organización, los contratos con proveedores, el documento BIA, procesos de fusión y adquisición (M&A, por sus siglas en inglés), etcétera.

## Fase 2: evaluación del riesgo

Esta fase consta de tres partes: **identificación del riesgo, análisis del riesgo y evaluación del riesgo.**

Existen numerosos métodos para la evaluación de riesgos, que incluyen OCTAVE, FAIR e ISO 27005. Cada uno de ellos presenta características y beneficios únicos. Esta publicación presenta un método que combina numerosas ventajas de los métodos conocidos y les suma

los conocimientos de la experiencia práctica obtenida sobre el terreno, adaptándolos a la economía israelí.

## 2.1 Identificación del riesgo

Esta actividad consta de las dos fases siguientes:

# 01

**Mapeo de los objetivos de protección:** consiste en identificar los objetivos que la organización debe proteger en el ámbito cibernético. Este mapeo puede incluir una lista de activos, como aplicaciones, redes o sistemas operativos. Asimismo, puede incluir una lista de procesos comerciales importantes, a los que se asignen los activos digitales que sirvan a dichos procesos (tales como procesos de salarios, informes bursátiles o liquidación de tarjetas de crédito). Se recomienda priorizar el mapeo de los procesos comerciales sobre el mapeo de los objetivos de protección, analizando las distintas interacciones.

# 02

**Asignación de riesgos y/o amenazas y vulnerabilidades:** tras mapear los objetivos de protección, deben examinarse las ciberamenazas pertinentes para los procesos y los activos identificados. Por ejemplo, cuáles son los posibles cursos de acción a través de los cuales

un atacante podría materializar la amenaza, como la alteración del proceso de producción o la obtención de acceso a la base de datos sensible de la organización. En el anexo 2 de esta publicación encontrará una lista de amenazas y vulnerabilidades frecuentes.

A fin de efectuar un mapeo integral de los activos de TI, se recomienda obtener una lista de activos del departamento de sistemas de información de la organización. También es importante contar con una lista de proveedores de productos y servicios del departamento de adquisiciones, que permita

detectar los sistemas que se brinden como un servicio y ocasionalmente no sean administrados por el departamento informático central de la organización (*shadow IT*). A fin de mapear los activos de tecnologías operativas (OT, por sus siglas en inglés), se recomienda reunirse con los responsables de operaciones y de seguridad (en particular, en organizaciones industriales).

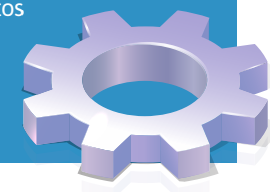
Las organizaciones que hayan formulado un plan de continuidad del negocio, podrán emplearlo para mapear los procesos comerciales esenciales (uso de BIA).

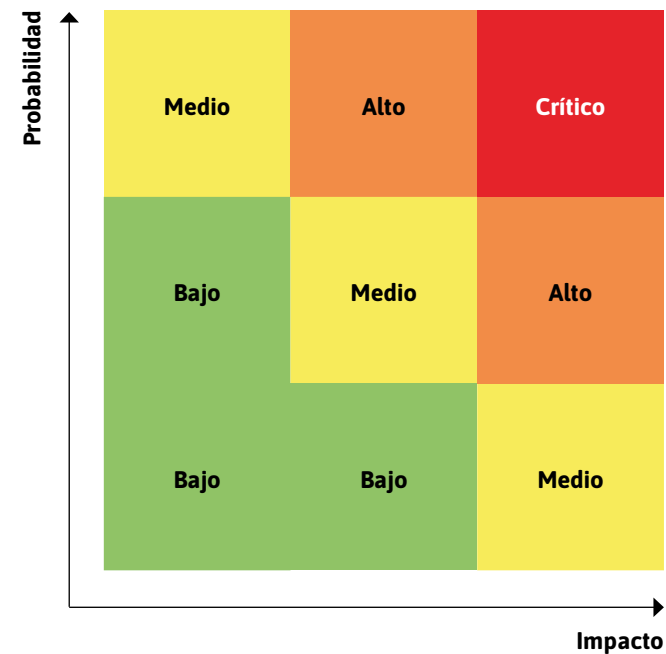
### Consejo: resolución del mapeo de objetivos

El mapeo de los objetivos de defensa es un proceso que requiere tiempo y recursos. A fin de realizar este proceso de manera eficaz, debe prestarse atención a la resolución del mapeo.

Por ejemplo: por un lado, es evidente que no es necesario enumerar todos los servidores y estaciones finales, pero, por el otro lado, definir todos los servidores de manera generalizada como un todo podría resultar en costos de protección desproporcionados (exceso o falta de inversión con respecto al riesgo real).

Atención: en ocasiones, la información sensible de la organización se encuentra en poder de los proveedores o se almacena en la nube. Además, a veces la información sensible se almacena en un archivo en lugar de hacerlo en una base de datos o un sistema de información específicos. Un buen mapeo también deberá incluir estos activos. Una descripción de los procesos centrales del negocio es una buena forma de asegurarse de que el mapeo en cuestión tenga en cuenta todos los activos esenciales.



**Gráfico 6.** Matriz de riesgos**Análisis del riesgo**

Su finalidad es determinar los eventos que podrían tener lugar tomando como base la información a disposición de la organización. Existen diferentes métodos para evaluar el nivel de riesgo que plantea cada posible evento. Uno de los más comunes es el uso de una fórmula:

$$\text{Riesgo} = \text{impacto} \times \text{probabilidad}$$

Esta fórmula se basa en la norma ISO 31000, que define el riesgo como el producto de la in-

tensidad de los daños potenciales con la probabilidad de su materialización (cuáles serán los riesgos en caso de producirse el evento y cuál es la probabilidad de que este ocurra).

**Cálculo de la intensidad de los daños**

Por lo general, se lleva a cabo examinando el potencial máximo de los daños como resultado de una violación de la confidencialidad (C), integridad (I) o disponibilidad de los datos (D) (CID). Para efectuar el cálculo de la intensidad, se recomienda utilizar el cuadro 3.

**Cuadro 3.** Cuestionario para determinar el cálculo de intensidad de los daños

Pregunta	Nivel 1	Nivel 2	Nivel 3	Nivel 4
<p>1. ¿Cuál es el nivel de daños que sufrirá la organización como resultado de la exposición de información del proceso/activo?</p> <p><b>C</b></p> <p>Confidencialidad</p>	<p>Los daños estimados cumplen uno o más de los siguientes criterios:</p> <p>A) Costo de hasta US\$1,5 millones para la organización.</p> <p>B) Inversión de hasta dos meses de mano de obra del personal para manejar el incidente.</p> <p>C) El activo está definido como una base de datos gestionada por un individuo de acuerdo con las regulaciones de protección de la privacidad (seguridad de la información).</p>	<p>Los daños estimados cumplen uno o más de los siguientes criterios:</p> <p>A) Costo de entre US\$1,5 y US\$3 millones para la organización.</p> <p>B) Una inversión de más de seis meses y menos de cinco años de mano de obra del personal para manejar el incidente.</p> <p>C) El activo está definido como una base de datos a la que se aplica un nivel de seguridad bajo de acuerdo con las regulaciones de protección de la privacidad (seguridad de la información).</p>	<p>Los daños estimados cumplen uno o más de los siguientes criterios:</p> <p>A) Costo de más de US\$3 millones para la organización.</p> <p>B) Inversión de más de cinco años de mano de obra del personal para manejar el incidente.</p> <p>C) El activo está definido como una base de datos a la que se aplica un nivel de seguridad medio de acuerdo con las regulaciones de protección de la privacidad (seguridad de la información).</p> <p>D) Existe un peligro posible para la vida humana.</p>	<p>Los daños estimados cumplen uno o más de los siguientes criterios:</p> <p>A) Existe un peligro claro e inmediato para la vida de muchas personas.</p> <p>B) Daños económicos estimados en más de US\$30 millones.</p> <p>C) El activo está definido como una base de datos a la que se aplica un nivel de seguridad alto de acuerdo con las regulaciones de protección de la privacidad (seguridad de la información).</p> <p>D) Existe un peligro claro para la salud pública.</p> <p>E) Existe un peligro claro para la vida humana.</p>
<p>2. ¿Cuál es el nivel de daños que sufrirá la organización como resultado de la alteración de la información (o los datos) en el proceso/activo?</p> <p><b>I</b></p> <p>Integridad</p>				
<p>3. ¿Cuál es el nivel de daños que sufrirá la organización debido a la interrupción del proceso/activo por un período de tiempo prolongado?</p> <p><b>D</b></p> <p>Disponibilidad</p>				



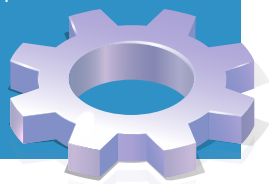
El valor de cada proceso/activo será la puntuación más alta que se obtenga para las tres preguntas (Impacto = MAX 1-4). Esta puntuación también se conoce como la **intensidad** del riesgo y define el potencial máximo de los daños para la organización como resultado de un daño en el proceso/activo en cuestión.

**Atención.** En el ámbito de la ciberprotección y la seguridad de la información, es habitual examinar los daños que pueden sufrirse a través de tres categorías:

**Violación de la confidencialidad de los datos:** por ejemplo, un ciberataque destinado a filtrar información de clientes o un secreto comercial a Internet.

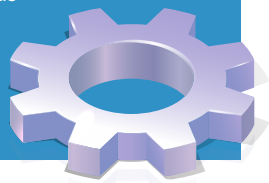
**Daños a la fiabilidad (confiabilidad) de los datos:** por ejemplo, un ciberataque que modifique los datos del informe financiero de una compañía a fin de que no represente correctamente su situación, o un ciberataque destinado a interrumpir el funcionamiento correcto de una línea de protección.

**Daños a la disponibilidad de los datos:** por ejemplo, un ciberataque destinado a que la información no esté disponible para la compañía o para sus clientes, como al bloquear un sitio o archivos (ransomware).



#### Consejo: desviaciones comunes en la evaluación del activo

El análisis del valor del activo debe llevarse a cabo junto a las partes comerciales. En ocasiones, los propietarios de activos comerciales se sienten “sobrevalorados” y consideran que su activo es el más importante para la organización. Adherirse a los criterios del cuestionario neutralizará esta percepción y ayudará a evaluar los sistemas en una escala uniforme y sin desviaciones. Debe tenerse en cuenta que, en ocasiones, los daños a la fiabilidad de los datos pueden tener consecuencias para los procesos en el espacio físico. Por consiguiente, en el proceso de evaluación de riesgos, es importante examinar las repercusiones de un incidente cibernético en el entorno OT, los sistemas de control industriales (ICS, por sus siglas en inglés), las cámaras de seguridad, los sistemas de auditoría y control o los equipos que a menudo no son gestionados por el personal de TI.



**El cálculo del grado de probabilidad puede basarse en una ponderación de distintos parámetros.**

Entre los parámetros que pueden tenerse en cuenta, se encuentran los siguientes:

# 01

**Historial de eventos:** una descripción de los incidentes cibernéticos que hayan tenido lugar en los últimos años, examinando el sector en el que opere la organización, sus características, sus sistemas característicos, etc. La finalidad de esto es comprender los tipos de ataques conocidos en el mundo y la frecuencia y prevalencia de cada uno. Identificar las tendencias en el mundo ayudará a prestar especial atención a los incidentes que se hayan producido recientemente, lo que permitirá prepararse para los retos a los que se enfrente la organización/el sector en la actualidad.

# 02

**Ciberinteligencia:** localizar inteligencia en la web (utilizando recursos internos o adquiriendo un servicio externo) permitirá a la organización tener una perspectiva más precisa y prepararse de forma puntual para protegerse en función de la situación desde el punto de vista del atacante.

# 03

**Facilidad de implementación:** la facilidad de implementación del ataque puede verse afectada por numerosas variables, como el tamaño de la superficie de ataque (incluyendo la cantidad y el tipo de usuarios), el nivel de protección y la accesibilidad física al activo, la cantidad y el tipo de interfaces, así como las posibles acciones del oponente en relación con las rutas críticas (rutas de entrada y salida a la organización).

# 04

**Motivación del ataque y tipo de información:** a menudo, el tamaño y el tipo de la base de datos, la identidad de su propietario, la existencia de competidores comerciales y partes adicionales afectan la motivación de diferentes partes interesadas para atacar a la organización. Por ejemplo, los sistemas que contienen información médica y/o financiera están expuestos a un nivel de amenaza distinto de los sistemas que contienen un tipo de información diferente.

Ponderar la motivación, los tipos de información, las partes interesadas y los daños potenciales puede ayudar a la organización a producir un mapa de riesgos más preciso, que tenga en consideración la visión del oponente.

El cuadro 4 puede utilizarse como herramienta de apoyo para la toma de decisiones en este proceso.

#### **Cuadro 4.** Guía para analizar la visión del oponente



##### **Actores**

- Gobierno / autoridades / personas enviadas
- Organizaciones criminales
- Empleado con privilegios
- Grupos terroristas
- *Hackers* activistas
- Competidores comerciales
- *Hacker* solitario cualificado
- Usuario de *scripts* no cualificado (*script kiddie*)



##### **Motivación**

- Espionaje militar
- Información para operaciones
- Política
- Beneficios financieros
- Ventaja competitiva
- Anarquía / caos
- Venganza / rencor
- Interrupción / inutilización / sabotaje
- Táctica / estrategia
- Social / moral
- Publicación de una declaración



##### **Objetivos**

- Daños y alteración de la información
- Propiedad intelectual
- Servicios
- Filtración de información sensible
- Imagen y reputación



##### **Impacto**

- Daños a la vida humana / seguridad
- Pérdida de ingresos / daños económicos
- Robo del protocolo de internet (IP, por sus siglas en inglés)
- Daños a la reputación
- Destrucción de infraestructura
- Demanda / incriminación
- Sanciones y restricciones
- Pérdida de confianza pública / de los inversores
- Daños a la continuidad funcional
- Calidad medioambiental
- Percepción

A fin de calcular la probabilidad, puede utilizarse el cuadro 5. Al usarlo, debe darse una puntuación del 1 al 4 para cada uno de los parámetros/criterios. En los parámetros com-

puestos por una serie de subapartados, debe darse a cada apartado su propia puntuación (del 1 al 4) y finalmente calcularse el promedio de las respuestas en todos los apartados.

**Cuadro 5.** Herramienta para calcular la probabilidad de acuerdo a los parámetros

Parámetro/criterio	Preguntas de ayuda
Historial de incidentes (valor entre 1 y 4)	¿Ha tenido lugar algún incidente en la organización y/o entre los proveedores de la organización en los últimos cinco años?
Inteligencia sobre ciberamenazas (valor entre 1 y 4)	¿Los hallazgos de la inteligencia en materia cibernética indican que la información que la organización posee constituye un objetivo de preferencia para un ataque?  ¿Los hallazgos de la inteligencia en materia cibernética indican que la organización y/o los proveedores de la organización y/u organizaciones en un sector de actividad similar en Israel/en otra parte del mundo constituyen un objetivo de preferencia para un ataque?
Superficie de ataque (valor entre 1 y 4)	¿Cuál es el nivel de seguridad física del proceso o activo? ¿Cuál es la política relativa a actualizaciones y parches de seguridad? ¿Cuál es el nivel de actualización del proceso/del activo? ¿Cuál es el nivel de compartimentación del sistema? ¿Existe acceso remoto al sistema? ¿Qué tipo de información contiene el sistema? ¿Cuál es la naturaleza de las interfaces del proceso o activo? ¿Cuántas interfaces tiene el sistema? ¿Quiénes son los usuarios humanos en el proceso/el activo? ¿Cuál es el número de usuarios (humanos, aplicaciones o computadoras) en el proceso/el activo?

La puntuación otorgada a cada uno de los parámetros debe colocarse en la fórmula que figura abajo. Debe tenerse en cuenta que puede darse a cada parámetro un coeficiente diferente en función de su importancia para la organización (la suma total de los coeficientes debe ser 1). En el ejemplo que se presenta a continuación, se ha dado mayor importancia al parámetro de la superficie de ataque (coeficiente 0,5), mientras que se ha considerado que el parámetro del historial de incidentes es de menor importancia (con un coeficiente de solo 0,2).

{0,5 x (puntuación de la superficie de ataque)

+

0,3 x (puntuación de inteligencia)

+

0,2 x (puntuación del historial de eventos)}

=

Probabilidad (likelihood)

**Cálculo del nivel de riesgo para el activo:**  
modo de ponderación de los datos

**Riesgo inherente (inherent risk):** se calcula al ponderar la intensidad de los daños potenciales (impact) derivados de la valencia del objetivo de protección y el grado de probabilidad de que tenga lugar un incidente cibernético en ese activo o proceso (likelihood). El cálculo

lo puede realizarse colocando los valores de intensidad/valencia (I) y de probabilidad (P) en la matriz que se presenta en el cuadro 6 (el riesgo es mayor a medida que aumenta el número y que el color cambia de verde a rojo).

**02**  
**Riesgo residual (residual risk):** debido a que las organizaciones implementan controles de protección, como la gestión de los privilegios de acceso, cifrado o monitorización, el nivel de riesgo al que se enfrentan en la práctica es menor que el nivel de riesgo inherente. Después de ponderar los controles existentes, el nivel de riesgo estará representado mediante el valor denominado riesgo residual.

En ocasiones, la organización podrá reducir el riesgo mediante una disminución del potencial de daños (impact), por ejemplo creando un sistema de copias de seguridad eficaz o adquiriendo un seguro cibernético. Sin embargo, en la mayoría de los casos, la organización reducirá el riesgo mediante una disminución del área de exposición y de la probabilidad de que se materialice un incidente cibernético, ya sea a través de la implementación de controles, tecnologías, procedimientos o procesos de protección.

Cuadro 6. Cálculo del nivel de riesgo de un activo

Probabilidad (P)				Impacto (I)
1	2	3	4	
7	10	13	16	4
6	9	12	15	3
5	8	11	14	2
4	7	10	13	1

A fin de calcular el riesgo residual, debe reducirse el nivel de riesgo (calculado en la matriz anterior) de acuerdo con el nivel efectivo de implementación de los controles existentes. De esta forma, el nivel de riesgo residual puede representarse mediante la siguiente fórmula:

(Impacto (I) x Probabilidad (P)) – Controles

A continuación, figuran dos ejemplos sobre cómo evaluar cuántos niveles se reducirá el riesgo de implementación de los controles:

- Una prueba que sugiera, por ejemplo, que la implementación de todos los controles reduciría el nivel de riesgo en dos niveles, mientras que una implementación del 50% de esos controles lo reduciría en un nivel.
- Realizar una reevaluación del riesgo (intensidad y probabilidad), partiendo de la base de que la organización implementará los controles que haya decidido integrar en el plan de mitigación de riesgos.

2.2 Evaluación del riesgo

Tras haber formulado una lista de riesgos y/o amenazas, con una clasificación según la prioridad de su tratamiento, deberá realizarse una estimación de cada uno de ellos en comparación con el nivel de riesgo aceptado por la organización.

**Riesgo objetivo.** Cuando el nivel de riesgo residual sea mayor que el nivel de riesgo aceptado por la organización (lo que se conoce como apetito de riesgo [*risk appetite*]), deberá elaborarse un plan de mitigación destinado a reducir el riesgo residual al nivel de riesgo deseado (a menos que la directiva hubiese optado por una estrategia de gestión de riesgos diferente, como su transferencia o aceptación).

Tras examinar la literatura profesional existente, se ha constatado que no existe un método y/o fórmula aceptados internacionalmente para calcular el riesgo objetivo. Por consiguiente, pueden utilizarse una de las dos alternativas presentadas a continuación:

01

Uso del método con el que la organización realice la gestión de riesgos (riesgos de cumplimiento, crédito, operaciones, etc.).

02

Empleo de pautas a establecer por la organización, como definir el riesgo máximo que la organización pueda soportar (por ejemplo, la decisión de no llegar a un riesgo con un nivel superior a 10), crear un plan para mitigar los riesgos que figuran en el mapa anterior a este valor y reducir los riesgos altos.

A fin de definir el riesgo objetivo y el apetito de riesgo en función del riesgo inherente, puede utilizarse una herramienta como la que se muestra en el cuadro 7.



**Cuadro 7.** Herramienta para definir el riesgo objetivo y apetito de riesgo

	Potencial de los daños			
	1	2	3	4
<b>Daños humanos</b>	Sin riesgo evidente	Peligro leve para la salud del entorno	Peligro grave para la salud de empleados o clientes	Peligro de pérdida de vidas humanas
<b>Daños económicos</b>	Costo de hasta US\$1,5 millones para la organización	Costo de US\$1,5 a 3 millones para la organización	Costo de más de US\$3 millones para la organización	Daños económicos estimados en más de US\$30 millones
<b>Daños funcionales</b>	Inversión de hasta dos meses de mano de obra para manejar el incidente hasta la vuelta a la normalidad. Daños leves para el servicio a los clientes y partes interesadas	Inversión de más de seis meses y menos de cinco años de mano de obra para manejar el incidente hasta la vuelta a la normalidad. Daños medianos para el servicio a los clientes y a las partes interesadas	Inversión de más de 5 años de mano de obra para manejar el incidente. La organización sufrirá un daño irreparable o daños graves y continuos para la continuidad operativa	Peligro de cierre para la organización como resultado del incidente
<b>Daños a la imagen</b>	No se esperan daños a la imagen considerables	La organización sufrirá daños a su imagen durante la gestión del incidente. Potencial de demandas colectivas	La organización perderá una ventaja competitiva y perderá su posicionamiento respecto de sus competidores y clientes	La organización perderá la confianza de sus clientes y sufrirá duras críticas públicas
<b>Daños sociales, medioambientales o públicos</b>	Daños leves a la continuidad del servicio a los clientes de la compañía	Daños medianos a los clientes o proveedores de la organización (cadena de suministro)	Daños graves a la privacidad de los empleados o clientes de la organización	Daños graves e irreversibles para el medio ambiente
<b>Daños a la confidencialidad de la información</b>	En caso de un ataque con <i>ransomware</i> que incluya el robo de información, los daños económicos se estiman en US\$500.000 a US\$1 millón	Temor de daños económicos debido a la pérdida de información a causa de una parte interna, con énfasis en aquellas personas con altos privilegios en el sistema de gestión de relaciones con clientes (CRM, por sus siglas en inglés) internacional	Filtración de toda la base de datos médica, que cause un daño irreversible a los clientes de la organización	
<b>Daños a la disponibilidad de la información y la continuidad operativa</b>	En caso de un ataque con <i>ransomware</i> , se estima que se requerirá una semana para la recuperación y para subir copias de seguridad. Habrá daños leves para la continuidad operativa		En caso de daños a la línea de producción (ICS) debido a un incidente cibernético, se esperan daños de decenas de millones de dólares, con un daño significativo para la continuidad operativa	
<b>Daños a la fiabilidad de la información y los datos</b>	Daños económicos que ascienden a cientos de miles de dólares como resultado de trabajar con información gestionada en aplicaciones que no permitan un registro de auditoría ( <i>audit trail</i> ), gestión de privilegios, gestión de versiones, etc. En caso de alterarse la información, se requerirán varios meses de trabajo para corregir y restaurar los datos	En caso de alterarse el proceso de presentación de informes a la bolsa y de alterarse los datos de los estados financieros, los daños a la organización incluirán daños a su imagen y un costo económico estimado en varios millones de dólares		Cancelación de pedidos de trabajo y contratos con la organización, hasta un riesgo de cierre, debido a la alteración de los datos en la base de datos principal de la organización, que contenga información de vital importancia para el servicio que se preste a los clientes

### 2.3 Evaluación de riesgos

En esta fase, se evaluarán los riesgos analizados y se decidirá cómo abordarlos.

La decisión debe tener en cuenta, entre otras cosas, las siguientes consideraciones: el nivel de criticidad del proceso comercial, la topología de la organización, los sistemas de información y proveedores de servicios o productos involucrados en los procesos críticos y la capacidad para responder y manejar los riesgos.

En esta fase, la organización tendrá un cuadro que resuma los riesgos identificados y clasificados, que podría parecerse al cuadro 8.

Al final de esta fase, la organización tendrá un mapa de amenazas / riesgos clasificados.

**Cuadro 8.** Resumen de los riesgos identificados y clasificados

Nombre del riesgo	Descripción del escenario	Probabilidad (puntuación 1-4)	Intensidad (puntuación 1-4)	Riesgo inherente (ponderación de intensidad y probabilidad)	Calidad de los controles existentes	Riesgo inherente
Pérdida de la ventaja competitiva como resultado de una fuga de información sensible	Extracción no autorizada de información por parte de un empleado de la organización mediante la instalación de una unidad de memoria portátil o el envío de un correo electrónico privado/comercial					
Pérdida de ingresos como resultado de una interrupción de la comunicación entre sucursales	Incidente con <i>ransomware</i> en la red de la organización					
Exposición jurídica debido al incumplimiento de una ley o normativa	Extracción no controlada de información por parte de un proveedor al subirla a un servicio de nube					
Pérdida de ingresos debido a la incapacidad de efectuar liquidaciones	Ataque DoS en el sitio web de la compañía					
Daños a la reputación como resultado de una filtración en un proveedor significativo para la organización	Aprovechamiento de una interfaz de acceso remoto a la organización de un proveedor de esta					

### Fase 3: tratamiento del riesgo

Por lo general, es imposible realizar una actividad sin exposición a riesgos.

La inversión en insumos para reducir el riesgo debe llevarse a cabo ponderando una serie de parámetros: examen del costo-beneficio económico para la organización; duración de la implementación; nivel de probabilidad de la materialización del riesgo; obligaciones legales de la organización en virtud de los contratos con proveedores y/o de leyes o normativas; consideraciones morales (como la responsabilidad social); y otros parámetros a decidir por la Dirección de la organización.

Al final de esta fase, la organización categorizará cada uno de los riesgos bajo una de las siguientes cuatro posibilidades que se utilizan habitualmente para tratar los riesgos en todo el mundo:

## 01

**Aceptación del riesgo (risk acceptance):** en caso de que el riesgo no sea alto, la organización podrá decidir realizar las actividades sin implementar controles de protección específicos. Una organización podrá decidir aceptar el riesgo, por ejemplo, en caso de que los pasos necesarios para reducirlo requieran más recursos que los que la organización esté dispuesta a invertir en relación con una amenaza concreta. Por ejemplo: es posible que una organización decida que el acceso a sus com-

putadoras se realice sin un proceso de identificación fuerte debido al costo necesario para la implementación de ese mecanismo o debido a que el riesgo de una fuga de información en el sistema haya sido estimado como bajo.

## 02

**Reducción del riesgo (risk reduction):** en caso de que la organización deba llevar a cabo una actividad a pesar de los riesgos latentes, podrá examinar la implementación de controles de protección que reduzcan la probabilidad de que se materialice un incidente cibernético. Por ejemplo: si la organización tiene puntos de venta que lleven a cabo liquidaciones mediante tarjeta de crédito, es habitual implementar controles de protección para reducir el riesgo de que se produzcan filtraciones de los datos de crédito. Estos controles pueden incluir mecanismos para impedir la conexión de dispositivos externos, la gestión de privilegios en las estaciones de trabajo, el cifrado de datos sensible, etcétera.

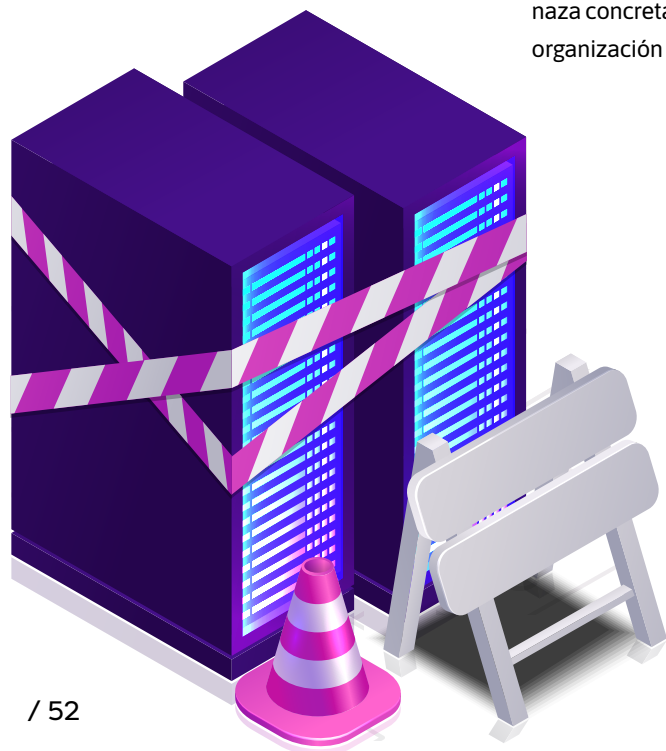
## 03

**Transferencia del riesgo (risk transfer):** en caso de que deba realizarse una actividad, pero la organización no esté interesada en adquirir los recursos de protección necesarios (conocimientos, herramientas, mano de obra, etc.), podrá transferir dicha actividad a un tercero. Por ejemplo: si una organiza-

ción deseara crear un sitio web o un perfil en las redes sociales, pero no dispusiera de los recursos necesarios para protegerlo, podrá transferir estas tareas a un subcontratista que cree el sitio web y/o el perfil y lo proteja. Otra opción para la transferencia del riesgo consiste en adquirir un seguro cibernético contra el riesgo en cuestión. Sin embargo, debe tenerse en cuenta que, a menudo, la ley no eximirá de responsabilidad a la organización en caso de producirse un incidente cibernético, como la fuga de datos personales.

## 04

**Evitación del riesgo (risk avoidance):** en caso de que el nivel de riesgo sea muy alto y la probabilidad de materialización sea alta, podrá decidirse evitar el riesgo “poniendo a cero la probabilidad de materialización”. Por ejemplo: si la Dirección de la organización comprende que no dispone de los conocimientos y herramientas para proteger una base de datos que quiere crear, es posible que decida no tener tal base de datos o no almacenar información muy sensible en ella.



## Implementación de controles de protección

Después de que la organización haya decidido cuáles son los activos/procesos en los que deben realizarse las actividades de mitigación de riesgos, deberán crearse controles de protección para ellos. Dichos controles incluirán procesos, productos y personas, que llevarán a cabo distintas actividades destinadas a reducir los riesgos cibernéticos para la organización, como gestión de usuarios, cifrado, monitorización, copias de seguridad, etc.

En el nivel de protección de cada activo/proceso influirá directamente su nivel de riesgo residual.


La rutina de ciberprotección incluirá la planificación, implementación y aplicación de controles de protección. Este capítulo forma la base de dicha rutina. Para su implementación, deberá emplearse el anexo 3 de la presente publicación y la lista de controles de la Metodología de Ciberdefensa para Organizaciones que puede encontrarse en el sitio web del Plan Cibernético Nacional.<sup>2</sup>

Generalmente, los distintos controles se presentan en un marco organizado en el que se reflejan las conexiones entre ellos (*framework*). El Plan Cibernético Nacional ha elaborado controles específicos que corresponden al esquema de amenazas actuales, los cuales se incorporan a un marco similar: el *Cyber Security Framework* (CSF) del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST, por sus siglas en inglés). Estos controles permiten aportar los conocimientos profesionales y la amplia experiencia acumulada en el sis-

tema cibernético local, a la vez que permiten que las organizaciones de la economía operen de conformidad con los marcos de trabajo habituales en todo el mundo.

Los controles de la Metodología de Ciberdefensa comprenden características únicas, tales como la profundidad de aplicación de la implementación, el énfasis en una implementación óptima de cada control, así como el énfasis y las evidencias necesarias para crear una infraestructura profesional conforme a este método.

**Cuadro 9.** Marco de controles de la Metodología de Ciberdefensa

Identificar	Proteger	Detectar	Responder	Recuperar
<ul style="list-style-type: none"><li>Responsabilidad de la Dirección</li><li>Gestión y evaluación de riesgos</li></ul>	<ul style="list-style-type: none"><li>Control de acceso</li><li>Protección de la información</li><li>Computación en la nube</li><li>Protección de los objetivos de protección</li><li>Protección de estaciones de trabajo y servidores</li><li>Protección física y del medio ambiente</li><li>Factor humano</li><li>Protección de entornos OT</li><li>Seguridad de la red</li><li>Criptografía</li></ul>	<ul style="list-style-type: none"><li>Metodología y procedimientos de trabajo para el monitoreo de la ciberprotección y la protección de la información proactiva (mapeo)</li><li>Recolección y protección de artefactos</li><li>Sistema de monitoreo central</li><li>Análisis</li></ul>	<ul style="list-style-type: none"><li>Gestión de incidentes e informes</li></ul>	<ul style="list-style-type: none"><li>Continuidad del negocio</li></ul> <div></div>

2. Véase la herramienta “ICDM Controls”, disponible en: [https://www.gov.il/en/departments/general/cyber\\_security\\_methodology\\_2](https://www.gov.il/en/departments/general/cyber_security_methodology_2)

A fin de decidir qué controles son pertinentes para un activo/proceso comercial en el que deba reducirse el nivel de riesgo, consúltase la lista de controles de protección en el anexo 3. Además, debe llevarse a cabo un proceso de análisis de brechas de protección (*gap analysis*), en el que se defina la profundidad de implementación requerida en cada uno de los controles pertinentes.

Al final de este proceso, la organización recibirá una lista de brechas de controles requeridos, en función de la profundidad de implementación pertinente.

Dado que los diferentes controles responden a riesgos y procesos distintos, en ocasiones las organizaciones optan por realizar una transición a controles “continuos” y, de hecho, los utilizan como lista de verificación (*checklist*).

El principal inconveniente de este método radica en que la organización examina los controles desde un punto de vista del cumplimiento y con base en su conformidad a una norma/regulación, y no desde un punto de vista basado en la gestión de riesgos (*risk based vs control based*).

Debido a que no todos los controles se implementan en la organización de la misma manera, y que no todos los controles son necesarios para cada proceso/activo, es preciso asegurarse de que se lleve a cabo una comprobación individual para los **objetivos de protección esenciales** para la organización. La experiencia muestra que, aunque en las organizaciones generalmente se implementan controles de manera transversal, a menudo no se implementan en un proceso/sistema específico.

Dado que no todos los controles son necesarios en cada activo, se debe emplear el nivel definido para cada activo en la fase 3 para centrarse en la lista de brechas. Esta lista constituirá la base para elaborar el plan de trabajo de la organización (fase 4).

Al final de esta fase, la organización tendrá una lista similar a la que se incluye en el cuadro 10.

Cuadro 10. Lista de controles

Control	Totalidad de la organización	Sistema CRM	Sistema de pago a proveedores
Debe implementarse una identificación multifactor para conectarse a cuentas con privilegios altos a través de la red, de acuerdo con la profundidad de implementación	Existe parcialmente	Existe	Debe implementarse
Deben definirse e implementarse medios de protección para localizar y alertar sobre cambios no autorizados en los ajustes de configuración, de acuerdo con la profundidad de implementación	Existe un proceso sistematizado en la organización	El sistema está en la nube y no tiene control directo sobre la implementación de este requisito, pero pueden imponerse requisitos al proveedor	Existe
Deben emplearse herramientas contractuales y jurídicas a la hora de adquirir un sistema de información o un servicio de proveedores, de acuerdo con la profundidad de implementación	No existe un proceso sistematizado para hacer firmar a los proveedores de la organización	Se ha hecho firmar una declaración al proveedor	Es un proveedor extranjero al que no se puede hacer firmar. Se examinarán los requisitos con respecto al acuerdo genérico con el proveedor

## Fase 4: creación de un plan de trabajo

Tras mapear los objetivos de protección y examinar los controles que deban implementarse en la organización para reducir el riesgo residual (en función de la profundidad de implementación seleccionada en cada caso), deberá llevarse a cabo un proceso de priorización y definirse un plan de trabajo para la implementación.

A fin de optimizar el orden de las acciones y maximizar el beneficio de los recursos asignados en el citado plan de trabajo, es recomendable tener en cuenta la visión del oponente. Cabe destacar que una parte considerable de la información requerida para completar esta fase debe obtenerse de la fase 2 “Cálculo del grado de probabilidad”.

Es posible realizar una clasificación simplificada de los atacantes y los ataques según la siguiente división:

### 01

**Origen del ataque:** parte interna en la organización, socio externo/tercero de la organización, parte externa a la organización.

### 02

**Causa del ataque/incidente:** accidental o intencional.

Esta división presentará a la organización una matriz que le permitirá centrarse en las amenazas que requieran una mayor atención; por ejemplo: un empleado interno que, maliciosamente, intente extraer información sensible de la organización; un proveedor de servicios externo que, accidentalmente, cause daños debido a un nivel de protección bajo; o un ataque externo destinado a causar daños a la organización u obtener otro beneficio.

Este enfoque permitirá a la organización centrarse en los puntos críticos y ayudará a clasificar las áreas de riesgo en las que no se hayan invertido recursos para hacer frente a los riesgos.



Un análisis de numerosos incidentes ha mostrado que la inmensa mayoría de los ciberataques utilizan uno de los siguientes canales:

### 01

Aprovechamiento de interfaces externas como un intérprete de comandos seguro (SSH, por sus siglas en inglés), protocolo de escritorio remoto (RDP, por sus siglas en inglés) o protocolo de transferencia de archivos (FTP, por sus siglas en inglés).

### 02

Introducción de un *software* malicioso mediante el envío de un correo electrónico con un archivo malicioso o un enlace a un sitio infectado.

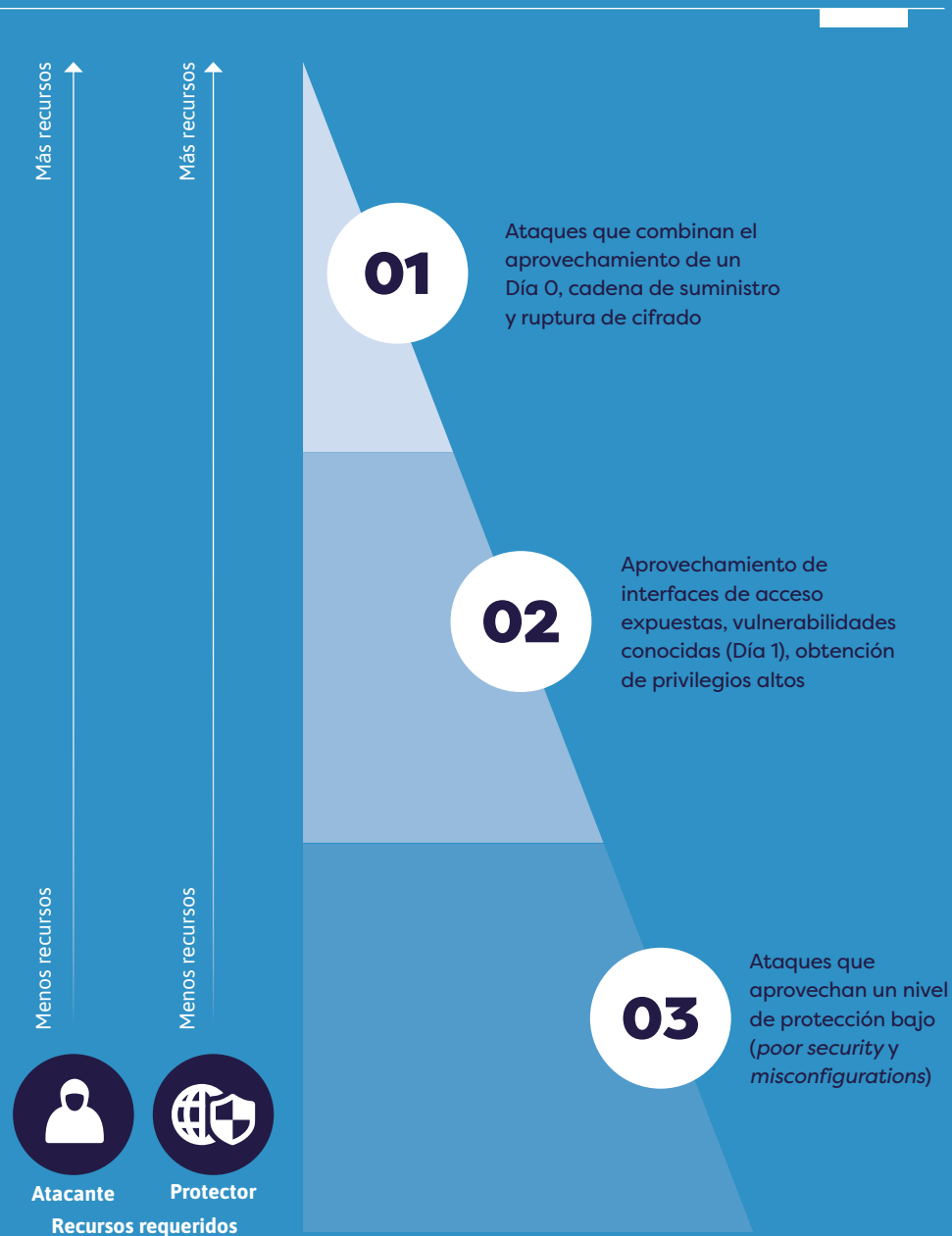
### 03

Navegación a sitios web infectados que descarguen un *malware* en la estación final.

Un ataque que no se realice directamente a través de Internet requiere que el atacante emplee numerosos recursos y recurra a medios adicionales, como el uso de ingeniería social, el aprovechamiento de la cadena de suministro o la obtención de accesibilidad física, entre otros. Debido a lo anterior, el ataque será más completo y costoso.

Una contemplación desde este punto de vista permitirá a la organización priorizar iniciativas que dificulten al atacante la obtención de acceso y la toma de control de la red de la organización. Tales iniciativas pueden incluir, entre otras cosas, la protección de las interfaces (por ejemplo, mediante la implementación de identificación multifactor [MFA, por sus siglas en inglés]), la protección del servidor de correo electrónico (por ejemplo, mediante *mail relay*, caja de arena [*sandbox*]) y la securización de las interfaces a fin de minimizar el uso de protocolos peligrosos.

La implementación de procesos de securización y medios de protección para estas rutas puede dar respuesta a las dos capas inferiores que se muestran en la pirámide del gráfico 7.

**Gráfico 7.** Ataques y aprovechamiento de vulnerabilidades

Debe tenerse en cuenta que diferentes organizaciones tienen riesgos cibernéticos distintos, derivados de la naturaleza y características únicas de la organización. Por ejemplo, una organización cuya principal fuente de ingresos sea su sitio web podrá preferir invertir en medios de protección para dicho sitio web (tales como antiataques de denegación de servicio distribuido [DDoS, por sus siglas en inglés] o cortafuegos para aplicaciones web [WAF, por sus siglas en inglés]) antes de proceder a proteger las bandejas de correo electrónico de la organización.

**Sin embargo, se ha constatado que, para la mayoría de las organizaciones en todo el mundo, la protección de los canales de entrada de Internet en las distintas interfaces es la base mínima necesaria para hacer frente a la mayoría de los tipos de ataques.**

La mejora continua del nivel de resiliencia de la organización frente a una amenaza de referencia a la que se enfrente puede verse reflejada en la adopción e implementación de controles de un nivel superior (como los controles de los niveles 3 y 4). Dicha mejora también puede verse reflejada en la profundización de la eficacia de los controles (profundidad de implementación del control).

## Formulación y adopción de un concepto avanzado para hacer frente a amenazas avanzadas

Una organización que deba hacer frente a amenazas más avanzadas, a menudo relacionadas con grupos de ataque avanzados o agentes estatales, deberá realizar una planificación basada en un **concepto de protección** más complejo.

Este concepto de protección avanzado abordará aspectos como la capacidad de la organización de crear disuasión en el ciberespacio, su política con respecto a la búsqueda de amenazas, la inteligencia proactiva, los programas de recompensa por la localización de errores (*bug bounty*) y los cambios en la topología de protección y los procesos que se lleven a cabo en la organización. Este enfoque requiere madurez organizacional y un diálogo con la Dirección con respecto al concepto de la organización para hacer frente a las amenazas cibernéticas de manera avanzada. Por ejemplo, el uso de mecanismos alternativos y redundancia de la infraestructura tecnológica podría permitir a una organización cuyo sitio web haya caído continuar brindando servicio o información de manera continua, sin interrupción de su actividad comercial.

En el anexo 7 se enumeran ejemplos de componentes en el desarrollo de un concepto de protección para la organización.

## Fase 5: auditorías y control continuo

La gestión de riesgos es un proceso que comprende una serie de fases de trabajo establecidas que se deben llevar a cabo en ciclos a lo largo de los años. Su finalidad es actualizar periódicamente el mapa de riesgos y las respuestas requeridas para ellos. Esta actualización es importante, entre otras cosas, por la implementación de controles de protección y por los cambios en el espacio interno y externo de la organización.

Asimismo, las organizaciones deben trabajar para incrementar su nivel de resiliencia cibernética a lo largo de los años mediante la adopción de procesos de mejora continua.

Debido a que la realización de un estudio de riesgos integral en la organización y la implementación de los pasos requeridos tras dicho estudio llevan mucho tiempo, en numerosas organizaciones este proceso puede ser tal y como se muestra en el gráfico 8.

**Gráfico 8.** Ciclo de mejora continua



A lo largo de varios meses se lleva a cabo un proceso de evaluación de los riesgos de la organización, tras lo cual se presentan a la Dirección el mapa de riesgos y los pasos requeridos para reducirlos (el plan de trabajo). Estos pasos constituyen la base para planificar el presupuesto y el plan de trabajo que las partes responsables de ciberprotección en la organización aplicarán durante los años siguientes. Este plan puede incluir, entre otras cosas, la necesidad de poner en marcha procesos de adquisición y la implementación de tecnologías de protección y de distintos procedimientos en la organización.

Este proceso no es exclusivo de la gestión de riesgos cibernéticos y también es habitual en muchos otros ámbitos en los que la organización gestione sus riesgos (como los riesgos de cumplimiento o los operativos).

Dado que el ritmo de los cambios es un factor crítico en el mundo digital, particularmente en el ámbito de la ciberprotección y los ciberataques, las organizaciones deben desarrollar su capacidad de realizar auditorías y controles de forma rápida y flexible. El objetivo de esto es que puedan responder en cualquier momento a la pregunta de **hasta qué punto la organización está protegida contra amenazas cibernéticas y cuáles son los pasos inmediatos que se tomarán a fin de minimizar dichos riesgos**.

Junto con la planificación presupuestaria, contratación y formación de empleados y procesos a largo plazo derivados de un estudio de riesgos transversal, la organización deberá desarrollar **simultáneamente** su capacidad de realizar auditorías y controles continuos de forma independiente. Esta capacidad se conoce como control y monitoreo continuo (CMC).

A fin de desarrollar la capacidad de CMC e implementarla de manera eficaz, la organización deberá formular un concepto que incluya, entre otros, los siguientes aspectos:

# 01

Análisis de la forma en que la organización esté protegida contra ataques que se originen en la cadena de suministro (*supply chain risk management*).

# 02

Evaluación de la forma en que la organización esté protegida contra ataques que se originen en activos digitales sobre los que no tenga control operativo o tecnológico (*digital risk protection* y todo como servicio [XaaS, por sus siglas en inglés]).

## 03

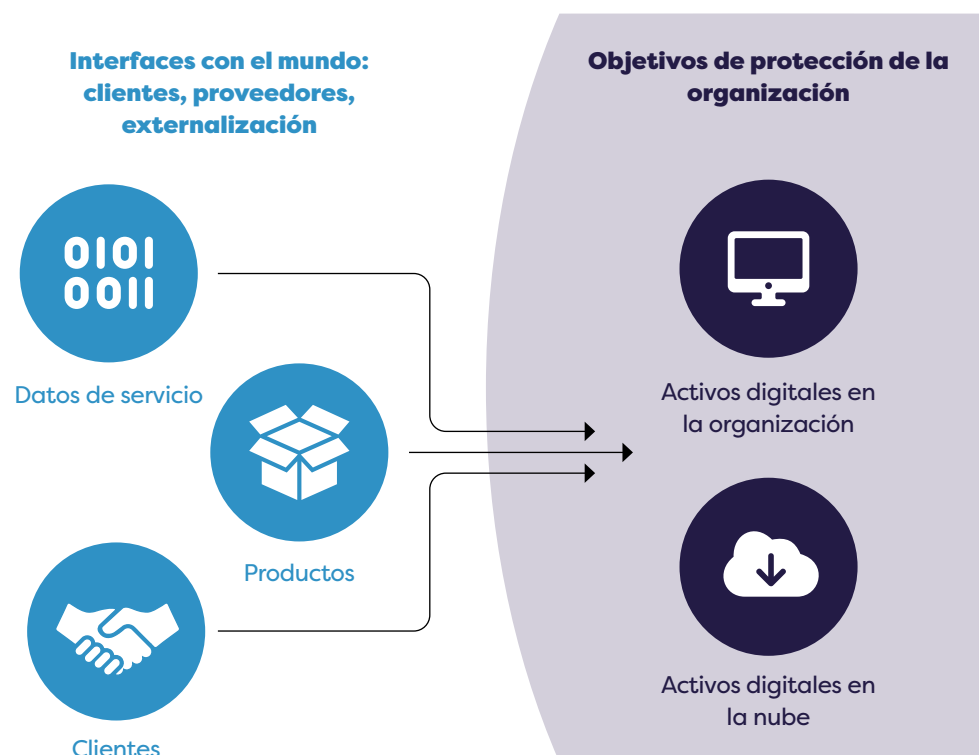
Análisis de la forma en que la organización está protegida contra ataques que se originen en su superficie de exposición, teniendo en cuenta las intenciones y capacidades desde el punto de vista del oponente. Esto se ve reflejado principalmente en la superficie de exposición (*attack surface management*)

y en la detección de vulnerabilidades (*vulnerability scanning* y *breach attack simulator*).

## 04

Monitoreo 24/7 (las 24 horas del día, los 7 días de la semana) de la infraestructura y los sistemas, ya sea de manera independiente o mediante servicios de externalización.

**Gráfico 9.** Visión integral de los riesgos cibernéticos en la organización



En el pasado, la mayoría de los esfuerzos en materia de protección se basaban en una visión de la organización como una unidad orgánica cerrada y delimitada. La aceleración del uso de la nube, unido a la creciente dependencia de proveedores de servicios y productos, ha difuminado los límites de la organización. En la actualidad, los activos digitales que utilizan las organizaciones, como las redes sociales, los servicios de almacenamiento, los sistemas CRM y de planificación de recursos empresariales (ERP, por sus siglas en inglés) e incluso los servicios de correo electrónico, se proporcionan en una configuración de *software* como servicio (SaaS, por sus siglas en inglés). Esta nueva realidad obliga a las organizaciones a examinar de manera integral sus riesgos cibernéticos internos y externos, así como su capacidad de monitorización, de respuesta y de recuperación.

**Por lo general, esta información es gestionada por una serie de herramientas y servicios en la organización, entre los que se encuentran los siguientes:**

## 01

Sistemas para la gestión de riesgos cibernéticos en la cadena de suministro (VRM, por sus siglas en inglés).

## 02

Sistemas para la recopilación de inteligencia cibernética (CTI, por sus siglas en inglés) y para la gestión de la protección de activos digitales (DRP, por sus siglas en inglés), como cuentas de usuario en las redes sociales.

## 03

Sistemas para el mapeo de la superficie de exposición de la organización (ASM, por sus siglas en inglés).

## 04

Sistemas para el estudio de simulaciones de ataque (BAS, por sus siglas en inglés).

Una implementación eficaz de este plan proporcionará a la organización una imagen de espejo que reflejará su nivel de resiliencia, también desde el punto de vista del atacante. Dicha imagen de espejo permitirá mostrar a la Dirección el nivel de madurez y preparación en distintos ámbitos de contenido, así como priorizar adecuadamente las amenazas y vulnerabilidades.

**Gráfico 10.** Proceso de materialización de un ataque

### Descripción del proceso de ataque según el método de la cadena de ciberataque (*cyber kill chain*)

Mientras que la parte encargada de la protección trabaja para reducir la superficie de ataque en todos los canales e implementa controles de protección, como cifrado, identificación fuerte o securización de las estaciones finales, la parte atacante puede conformarse con localizar una única ruta de entrada.

Debido a esta asimetría entre la parte encargada de la protección y el atacante, es importante crear un mecanismo de priorización de tareas.

La securización de **todas** las estaciones de trabajo **todo el tiempo**, la actualización de todos los parches de seguridad pertinentes y la difusión de avisos a todos los empleados y proveedores requieren numerosos recursos.

A fin de aprovechar de forma efectiva los recursos de la organización, se precisa la capacidad de crear en tiempo real un informe actualizado del mapa de posibilidades del atacante para llevar a cabo el ataque. Este informe deberá contar con una clasificación que permita obtener el valor máximo que posibiliten los recursos asignados a la protección. Esta clasificación puede basarse en los siguientes parámetros:

## 01

**En el eje humano:** ¿Quiénes son las personas con los privilegios más altos en la organización? ¿Quiénes son las partes con un alto perfil de exposición a los medios?

## 02

**En el eje tecnológico:** ¿Cuáles son los sistemas externalizados a Internet? ¿Cuáles son las tecnologías que utiliza la organización y de las que cualquier parte en la economía puede tener conocimiento?

## 03

**En el eje de procesos:** ¿Qué proyectos han recibido una amplia cobertura mediática? ¿Cuáles son los procesos con un mayor impacto en la percepción pública o en las actividades comerciales de la organización?

Un análisis de la información sobre las personas, procesos y sistemas de la organización (con los que el oponente pueda querer hacerse para planificar su ataque) puede ayudar a la hora de priorizar los esfuerzos de protección y poner obstáculos al atacante en la fase de recopilación (*passive & active recon*).

**Gráfico 11.** Elementos de información comunes que el atacante podría buscar en la fase de preparación para el ataque (*recon*)



**Nota:** DNS: servicio de traducción de direcciones (siglas en inglés).

En el anexo 4 se incluyen herramientas y métodos recomendados para la implementación del principio de control continuo.

# Anexos

## Anexo 1. Controles de protección para una organización de la categoría A

**Cuadro A1.1.** Aspectos destacados para el profesional informático

Familia	Apartado	Control	Explicación complementaria
Responsabilidad de la Dirección	Gobernanza corporativa	Debe examinarse periódicamente el enfoque de la organización para gestionar la seguridad de la información y la ciberprotección, así como su modo de implementación.	Deben examinarse los controles de seguridad implementados en la organización, las políticas de seguridad de la información y la protección de los procesos comerciales críticos para la organización.
Prevención de código malicioso	Detección y prevención de códigos maliciosos en las estaciones finales y los servidores de la organización	Deben implementarse las herramientas apropiadas para detectar y prevenir códigos maliciosos en las estaciones finales y los servidores de la organización. Dichas herramientas serán activadas en forma de protección activa y se llevarán a cabo análisis periódicos.	Debido a que algunos atacantes pueden infiltrarse a través de los mecanismos de seguridad, es necesario asegurarse de que los controles para el tratamiento de código malicioso también sean implementados a nivel de las estaciones de trabajo.

Familia	Apartado	Control	Explicación complementaria
Prevención de código malicioso	Actualizaciones automáticas	Debe habilitarse la actualización automática de todos los sistemas destinados a detectar y prevenir código malicioso en la organización.	La organización realizará una actualización automática desde un servidor central gestionado por la organización o por un proveedor de servicios conocido. Estas actualizaciones asegurarán que las herramientas de protección se actualicen de forma constante.
Cifrado	Criterios para el cifrado	Deben definirse los usos que requieran cifrado y el tipo de cifrado necesario de acuerdo con las distintas leyes, directrices, procedimientos, regulaciones y obligaciones comerciales.	La organización establecerá cuáles son los sistemas y la información por cifrar y documentará la configuración del cifrado de la información. Los requisitos pertinentes se derivarán de aquellos que se apliquen a la organización o a los criterios para guardar la información.
Protección de las estaciones de trabajo y los servidores	Política de securización	Deben definirse, documentarse e implementarse políticas de securización para las estaciones de trabajo y los servidores, que den respuesta a los requisitos de seguridad de la información de la organización.	La organización establecerá los requisitos de securización para los sistemas de la organización, enfatizando en los requisitos básicos, la frecuencia de las actualizaciones y el nivel de categorización. Después de esto, se deberán documentar los requisitos en un marco superior, que servirá como base para la elaboración de procedimientos de securización.

Familia	Apartado	Control	Explicación complementaria
Protección de las estaciones de trabajo y los servidores	Implementación de la securización	Deben configurarse los ajustes del sistema para que proporcionen la funcionalidad mínima necesaria, a la vez que se bloquean funciones, puertos y protocolos que no sean necesarios.	<p>La organización establecerá procedimientos de securización para cada tipo de sistema y servidor con base en prácticas aceptadas, de tal forma que incluyan al menos:</p> <ul style="list-style-type: none"> <li>• Reducción de la superficie de ataque del sistema mediante el bloqueo de puertos innecesarios.</li> <li>• Apagado de servicios innecesarios.</li> <li>• Eliminación de cuentas de usuarios visitantes.</li> <li>• Preferencia por el uso de protocolos seguros en la comunicación entre los servidores.</li> <li>• Recepción de actualizaciones de forma organizada.</li> <li>• Bloqueo de funciones sensibles del sistema.</li> <li>• Envío de registros sobre incidentes del sistema a un servidor de monitoreo.</li> <li>• Bloqueo de la instalación de <i>software</i> por parte de usuarios no autorizados.</li> </ul>

Familia	Apartado	Control	Explicación complementaria
Computación de la nube pública	Responsabilidad compartida	Debe comprenderse la división de responsabilidad de la seguridad del servicio entre el proveedor de servicios y la organización, y también, implementarse los controles de protección correspondientes.	Al utilizar servicios en la nube pública, existirá una división de responsabilidad de la ciberprotección entre asuntos que sean responsabilidad del proveedor y aquellos que sean responsabilidad del cliente. Dicha división de responsabilidad dependerá de la naturaleza del servicio y del modelo de implementación. La organización deberá comprender los asuntos que sean su responsabilidad y poner en práctica las implicaciones de tal responsabilidad.
Computación de la nube pública	Intercambio de información sensible	Debe asegurarse de que no se transfieran al servicio en la nube los datos que la regulación y las obligaciones de la organización prohíban transferir.	Existen datos que la organización tiene prohibido transferir a un servicio en la nube para su procesamiento o su almacenamiento, con base en las regulaciones o compromisos con terceros. Antes de transferir datos a la nube, deberá asegurarse de que no formen parte de esta categoría.
Protección de la información	Protección de la información almacenada en recursos compartidos	Debe evitarse la transmisión no autorizada o involuntaria de información a través de recursos compartidos del sistema.	La organización deberá prevenir y hacer frente a la transferencia de información no autorizada a través de carpetas compartidas, correo electrónico, medios extraíbles, etc.

Familia	Apartado	Control	Explicación complementaria
Seguridad de la red	Gestión de conexiones (sessions) a nivel de servidor	La organización debe utilizar medios tecnológicos para proteger sus servicios contra posibles ataques DoS.	Deberá protegerse contra diferentes tipos de ataques DoS, como la sobrecarga de recursos informáticos hasta provocar su falla, la sobrecarga del ancho de banda o la sobrecarga de un sitio web hasta provocar su falla.
Seguridad de la red	Fiabilidad de la conexión (sessions)	Debe asegurarse de que el servicio DNS sea proporcionado por un servidor fiable (dentro o fuera de la organización).	La organización únicamente aceptará un servicio DNS de un servidor interno seguro, a fin de prevenir rutas de comunicación erróneas (accidental o intencionalmente) a destinos hostiles.
Seguridad de la red	Límites de la red	Debe limitarse el número de canales de comunicaciones externos al sistema.	La organización reducirá y unificará los canales de comunicación a fin de asegurar un control adecuado de las conexiones al sistema.
Seguridad de la red	Límites de la red	Debe bloquearse todo el tráfico de la red de forma predeterminada y permitirse manualmente el tráfico deseado por medio de una regla de excepción.	La organización establecerá las reglas de filtrado del tráfico de la red de modo que bloquee de forma predeterminada cualquier tráfico que no haya sido definido expresamente como permitido.
Seguridad de la red	Límites de la red	Deben usarse direcciones de red separadas (subred diferente) para conectarse a los sistemas en zonas de seguridad diferentes.	La organización establecerá que cada subred tenga un rango de direcciones separado que se publicará en el cortafuegos y los enrutadores.

Familia	Apartado	Control	Explicación complementaria
Control de acceso	Gestión de usuarios	Deben configurarse cuentas de usuario que sean compatibles con las funciones comerciales de la organización.	Al menos, deberá separarse una cuenta de “administrador” de una cuenta de “usuario”. Además, deberán establecerse usuarios que gestionen las funciones de seguridad en el sistema (como la creación de usuarios, gestión de privilegios de acceso y del sistema, o gestión del sistema de seguridad de la información).
Control de acceso	Gestión de permisos	Deben establecerse y aplicarse privilegios de acceso lógicos al sistema y a la información de acuerdo con la política de control de acceso existente.	El control de acceso podrá tener lugar a nivel personal ( <i>identity-based</i> ) o a nivel de cargo ( <i>role-based</i> ), con el objetivo de controlar el acceso de entidades (usuarios o procesos informáticos) a objetos (archivos, registros, dispositivos, etc.).
Recursos humanos y concienciación de los empleados	Reglas de conducta de los empleados	Deben definirse reglas de conducta al trabajar con los sistemas de información de la organización. Dichas reglas establecen los ámbitos de responsabilidad y las reglas para un uso adecuado, haciendo énfasis en los sistemas sensibles.	La organización establecerá procedimientos relativos a la conducta al trabajar con los sistemas de información y los distribuirá entre todos los empleados.

Familia	Apartado	Control	Explicación complementaria
Recursos humanos y concienciación de los empleados	Gestión de privilegios al contratar, cambiar de puesto o irse de vacaciones largas (como un expediente de regulación temporal de empleo [ERTE] o bajas por maternidad) o al dejar la organización	Deben revisarse y actualizarse los privilegios de acceso de los empleados al cambiar de un puesto a otro.	Deberá establecerse un proceso de actualización en relación con la movilidad de los empleados y el cambio de privilegios de acuerdo con el nuevo puesto (eliminación de privilegios innecesarios y creación de los privilegios necesarios para el nuevo puesto). Deberán abordarse diferentes formas de contratación, por ejemplo: proveedores frente a empleados de la organización o empleados de la organización frente a externalización.
Seguridad en la adquisición y el desarrollo	Requisitos de seguridad en el contexto de las adquisiciones y desarrollo de sistemas	Seguridad de la cadena de suministro: debe exigirse a los proveedores de servicios que cumplan con los distintos requisitos, regulaciones, estándares y directrices de la organización.	La organización se asegurará de que los proveedores de servicios cumplan con los requisitos de cumplimiento ( <i>compliance</i> ) de la organización, así como con los requisitos de las normativas de los países en los que opere la organización.
Protección física y del entorno	Iluminación de emergencia	Debe instalarse y mantenerse un sistema de iluminación de emergencia automático, que se activará en caso de producirse un corte de electricidad o un mal funcionamiento. El sistema incluirá las salidas de emergencia y las vías de evacuación en las instalaciones.	

Familia	Apartado	Control	Explicación complementaria
Protección física y del entorno	Protección contra incendios	A fin de mantener los sistemas de información, deben instalarse y mantenerse sistemas de detección y extinción de incendios, que deben estar respaldados por una fuente de energía independiente.	
Documentación y monitoreo	Mecanismo de documentación	Debe activarse un mecanismo que cree registros de control sobre incidentes en los sistemas de la organización. Deben realizarse registros, al menos, de los incidentes de sistemas que contengan información sensible sobre clientes, sistemas críticos para el funcionamiento de la organización y sistemas centrales (servidores, componentes de comunicación, aplicaciones, bases de datos, etc.).	La organización se asegurará de que los sistemas de infraestructura y los sistemas de aplicaciones activen un mecanismo de registro de incidentes, así como que estos se guarden durante el período de tiempo establecido. Los registros de control contendrán información como el tipo de incidente, cuando tenga lugar, su origen y el nombre del usuario. En cualquier caso, deberán monitorearse los sistemas que procesen información sensible, que formen parte de la infraestructura crítica de la organización o que gestionen los procesos centrales de la organización.
Documentación y monitoreo	Mecanismo de documentación	Los mecanismos de registro deben incluir, como mínimo, información sobre la naturaleza de la acción realizada, la firma de tiempo, el origen y el destino de la acción, la identificación del usuario, la identificación del proceso, si fue una falla/éxito y el nombre del archivo involucrado.	

Familia	Apartado	Control	Explicación complementaria
Gestión de incidentes e informes	Tratamiento de incidentes cibernéticos y seguridad de la información	Deben establecerse canales de comunicación entre los empleados y los responsables a fin de informar sobre sospechas de incidentes de seguridad.	La organización aplicará procedimientos que definan los incidentes cibernéticos que requieran reportes y determinarán cómo informar sobre ellos.
Continuidad del negocio	Disponibilidad de los recursos	Deben realizarse copias de seguridad a nivel de usuario, sistema y documentación del sistema, y asegurar que las copias de seguridad estén protegidas.	La organización realizará una copia de seguridad de toda la información crítica en los sistemas de información que respalden los procesos comerciales y garantizará la disponibilidad, integridad y fiabilidad de dichas copias de seguridad.



## Anexo 2. Ejemplos de amenazas y vulnerabilidades

Es posible clasificar todos los incidentes cibernéticos en función del origen del ataque (una parte interna, un proveedor o una parte externa) y la motivación del ataque (intencional o accidental). A continuación, se presentan ejemplos de distintos incidentes, clasificados según lo mencionado.

Así, por ejemplo, un archivo con información sensible puede ser filtrado de forma accidental o intencional por un empleado de la organización, por un proveedor y/o por un atacante.

El cálculo del **riesgo** cibernético requiere ponderar **las vulnerabilidades y amenazas** para la organización. Ejemplos de vulnerabilidades son: la ausencia de un mecanismo de gestión de privilegios, la falta de un mecanismo de bloqueo automático de la computadora tras un período de inactividad o un mecanismo de identificación débil. Existirá una amenaza cuando haya una parte que

pueda aprovechar esta vulnerabilidad en la organización; por ejemplo, un empleado interno que se vale de sus privilegios altos, un atacante que aprovecha un mecanismo de restablecimiento de contraseña débil o un proveedor que se beneficia su acceso a información sensible.

**Al calcular el riesgo, debe examinarse el grado de motivación y la probabilidad de que la amenaza se materialice, teniendo en consideración tanto su prevalencia como su capacidad para ponerla en práctica (explotando una o más de las citadas vulnerabilidades).**



**Gráfico A2.1.** La parte involucrada en el incidente cibernético frente a la motivación del incidente



Cuadro A2.1. Lista de ejemplos de amenazas y vulnerabilidades

Parte involucrada en la amenaza	Forma de materialización	Daños potenciales	Escenarios
Atacante remoto	Escuchas remotas	Teléfono IP interno	Activación de forma remota del micrófono en el teléfono IP
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Correo electrónico	Archivo infectado adjunto a un mensaje
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Correo electrónico	Implementación de un enlace a un servidor infectado como parte de un mensaje
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Correo electrónico	Implementación de un código hostil en la organización mediante un mensaje
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Entrada de la comunicación	Aprovechamiento de vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés)
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Entrada de la comunicación	Uso de una cuenta de gestión
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Servicios web	Aprovechamiento de una vulnerabilidad
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Servicios web	Introducción de un código hostil

Parte involucrada en la amenaza	Forma de materialización	Daños potenciales	Escenarios
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Propagación por el servidor de correo electrónico de la organización	Aprovechamiento de CVE
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Propagación por el servidor de correo electrónico de la organización	Uso de una cuenta de gestión
Atacante remoto	Penetración desde Internet directamente a la red de la organización	Propagación por el servidor de correo electrónico de la organización	Infección de una computadora mediante la navegación a un servidor infectado
Empleados	Maliciosa	Empleado con rencor	Uso de sus privilegios legítimos en acciones para las que esté autorizado
Empleados	Maliciosa	Empleado con rencor	Uso de sus privilegios legítimos en acciones para las que no esté autorizado o para acceder a información no destinada a él
Empleados	Maliciosa	Empleado con rencor	Uso de la cuenta de otro empleado para realizar acciones para las que esté o no autorizado
Empleados	Maliciosa	Empleado con rencor	Uso de herramientas de gestión legítimas en la cuenta del empleado
Empleados	Accidental	Ingeniería social a un empleado interno	Infección de la computadora de un empleado por medios web (correo electrónico, navegación)

Parte involucrada en la amenaza	Forma de materialización	Daños potenciales	Escenarios
Empleados	Accidental	Negligencia profesional	Creación de un enlace no seguro entre servidores separados
Empleados	Accidental	Negligencia profesional	Configuración o securización insuficiente/incorrecta de medios de seguridad e informáticos
Empleados	Accidental	Indisciplina	Conexión de equipos infectados a la computadora
Empleados	Accidental	Indisciplina	Conexión de una computadora separada a Internet

Las organizaciones que se enfrenten a ataques avanzados deberán estar preparadas para hacer frente a técnicas tales como las siguientes:

# 01

La desactivación de productos de protección en la organización, como antivirus o *endpoint detection and response* (EDR), a fin de ejecutar *software* malicioso más adelante. Este escenario puede materializarse, entre otras cosas, por medio de:

- Inicio de la computadora en modo seguro (*safe mode*), destinado a restaurar el sistema operativo en caso de producirse una falla, ya que la mayoría de los programas antivirus no se ejecutan en dicho modo.

- Desactivación de productos de seguridad mediante la instalación de *software* con acceso *Kernel* y aprovechando las vulnerabilidades existentes en este.
- Desactivación de productos de seguridad mediante un *software* malicioso que contenga un código para finalizar procesos (*processes killing*).
- Evitación de productos de seguridad mediante el uso de una máquina virtual.
- Firma de los archivos de *software* malicioso por medio de certificados digitales legítimos.
- Uso de un ataque *fileless*.

# 02

El aprovechamiento de programas de *software* y herramientas legítimos instalados en la computadora de la víctima por iniciativa propia, o instalados como parte de una herramienta del sistema operativo (*living off the land*), de modo que su uso por parte de los atacantes no levante sospechas. Hacer frente a este escenario no es sencillo, por varios motivos:

- El ataque se lleva a cabo por medio de productos listos para usar (COTS, por sus siglas en inglés) y *software* instalado previamente en la computadora de la víctima, sin ninguna instalación de archivos binarios por parte del atacante.
- Dado que a menudo estas herramientas son instaladas por gerentes del sistema para realizar acciones legítimas, resulta difícil bloquear el acceso a ellas e identificar posibles ataques. Además, aunque se detecte un ataque, resulta difícil asignarlo a un grupo de ataques concreto, ya que todos los grupos de ataques emplean herramientas existentes en lugar de herramientas desarrolladas por ellos mismos. Este tipo de ataque puede realizarse, entre otras cosas, utilizando documentos que contengan macros, *scripts*, o bien mediante el uso de una interfaz de comandos como una Interfaz de línea de comandos (CLI, por sus siglas en inglés).

Es posible hacer frente al aprovechamiento de programas de *software* y herramientas legítimas tal como se detalla en los capítulos sobre controles de esta Metodología de Ciberdefensa. Sin embargo, ello requiere hacer énfasis en ellos y una implementación avanzada en la organización. Asimismo, es importante establecer un conjunto de señales que lleven a investigar las sospechas de que se esté produciendo un incidente. Estas señales pueden incluir la adición de un usuario al grupo *Domain admin*, el cambio frecuente de las extensiones de los archivos, el intento de consultar servidores DNS y de protocolo de tiempo por red (NTP, por sus siglas en inglés) que no sean los servidores oficiales de la organización o la eliminación de registros.

Puede encontrarse una ampliación sobre los tipos de amenazas comunes en las fuentes aceptadas en este ámbito, como el Anexo D en la norma ISO 27005 o el proyecto MITRE.<sup>3</sup> El grado de vulnerabilidad puede calcularse con ayuda de herramientas como la calculadora *Common Vulnerability Scoring System* (CVSS),<sup>4</sup> que pondera distintos parámetros.

Las entidades que reciban asesoramiento u orientación por parte del Plan Cibernético Nacional podrán recibir una lista más actualizada con ejemplos de amenazas y vulnerabilidades.

3. Puede encontrarse más información disponible en: <http://attack.mitre.org/>

4. Para leer más sobre CVSS, visítese <http://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

## Anexo 3. Banco de controles

El propósito del banco de controles es unificar las recomendaciones en materia de ciberprotección en los distintos ámbitos. El banco de controles deberá actualizarse con frecuencia, en función del desarrollo de la tecnología y las amenazas derivadas de esta.

### Estructura del banco de controles

El banco de controles debe crearse en forma de cuadro. Las columnas principales incluidas en él serán las siguientes:

# 01

**Función:** uno de los cinco ámbitos principales en los que se divide la ciberprotección: identificar, responder, detectar, proteger y recuperar. Estas funciones se crearán de acuerdo con el marco NIST CSF.

# 02

**Asunto y asunto secundario:** estas columnas incluirán la familia del control y los apartados incluidos en ella. Por ejemplo, la familia Protección de la nube pública podrá incluir asuntos secundarios como la gestión de cambios en la nube, el trabajo con una nube híbrida o la continuidad operativa del trabajo en la nube.

# 03

**Control:** la propia recomendación de protección, que debe implementarse para efectuar el proceso de gestión de riesgos. Los controles incluirán recomendaciones como el nombramiento de un responsable de protección, la protección del navegador o la realización de actividades de monitoreo.

# 04

**Énfasis en la implementación del control:** para minimizar el alcance de la explicación, esta columna también podrá incluir un desglose de los conocimientos y los aspectos destacados que ayuden a implementar la recomendación de protección de forma adecuada y eficaz.

# 05

**Evidencias requeridas:** la documentación que deba presentarse a la parte solicitante para demostrar que realmente se esté implementando la recomendación de protección según lo requerido. Estas medidas respaldarán los procesos de auditoría y podrán resultar de ayuda para preparar la infraestructura para su certificación.

# 06

**Nivel de objetivo de control:** para cada recomendación de protección, se establecerá un nivel en un eje entre el 1 y el 4, donde 1 representa un control básico y 4 un control de deba implementarse donde el potencial de daños sea más considerable. Esta clasificación está destinada a servir de apoyo para

tomar decisiones cuando se considera si debe implementarse el control en un objetivo de protección en concreto, ya que no todos los controles se implementan de forma idéntica en todos los procesos y sistemas de la organización. Por otra parte, esta división ayudará a crear una diferenciación para una mayor proporcionalidad, de modo que las organizaciones puedan comenzar con la implementación de controles básicos y, a continuación, examinar la implementación de controles más avanzados y complejos.



# 07

**Profundidad de la aplicación/control de nivel X:** es posible implementar cada control en diferentes niveles de madurez y profundidad. Por ejemplo, la implementación de un sistema para prevenir las fugas de información puede realizarse únicamente a un nivel básico (adquisición de un producto y su implementación básica), pero también de una manera integral que tenga en cuenta las limitaciones de la organización, la clasificación de la información, la adaptación a los procesos comerciales, etc. El control de nivel X se encontrará en un eje que comienza con el control de nivel básico, que generalmente hace referencia a un proceso existente pero no gestionado y ejecutado manualmente, y finaliza con el nivel innovador, que hace referencia a la implementación del control de manera gestionada, documentada, automatizada, eficiente y eficaz.

# 08

**Columnas adicionales propuestas:** información sobre el mapeo frente a estándares adicionales, la adición de contenido por parte del usuario para realizar la fase de mapeo de brechas, etcétera.

## Modo de utilización del banco de controles

El trabajo con el banco de controles comprende dos fases principales:

# 01

El mapeo de todas las brechas frente a la lista de diferentes controles (haciendo énfasis en la columna "Control"). Este mapeo ayudará a comprender cuáles son los asuntos en los que la organización no está debidamente preparada y a obtener una lista de las brechas principales (*gap analysis*). Este proceso es conforme por su propia naturaleza y el producto obtenido es una lista de "Correcto/Incorrecto/No pertinente/Implementado parcialmente".

# 02

El mapeo individual de controles frente a amenazas y riesgos críticos en los objetivos de protección sensibles de la organización.

Debido a que la implementación de controles es un proceso dinámico y que varía entre un objetivo de protección y otro, debe examinarse individualmente el nivel de control para objetivos de protección concretos. Por ejemplo, en determinados objetivos de pro-

tección debe examinarse en profundidad la capacidad de monitoreo, el control de la cadena de suministro y la existencia de una copia de seguridad. Este enfoque pone en práctica de forma efectiva la transición de una visión basada en el cumplimiento a un enfoque basado en los riesgos. El uso del banco de controles como herramienta para reducir riesgos y amenazas individuales constituye la materialización de su propósito en la visión de la dirección de la organización.

## Características únicas del banco de controles en la Metodología de Ciberdefensa

# 01

**Énfasis en los controles con la máxima contribución a la protección:** en los que el costo frente a beneficio es el más alto.

# 02

**Profundidad de la implementación de controles:** es posible implementar controles de diferentes formas, desde una implementación en la organización de forma manual y no sistemática, hasta una implementación integrada

respaldada por capacidades de automatización completas y conocimientos profesionales actualizados. Para una implementación eficaz y gradual, que ofrezca a la organización una vía de mejora, junto a cada control se presentan distintas opciones para una profundidad de implementación diferente.

# 03

**Evidencias requeridas:** a fin de asegurarse de que los controles pertinentes se hayan implementado de manera correcta en la organización, se han adjuntado a cada uno de ellos aspectos destacados y requisitos de documentación. Estos datos también pueden emplearse como base para una regulación y/o certificación conforme a este método.

# 04

**Clasificación y definición del orden de prioridades:** a fin de desarrollar una Metodología de Ciberdefensa adecuada, los controles de la presente publicación han sido clasificados en niveles entre el 1 y el 4. Los controles de nivel 1 son los más básicos y son necesarios en cada organización para todos los activos, mientras que los controles de nivel 4 solo se requieren para objetivos de protección cuyo potencial de daños sea 4.

## Anexo 4. Herramientas y métodos para implementar controles continuos en la organización

El control continuo es fundamental para la organización, ya que le coloca delante un espejo y le sirve a modo de brújula. Este tipo de control permite que el responsable de ciberprotección de la organización sepa cuáles son las brechas de seguridad y qué medidas deben tomarse para mejorar la situación.

El control continuo puede llevarse a cabo a nivel de cumplimiento, abordando asuntos y controles definidos (como el estado de cumplimiento de los controles de la Metodología de Ciberdefensa) o mediante una medición de riesgos, amenazas, preparación para escenarios de ataque, etcétera.

A fin de crear un plan interno para la gestión del **control continuo**, en primer lugar, deben definirse una serie de parámetros para la medición. A continuación, deben implementarse mecanismos que tomen los resultados de la medición y presenten la situación existente junto a la tendencia en la organización (es importante que dichos mecanismos sean lo más automatizados posible).

**A continuación, se muestra una serie de herramientas y métodos que deben implementarse en la organización para efectuar un control continuo:**

### 01

Indicadores clave de rendimiento (KPI, por sus siglas en inglés): permiten a la organización medir y cuantificar el nivel de protección en un momento determinado, de manera de compararlo con el historial de medición y, de esta forma, examinar la tendencia. Estos indicadores pueden examinar, por ejemplo:

- El número de usuarios que hayan hecho clic en un enlace como parte de un evento de suplantación de identidad (*phishing*).

- El número/porcentaje de servidores y estaciones finales en los que se haya instalado EDR, en los que las actualizaciones de seguridad estén al día, etcétera.
- El porcentaje de servidores sensibles en los que se haya efectuado un estudio de riesgos.
- El tiempo promedio desde el lanzamiento de una actualización de seguridad crítica hasta su instalación; el tiempo promedio desde la recepción de una alerta de nivel de *hardware* en información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés) hasta el inicio/cierre del tratamiento (*Mean Time To Identify* [MTTI]/*Mean Time To Detect* [MTTD]).
- El porcentaje de controles no implementados de la norma/estándar, el número escenarios para los que la organización esté preparada.



### 02

Indicadores clave de riesgo (KRI, por sus siglas en inglés): permiten a la organización realizar un seguimiento de la imagen que resulte de la recopilación de datos y, de esta manera, distinguir la formación de un riesgo. Estos indicadores pueden examinar una tendencia, así como medir una desviación de un valor determinado que pueda indicar un potencial de riesgo. Estos indicadores pueden incluir, entre otros:

- La cantidad de búsquedas externas del sitio web.
- La cantidad de informes que contengan información sensible que se emitan desde el sistema.
- La cantidad de información copiada a unidades externas.
- El número de intentos de inicio de sesión fallidos (*failed log on*).

Ritmo de cambios y de medición

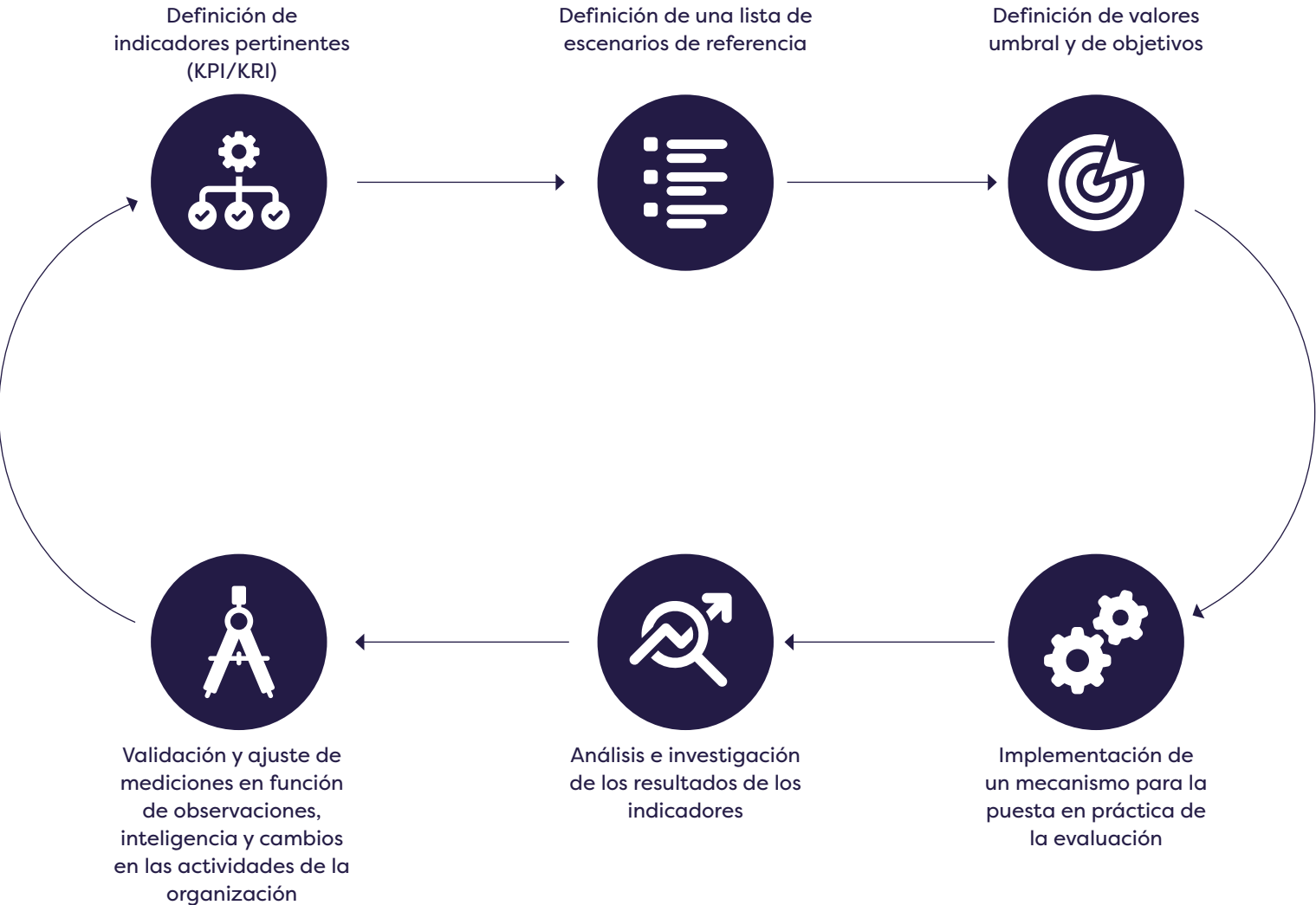
El seguimiento de indicadores como KRI o KPI requiere que la organización muestree su situación actual en distintos parámetros, en intervalos de tiempo definidos. En numerosas ocasiones, este proceso requiere intervención manual, unida al trabajo de procesamiento y análisis, de modo que lleva tiempo. Por lo tanto, solo es posible examinar estos indicadores mensual o trimestralmente.

En el entorno tecnológico, el ritmo de los cambios es rápido y para identificar una anomalía algunos de los indicadores deben muestrearse una vez al día o incluso cada varias horas, pero los procesos de medición tradicionales no pueden dar respuesta a este desafío. Los parámetros que cambian con una alta frecuencia requieren un mecanismo de medición diferente, que se conoce como CMC.

La implementación de este concepto en la organización le permitirá ver la situación actual en tiempo real y de una manera que no requiera intervención humana.

La organización no puede esperar a la siguiente medición de parámetros como interfaces que se abran (intencional o accidentalmente), actualizaciones críticas no implementadas, una constitución de cortafuegos configurada de tal manera que ponga en peligro la red, o graves de problemas de seguridad del código de software. Todo lo anterior (entre otras cosas) debe ser monitoreado de forma continua mediante la implementación de una tecnología específica.

Gráfico A4.1. Proceso de implementación de CMC en la organización



## Aspectos destacados para la implementación de un programa CMC

### 01

Debe establecerse una jerarquía organizacional, incluyendo la división de las competencias y la responsabilidad en este asunto. Por ejemplo: de qué manera se integra este proceso con la segunda línea de protección de la organización, si el gerente de riesgos principal de la organización está involucrado en la definición y medición de los indicadores, y si son necesarios administradores de ciberprotección en las distintas unidades de la organización.

### 02

Debe establecerse la plataforma en la que vaya a gestionarse el proceso de medición. Las herramientas de gobernanza, riesgo y cumplimiento (GRC) pueden brindar numerosos beneficios, aunque en algunos casos también es posible gestionar este proceso en otras aplicaciones, como un procesador de texto.

### 03

Debe examinarse la delimitación de los indicadores, haciendo referencia también a los indicadores que salgan de los límites de la organización, por ejemplo, una medición del nivel de protección de los proveedores y subcontratistas externos.

### 04

Paralelamente a la comprobación de la existencia de los controles, debe cuestionarse su efectividad. La finalidad de esta comprobación es examinar si un control que se haya puesto en práctica realmente aborda las amenazas y riesgos para los que ha sido implementado. Este cuestionamiento de los controles puede llevarse a cabo mediante herramientas de simulación de ataques, así como a través de comprobaciones proactivas de diferentes escenarios. Para este fin, puede emplearse un cuadro de comprobaciones efectivas iniciadas como el cuadro A4.1.



**Cuadro A4.1.** Comprobaciones efectivas iniciadas

N.º	Descripción del control	Resultado deseado en caso de incumplimiento de la política aceptada				
		Bloqueo activo	Desconexión de la red	Aviso	Investigación y corrección	Otro
1	Activación/envío de un archivo de prueba EICAR ( <i>EICAR test file</i> ) por medio de una interfaz aleatoria a un activo cibernético (por ejemplo, correo electrónico, acceso compartido o navegación a un sitio web que contenga el archivo)	X	X	X	X	
2	Filtrado de información sensible o confidencial en distintas interfaces (por ejemplo, el envío a una dirección de correo electrónico externa, su carga en BOX o su impresión)	X		X	X	Informe al gerente de usuarios
3	Conexión de un dispositivo DOK y un módem celular externo a estaciones finales aleatorias	X	X	X	X	
4	Eliminación/adición de un componente de <i>hardware</i> a una estación final (por ejemplo, memoria o disco duro)	X	X	X	X	
5	Realización de una actividad de red hostil silenciosa (por ejemplo, <i>port scanning</i> )			X	X	
6	Uso de una interfaz de carga de archivos legítima en un portal interno/externo para subir un archivo basado en un formato fraudulento (por ejemplo, un archivo EXE con un valor <i>MIME Type</i> o PDF)	X		X	X	

N.º	Descripción del control	Resultado deseado en caso de incumplimiento de la política aceptada				
		Bloqueo activo	Desconexión de la red	Aviso	Investigación y corrección	Otro
7	Conexión de una computadora que no pertenezca a la organización a un puerto de comunicación aleatorio	X	X	X	X	
8	Comprobación del número de computadoras registradas en el directorio de la organización en comparación con el registro en un sistema de protección (por ejemplo, un servidor de gestión de antivirus)				X	
9	Comprobación del número de usuarios registrados en el directorio de la organización en comparación con el número de registro en la oficina de recursos humanos (u otro órgano en la organización)				X	
10	Activación de una herramienta de ataque automática (por ejemplo, SQLMap) contra un portal de la organización (interno/externo)	X		X	X	
11	Comprobación de la configuración de securización de una estación final aleatoria en relación con una base de referencia ( <i>baseline</i> ) aprobada				X	
12	Comprobación de la lista de actualizaciones de seguridad (parches) en una estación final aleatoria en relación con una base de referencia aprobada				X	

N.º	Descripción del control	Resultado deseado en caso de incumplimiento de la política aceptada				
		Bloqueo activo	Desconexión de la red	Aviso	Investigación y corrección	Otro
13	Instalación/activación de una aplicación que no ha sido aprobada para su uso en la organización	X		X	X	
14	Acceso a un sitio web que incumpla las políticas permitidas de la organización (por ejemplo, un sitio web para compartir archivos)	X		X	X	
15	Intento de blanquear archivos de un tipo que no esté permitido en el perfil de usuario	X		X	X	
16	Acceso físico a áreas/instalaciones confidenciales			X	X	Investigación y comprobación de las imágenes por parte del responsable
17	Comprobación del grado de actualización de las herramientas de protección en una estación final aleatoria en relación con una base de referencia aprobada				X	
18	Creación/modificación/eliminación de una cuenta de usuario con privilegios altos			X	X	
19	Activación simultánea de dos o más estaciones con la misma dirección MAC o IP en diferentes áreas/instalaciones de la organización	X	X	X	X	

N.º	Descripción del control	Resultado deseado en caso de incumplimiento de la política aceptada				
		Bloqueo activo	Desconexión de la red	Aviso	Investigación y corrección	Otro
20	Localización de información sensible, confidencial o indicador de compromiso (IOC, por sus siglas en inglés) en una estación final			X	X	
21	Obtención de accesibilidad de una red a otra, pese a que la política oficial prohíba una comunicación directa			X	X	
22	Activación de varias sesiones (sessions) desde una sola dirección IP a un único servidor aislado	X		X	X	
23	Activación de varias sesiones desde una sola dirección IP a muchos servidores	X		X	X	
24	Alto consumo de ancho de banda desde una sola dirección IP o desde varias direcciones			X	X	
25	Acceso en Server Message Block (SMB), por ejemplo, de una estación de trabajo a otra (en lugar de acceder a un servidor central)	X		X	X	

# Anexo 5. Árbol de doctrinas: visión global de la Metodología de Ciberdefensa para Organizaciones

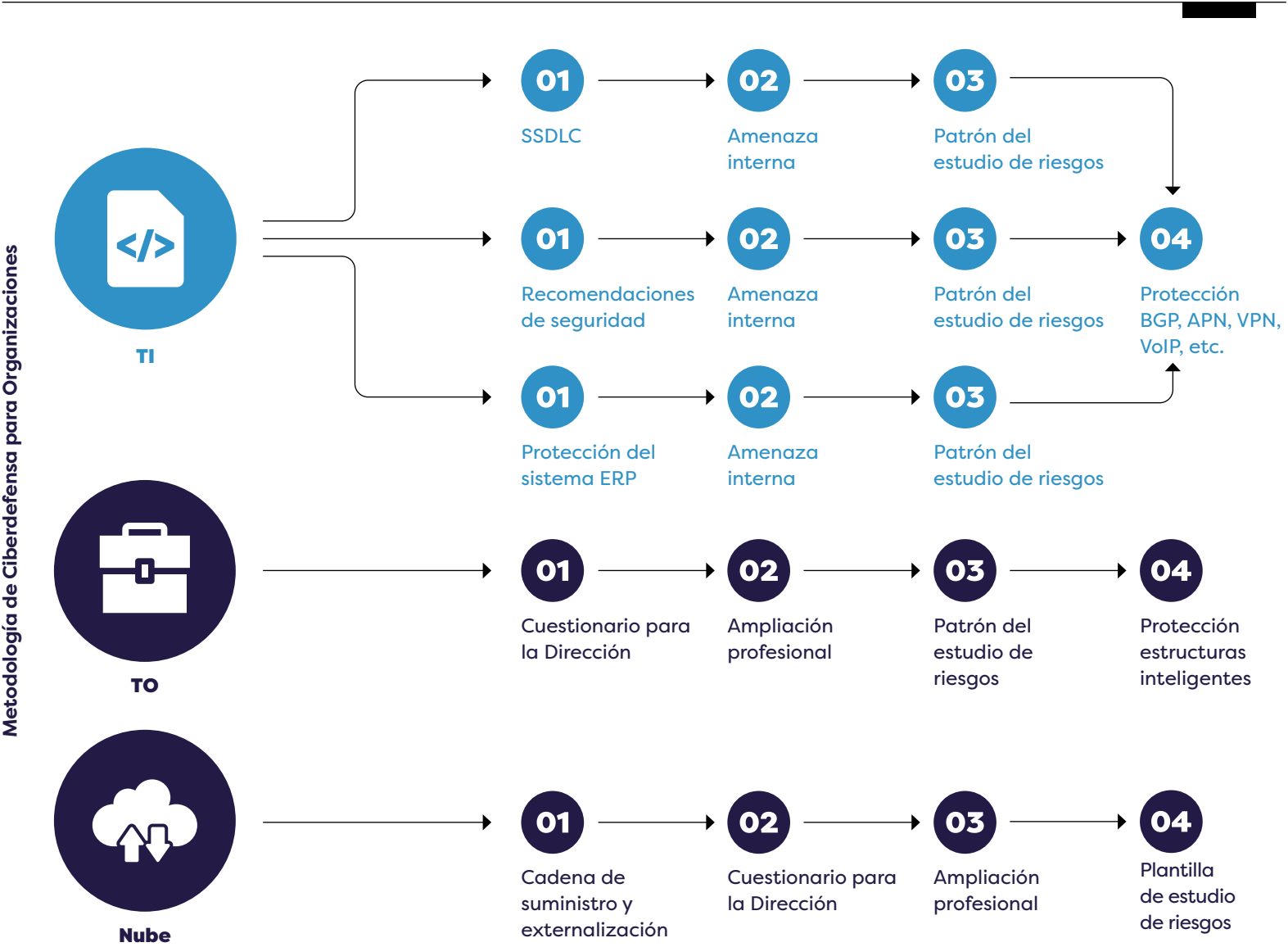
A fin de ayudar en la implementación de la Metodología de Ciberdefensa y hacerla accesible a distintos públicos objetivo, el Plan Cibernético Nacional ha desarrollado una serie de productos para ampliar los conocimientos profesionales en este ámbito. Además, el Plan Cibernético proporciona herramientas de apoyo para ayudar en este proceso.

Los productos desarrollados por el Plan Cibernético Nacional están disponibles en su sitio web: [https://www.gov.il/en/departments/topics/organization\\_cyber\\_protection/govil-landing-page](https://www.gov.il/en/departments/topics/organization_cyber_protection/govil-landing-page). Algunos de estos documentos han sido traducidos al español y forman parte de esta colección.

Además, la información está disponible en el sistema Yuval, una calculadora única que permite a cualquier organización en Israel comprobar fácilmente su nivel de ciberprotección.<sup>5</sup>

5. Puede encontrarse la calculadora Yuval en: <http://www.gov.il/he/departments/guides/yuvalrisk>  
Actualmente disponible en idioma hebreo.

**Gráfico A5.1.** Árbol de doctrinas: herramientas y metodologías de protección elaboradas por el Plan Cibernético Nacional



**Los productos de apoyo para la implementación de la Metodología de Ciberdefensa pueden presentarse de acuerdo a la siguiente jerarquía:**

# 01

**Concepto nacional:** con base en el cual se elabora la Metodología de Ciberdefensa para Organizaciones.

# 02

**Metodología de Ciberdefensa:** presenta los distintos asuntos relacionados con la protección en un nivel básico (por ejemplo: monitoreo, concienciación, separación de redes o gestión de la cadena de suministro) y los principios que han de tenerse en cuenta al elaborar un plan de trabajo para la organización. Este documento es la base profesional para realizar un estudio de riesgos y para crear un plan de trabajo cibernético para la organización.

# 03

**Mejores prácticas (best practices):** productos que profundizan en las recomendaciones

relativas a asuntos tecnológicos específicos. Estos documentos presentan al lector recomendaciones de protección individual a fin de implementar controles de la Metodología de Ciberdefensa para una tecnología determinada, como VoIP, VPN o identificación segura.

# 04

**Ampliaciones profesionales:** productos que presentan a los lectores un análisis acerca de un ámbito profesional y les proporcionan una amplia base profesional para acceder a un proyecto sobre un asunto determinado. Estos productos no se centran en una tecnología en particular, sino que presentan diferentes consideraciones: cómo abordar un tema; conocimientos y consejos que surgieron en el diálogo continuo con actores de la economía, una visión integral de ese ámbito y la presentación de un concepto para implementar el tratamiento del asunto en cuestión en la organización. Ejemplos de ampliaciones profesionales que están disponibles en el sitio web del Plan Cibernético son las tareas del Director de Seguridad de la Información (CISO, por sus siglas en inglés) con organismos de desarrollo, la protección de entornos operativos y la gestión de riesgos de la cadena de suministro.

**Gráfico A5.2.** Productos de apoyo para la implementación de la Metodología de Ciberdefensa

## Concepto

Metodología de Ciberprotección para Organizaciones / Estándar de ciberprotección

**A**

Mejor práctica A

**B**

Mejor práctica B

**C**

Mejor práctica C

**D**

Mejor práctica D

**E**

Mejor práctica E

## Ampliación profesional



Por ejemplo, desarrollo seguro, trabajo en un entorno de nube, externalización y cadena de suministro, continuidad del negocio, etc.



## Anexo 6. Protección de la información y la privacidad

La protección de la información puede tener diferentes propósitos, por ejemplo, evitar los daños a la reputación, prevenir las fugas de información comercial o prevenir la filtración de información privada.

Aunque en ocasiones, desde el punto de vista del personal informático, la protección sea la misma (como el cifrado de un archivo o el establecimiento de principios estrictos para el control de acceso), **el propósito** puede ser diferente.

El derecho a la privacidad ha sido recogido en la Ley Fundamental: La Dignidad de la Persona y su Libertad, en distintas leyes (principalmente en la Ley de Protección de la Privacidad), así como en tratados internacionales. La Ley de Protección de la Privacidad comprende una serie de principios centrales. Uno de ellos es el **principio del consentimiento**, que expresa el control del individuo sobre la información re-

lativa a él: él es quien decide qué información se divulgará y a quién.

Este principio se ve reflejado, entre otros, en el artículo 1 de la Ley de Protección de la Privacidad, que estipula que **“una persona no violará la privacidad de otra sin su consentimiento”**. En virtud de esa ley, el consentimiento debe ser informado, es decir, concedido solo después de que una persona comprenda su significado y sus implicaciones.

Otro principio central es el de **cercanía al propósito**. Según este principio, que está regulado en los artículos 2 (9) y 8 (b) de la citada Ley de Protección de la Privacidad, únicamente está permitido utilizar la información de acuerdo con el propósito para el que fue recopilada en un principio. Su uso para cualquier otro propósito constituye una violación de la privacidad.

La Ley de Protección de la Privacidad y los reglamentos promulgados en virtud de ella también estipulan distintas obligaciones relativas al registro de las bases de datos y a su forma de protección. Entre otras cosas, existe la obligación de examinar la necesidad de continuar el almacenamiento de la información de acuerdo con el propósito de su recopilación.

La mencionada Ley de Protección de la Privacidad también hace referencia a los **derechos del interesado**. De conformidad con el artículo 11 de esta ley, debe informarse al interesado (*data subject*) acerca de la intención de recopi-

lar información y especificarse los propósitos de su uso, y también indicar si tiene la obligación legal de facilitar dicha información o si está autorizado a denegarla. El artículo 13 de esta ley otorga al interesado el derecho a acceder a la información relativa a él y el artículo 14 le concede el derecho a exigir su corrección en las circunstancias pertinentes.

No obstante, como todos los derechos, el derecho a la privacidad no es absoluto, y pueden existir circunstancias en las que otros intereses justifiquen una violación determinada de él. Este concepto está regulado, entre otros, en las protecciones previstas en el artículo 18 de la Ley de Protección de la Privacidad. Sin embargo, tal violación deberá producirse de conformidad con el propósito de las disposiciones de la ley y cumplir con los principios generales de acción razonable y de buena fe y, en el caso de los organismos públicos, también el requisito de proporcionalidad.

De modo general, la ciberprotección constituye una **acción legítima** que no implica ninguna violación excepcional de la privacidad.

Sin embargo, su implementación efectiva debe llevarse a cabo abordando en profundidad los aspectos de la privacidad y el cumplimiento de los principios aceptados, como la **seguridad por diseño** (*security by design*), la **privacidad por diseño** (*privacy by design*) y la **protección consciente de amenazas** (*threat informed defense*). Estos principios requieren una comprensión

profunda de la tecnología y los procesos por parte del CISO, que también debe saber cómo encontrar el **equilibrio adecuado entre distintos intereses**, de modo que sus recomendaciones a la Dirección de la organización permitan tomar decisiones de manera informada.

La Metodología de Ciberdefensa hace hincapié en que es importante que el CISO involucre al **asesor jurídico** de la organización desde la fase de inicio y en la caracterización del plan de trabajo a fin de reducir las brechas de seguridad. Más adelante, debería involucrarse en intersecciones clave durante el ciclo de vida de la información, los procesos comerciales y distintos activos cibernéticos. Por ejemplo, la participación del asesor jurídico se requiere ya en la fase de **mapeo de los requisitos de la ley, regulaciones, requisitos contractuales y necesidades comerciales** con los cuales deba cumplir la organización. Todo ello forma la base de la existencia del proceso de gestión de riesgos y del cumplimiento por parte de la dirección de las obligaciones habituales, como los procedimientos de debida diligencia (*due diligence*).

También es importante que el asesor jurídico de la organización sea un miembro fijo en las reuniones del **comité directivo**, como el Comité de Protección de la Información y Ciberprotección. Además, debe estar involucrado en los **procesos de contratación y celebración de contratos** con las distintas partes de la cadena de suministro.

Además, la estructura de los controles de la Metodología de Ciberdefensa ofrece al CISO una **gran libertad de acción**, lo cual le permite reducir el nivel de riesgo a un valor aceptable, a la vez que se reduce al mínimo la violación de la privacidad.

La Metodología de Ciberdefensa enfatiza que la organización debe utilizar **círculos de seguridad independientes** para hacer frente a las distintas amenazas (como el mal uso de los privilegios legítimos) y que el proceso de toma de decisiones debe estar respaldado por evidencias. Como resultado de ello, además de la capacidad de obtener una visión real de la situación de seguridad en la organización (*security posture*), será posible incrementar la probabilidad de que las acciones que violen la privacidad solo se lleven a cabo en caso de necesidad real.

La Metodología de Ciberdefensa también hace hincapié en la importancia del **uso de procesos de automatización e instrumentación**. Ello **reduce la necesidad de intervención humana** en los procesos operativos y de protección, de modo que las probabilidades de que se produzca un error humano sean pequeñas y, simultáneamente, disminuye el nivel de exposición de las distintas partes a la información personal. Por ejemplo, mediante la adopción de la ontología MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK), la organización podrá utilizar soluciones mecanizadas avanzadas para

efectuar un control continuo y realizar procesos de respuesta, por lo que la intervención humana solo será necesaria en casos excepcionales.

Asimismo, la Metodología de Ciberdefensa **recomienda la realización acciones de protección proactivas** para preservar la información y las **capacidades efectivas para hacer frente** a incidentes de filtración de información, como adquirir la capacidad de eliminar información que se haya filtrado a Internet y a la red oscura (*darknet*).

En conclusión, el CISO es una parte significativa en la protección de la información y la privacidad, y debe involucrar a las distintas partes en la organización a fin de maximizar el nivel de protección.

### Integración de actividades de protección a fin de mejorar el nivel de protección de la privacidad en la organización

Los controles de la Metodología de Ciberdefensa se unen en un marco de trabajo que incluye aspectos de identificación, protección, localización, respuesta y recuperación. Mediante la implementación de recomendaciones en materia de ciberprotección y seguridad de la información, en algunos casos los aspectos que sirven a la protección de la privacidad están interrelacionados con los propios controles.

## Anexo 7. Concepto de protección avanzada para la organización

El concepto de protección requerido para hacer frente a las amenazas avanzadas comprende enfoques avanzados.

La puesta en práctica de estos enfoques ayudará a la organización a conseguir capacidades avanzadas, como confundir y engañar al atacante para ganar tiempo, desgastar al atacante e incluso lograr disuadir a los potenciales atacantes. Estos principios pueden incluir:

- **Denegación y engaño (D&D, por sus siglas en inglés).**
- **Encubrimiento y ofuscación.**
- **Resistencia a la manipulación y exposición a la manipulación.**
- **Defensa de silencio.**
- **Caza de amenazas.**
- **CMC.**
- **Diversidad / superficie de ataque dinámica (MTD, por sus siglas en inglés).**

Es posible aplicar los principios de protección avanzada mediante la adopción de marcos de trabajo y proyectos como MITRE ATT&CK o el modelo *cyber kill chain*, y mediante la creación de conceptos para procesos y rutinas de protección en la organización.

En el cuadro A7.1 se enumeran algunos ejemplos de componentes en un concepto organizacional y ejemplos de su implementación en rutinas de protección.

La base para la implementación de un concepto avanzado es la profesionalidad de los responsables de ciberprotección en la organización. Las organizaciones que tengan la intención de adoptar estos conceptos deben invertir en la formación avanzada y continua de los profesionales pertinentes.



**Cuadro A7.1.** Componentes en un concepto organizacional y ejemplos de implementación en rutinas de protección

Componente	Explicación	Propósito	Ejemplos
Desgaste	Agotamiento gradual y continuo de la capacidad de combate del atacante mediante el daño acumulativo a sus tropas, sus medios y su motivación (según el diccionario de conceptos de las Fuerzas de Defensa de Israel).	Cambiar la ecuación de conveniencia del atacante frente a la parte defensora. Levantar los muros para que la parte defensora no sea el objetivo preferido para lograr el propósito del ataque.	Realizar acciones proactivas con una alta frecuencia para examinar la integridad de la superficie de ataque externa/interna de la organización puede posibilitar la identificación, detección y tratamiento de las vulnerabilidades antes de que sean aprovechadas indebidamente. Como resultado de ello, un atacante potencial puede constatar que el uso de métodos de ataque convencionales (como Webshell) contra la organización no es lo suficientemente efectivo. Esto lo obligará a desarrollar medios de ataque alternativos (algo que hará más costoso y largo el ataque) o preferir pasar a un objetivo alternativo más accesible.
Comprensión de la situación cibernética (situational awareness)	Capacidad para comprender debidamente lo que está teniendo lugar en el ciberespacio y las implicaciones de ello para la continuidad operativa en la organización o la economía.	Crear una infraestructura para una toma de decisiones con base en la comprensión situacional de las principales amenazas para los activos centrales de la organización.	A menudo, el sistema de ciberprotección en las organizaciones sufre una escasez de recursos constante. Una organización que sea capaz de comprender cuáles son sus joyas de la corona y cuáles son sus vectores de ataque (attack vector) actuales que un atacante potencial podría utilizar, podrá priorizar sus esfuerzos de protección de manera más adecuada.
Disuasión	Una acción o proceso de amenaza que impida que el atacante realice una acción por temor a sus consecuencias. La disuasión crea en el atacante la sensación de que se cierne sobre él una amenaza creíble que no podría contrarrestar. Cabe destacar que la capacidad de crear disuasión dependerá de la existencia de la autoridad jurídica apropiada y, por lo tanto, la capacidad de la organización se basará principalmente en el uso de instrumentos jurídicos y financieros. A fin de mantener la credibilidad de la disuasión, la organización deberá asegurarse de activar dichos instrumentos cuando sea necesario.	Reducir la motivación de un oponente para llevar a cabo un ataque contra la organización.	Cuando un usuario realice una acción que levante sospechas de que se está recopilando inteligencia antes de realizar un ataque, aparecerá en la pantalla el mensaje: “Es posible que esté realizando una acción considerada ilegal; desde este momento, todas sus actividades serán monitoreadas y documentadas, y la organización se reserva el derecho de responder por distintos medios”. La disuasión podrá realizarse por medios más “suaves”, como acuerdos legales o <i>hack back</i> . En cualquier caso, será obligatorio que esta actividad cuente con asesoramiento jurídico, a causa de los riesgos latentes inherentes a ella.
Denegación y engaño	Uso de distintos medios y métodos para distraer al atacante e incluso recopilar información de inteligencia de valor. Sin embargo, el éxito efectivo dependerá de la capacidad de los medios y métodos de trabajo para adaptarse al entorno de producción existente o al que el atacante crea que exista.	Ganar tiempo desde el principio del ataque y hasta su materialización para aprender el curso de acción del oponente, además de recibir un aviso temprano de los intentos de ataque. Junto al retraso del atacante y el aprendizaje sobre él, las herramientas de engaño (deception) permiten realizar una mitigación (es decir, aislamiento [isolation] o bloqueo [blocking]) mediante la conexión a las herramientas existentes en la organización (cortafuegos, antivirus, control de acceso a la red [NAC, por sus siglas en inglés], EDR, etc.).	Esta familia incluye, por ejemplo, el uso de una trampa de miel (honeypot), emulación (emulator), frases falsas (honeytokens), redes de miel (honeynets), desinformación (disinformation), o medios ultrafalsos (deep fake). Es posible implementar todo lo anterior mediante distintos métodos, como Honeypot Full OS, Honeypot Emulation, Honeydocs. Asimismo, es posible combinar en apariencia operaciones al nivel de procesos.



#### **Estimados gerentes y expertos en seguridad de la información y ciberprotección:**

El ciberespacio es el resultado de los avances tecnológicos, la conectividad y la conexión global a Internet. La creciente dependencia del ciberespacio trae consigo una serie de innovaciones tecnológicas y enormes desarrollos para las personas y su entorno. Sin embargo, junto a ellos, también se crea un espacio de amenazas que afecta la continuidad del negocio, la integridad de los procesos de producción y la confidencialidad de la información de las organizaciones.

Los ciberataques pueden causar daños en las organizaciones, incluso que se detengan los procesos de producción, daños económicos y daños a su reputación. El Estado de Israel está haciendo un esfuerzo a nivel nacional en materia de ciberprotección en el espacio civil. La Metodología de Ciberdefensa para Organizaciones es una de las fases del Concepto de Defensa Nacional, que consta de distintas capas de protección para la economía israelí y su continuidad operativa.

Esta Metodología comprende a la organización como un todo y permite incrementar su nivel de resiliencia mediante una implementación continua de procesos, métodos y productos destinados a la protección. En consecuencia, la puesta en práctica de esta Metodología mejorará su resiliencia y su resistencia ante ciberataques.

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*

