

Metodología de Ciberdefensa para Organizaciones Versión 1.0

Mejores Prácticas en Ciberseguridad



A.01

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 “Metodología de ciberdefensa para una organización”. © (2017) 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/policies/cyber_security_methodology_for_organizations. Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

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

Índice

Prólogo

/Pág. 2

Resumen ejecutivo

/Pág. 8

01. Introducción

/Pág. 11

02. Principios de la Metodología de Ciberdefensa

/Pág. 14

03. Estructura de la Metodología de Ciberdefensa

/Pág. 16

04. Proceso de planificación organizacional

/Pág. 20

05. Metodología de Ciberdefensa desde la perspectiva de la organización

/Pág. 22

06. Capítulos de controles: etapas de implementación y control

/Pág. 45

Anexos

/Pág. 182

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.¹

El BID y la INCD: uniendo esfuerzos

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

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

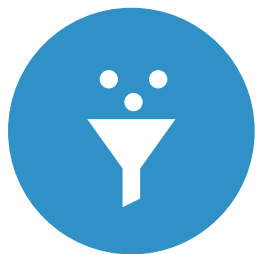
de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

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

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



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



Resumen ejecutivo

El propósito de la Metodología de Ciberdefensa es reducir al mínimo los riesgos cibernéticos para las organizaciones en Israel. Esta publicación presenta un método coherente que guía la responsabilidad de las empresas para construir un plan de trabajo plurianual para proteger la organización. Al usar esta metodología, la organización va a reconocer los riesgos relevantes, formular una respuesta de defensa y hacer realidad un programa para reducir los riesgos.

Etapa A. La organización identifica a qué categoría pertenece

Categoría A: organizaciones cuyo daño potencial debido a ciberincidentes no es significativo.

Categoría B: organizaciones cuyo daño potencial debido a ciberincidentes es significativo.

La pregunta para conocer a qué categoría pertenece la empresa figura en la página 23.

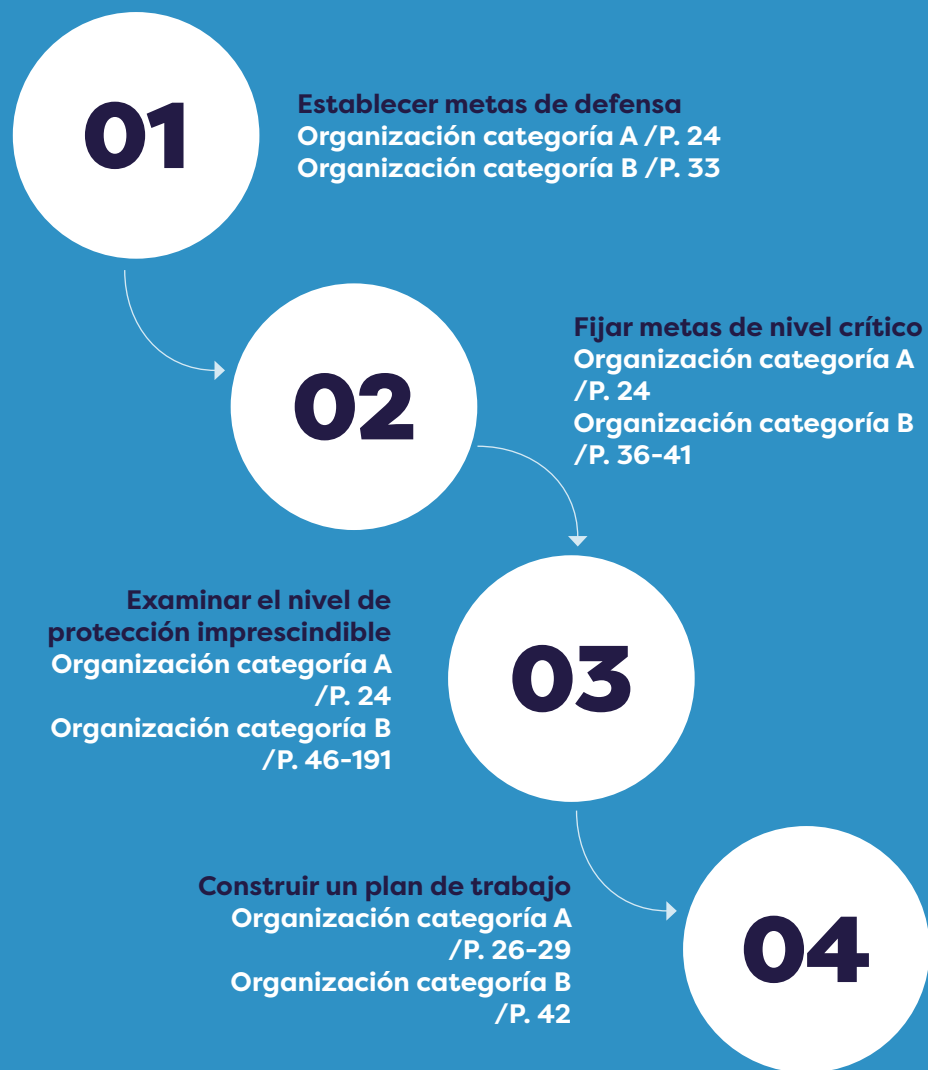
Etapa B. Formulación de un plan de trabajo para la organización

En cuanto a la formulación del plan de trabajo la organización va a definir, en primer lugar, lo que se precisa proteger, el nivel de protección requerido y los vacíos de protección en vista de la situación deseada, y, en segundo lugar, va a construir un plan de trabajo para reducir las brechas.

Una explicación sobre cómo configurar los objetivos de protección de la organización y el nivel de protección requerido se presenta en la página 24 para las organizaciones de la categoría A, y en las páginas 33-35 para las de la categoría B. En este punto, la organización debe entender los controles necesarios para sus distintos activos. Estos controles se presentan en las páginas 25-29 para las organizaciones de la categoría A, y en las páginas 46-191 para las de la categoría B.

Producto final a la luz del trabajo con esta publicación

Luego de trabajar con esta publicación, la organización va a entender cuáles son los controles necesarios que debe poner en práctica con el fin de reducir los riesgos cibernéticos a los que está expuesta. Estos controles constituirán el plan de trabajo para reducir esos riesgos. El plan de trabajo para las organizaciones que reciben la guía de un facilitador profesional en nombre de la Dirección Nacional de Ciberseguridad de Israel (INCD, por sus siglas en inglés), se construirá de acuerdo con la guía directa del facilitador del sector.

Gráfico 1. Plan de trabajo de una organización

/01. Introducción

El ciberespacio es una parte integral de nuestras vidas. En el plano individual, las personas buscan información en Internet, recorren un camino usando un *software* de navegación por carretera, hablan por teléfono celular, y algunas tienen un marcapasos o una bomba de insulina conectada a Internet; todo esto es parte del ciberespacio. En el plano empresarial, se usan tarjetas de crédito, se administra una base de datos de clientes, se gestiona una organización mundial a través de una red de ordenadores, se realizan operaciones comerciales, se compra y vende; todo esto también con base en el ciberespacio.

Para muchas personas en la vida cotidiana, en general, y en los negocios, en particular, un ciberespacio disponible, accesible y fiable constituye una condición necesaria. Esto es fácil de entender cuando no se dispone de alguno de esos recursos temporalmente: ¿Cómo manejar el negocio sin un teléfono móvil? ¿Sin la información almacenada en la red corporativa? ¿Sin la capacidad de ejecutar una compensación de tarjeta de crédito?

El ciberespacio es, por un lado, un lugar de posibilidades y oportunidades, pero, por otro, un espacio de amenazas y riesgos.

Una extensa gama de espionaje de Estado, espionaje comercial, crimen organizado, delincuencia ocasional, piratería de datos personales, entre otros, se está llevando a cabo en este espacio. Estos pueden afectar la seguridad nacional (por ejemplo, al dañar una infraestructura nacional crítica, como la red eléctrica o el sistema de agua), el ejercicio de una actividad (como el espionaje económico) y la privacidad (por ejemplo, mediante la publicación de información e imágenes personales).

En la actualidad, las organizaciones se protegen de estas amenazas de diversas formas. La información disponible en línea acerca de las maneras de protegerse de los riesgos cibernéticos es muy amplia y se compone de metodologías, mejores prácticas, “qué hacer y qué no hacer”, y mucho más.

Proteger a la organización contra las amenazas informáticas requiere de muchos conocimientos, los cuales incluyen un gran número de especialidades tecnológicas, organizativas y de procedimiento.

Muchas organizaciones locales y extranjeras se enfrentan a preguntas tales como: ¿Se está invirtiendo lo suficiente en ciberdefensa?, ¿se invierte de manera correcta?, ¿se invierte como se hace comúnmente en esta industria y en este sector? Las organizaciones desean protegerse y reducir sus principales riesgos en el ciberespacio, a fin de realizar la actividad empresarial sin miedo.

La Metodología de Ciberdefensa ayuda a las organizaciones a reconocer los riesgos cibernéticos a los que están expuestas, para comprender la importancia de los mismos y definir los medios para reducir los principales riesgos. Esta Metodología define también la protección adecuada para los activos de la empresa que tienen un impacto en un determinado sector o pertenecen al ámbito estatal.

La INCD se estableció, entre otras cosas, con el fin de diseñar, implementar e integrar una metodología nacional de protección cibernética (Decisión del Gobierno N° 2.444). En este marco, la INCD ha decidido publicar la Metodología de Ciberdefensa para Organizaciones de la economía israelí, comenzando con los ministerios del gobierno.

La INCD ha desarrollado esta metodología a partir de la combinación de las metodologías más importantes a nivel mundial, sumadas a la experiencia civil y de seguridad israelí, y la ha adaptado al entorno de Israel y a la cultura de negocios del país.



/02.

Principios de la Metodología de Ciberdefensa

El principal concepto de protección de la Metodología de Ciberdefensa es la organización como un todo, es decir, reconocer que lo que se requiere es una defensa para la continuidad funcional de la organización y sus objetivos comerciales. Este concepto se expresa en esta publicación de la siguiente manera:

01

Responsabilidad de la Dirección: la responsabilidad de defender la información recae principalmente en la Dirección de la organización.

02

Defensa de acuerdo con el daño potencial: la inversión en la protección de cada activo será proporcional a su importancia para el funcionamiento de la organización.

03

Defensa basada en el conocimiento y experiencia israelí: la Metodología de Ciberdefensa permite centrarse en los riesgos propios de cada organización. La INCD lleva a cabo revisiones periódicas y evaluaciones de inteligencia, lo que permite que las organizaciones se focalicen en aspectos específicos de los diversos círculos de defensa.

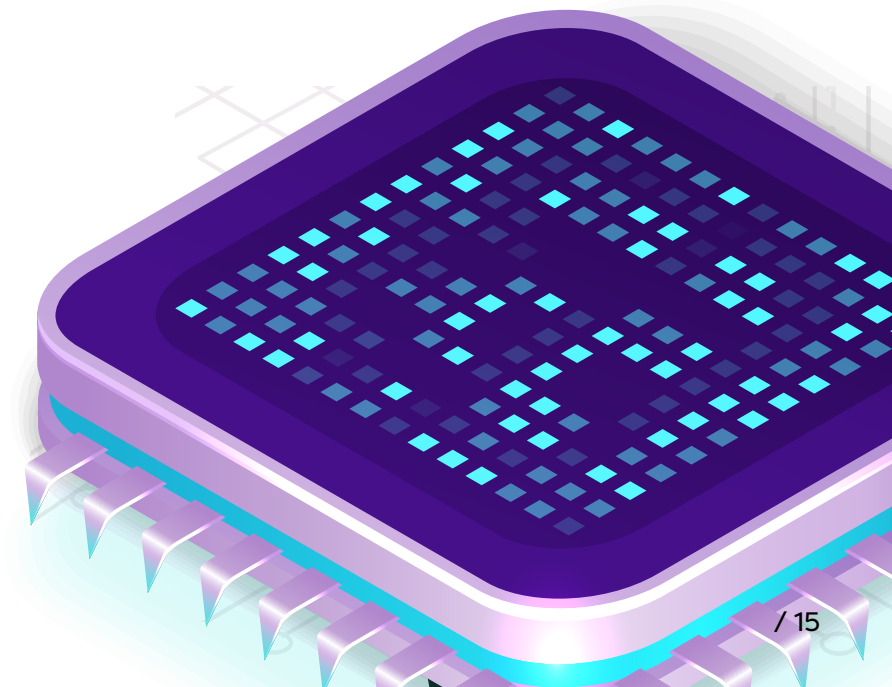
04

Defensa proactiva: los controles de defensa se definieron con base en el entendimiento de que es necesario que la organización in-

vierta esfuerzos más allá de la defensa pasiva tradicional. Este concepto se expresa en la definición de los controles de prevención, detección, respuesta y recuperación.

05

Defensa de múltiples niveles: es un proceso que combina tres componentes principales: personas, productos y procesos (3Ps). La Metodología de Ciberdefensa define una respuesta defensiva para cada nivel.



/03.

Estructura de la Metodología de Ciberdefensa

Dado que las organizaciones funcionan en entornos dinámicos, los cambios en la tecnología y en el carácter y actividad de las empresas influyen en la manera en que las organizaciones deben protegerse en el ciberespacio.

La siguiente metodología se basa en la necesidad de la organización de evaluar los riesgos periódicamente. Esta evaluación de riesgos es la base de un plan de trabajo plurianual para disminuir las brechas mediante la implementación de controles requeridos.

El proceso cíclico de defensa

El proceso de protección de esta metodología es cíclico y consta de tres etapas principales:

01

Planificación y evaluación: identificación de los objetivos de protección de la organización, evaluación de riesgos, inspección de los medios de defensa existentes (controles) y elaboración de un plan de trabajo para cerrar las brechas defensivas.

02

Ejecución del plan de trabajo mediante el desarrollo de los procesos organizacionales, integración de herramientas e integración organizacional de la ciberdefensa.

03

Mantenimiento de defensas actualizadas en la organización a la luz del dinamismo

del ciberespacio. Los procesos y tecnologías integradas en la organización están cambiando constantemente —se instalan nuevos ordenadores y redes, se adquieren paquetes avanzados de software, se vinculan nuevos elementos al ciberespacio (como Internet de las cosas [IoT, por sus siglas en inglés]), se ofrecen nuevos servicios (como la computación en la nube), etcétera—. Por su parte, las amenazas y los métodos de ataque están cambiando, por lo que se requieren herramientas de defensa, las cuales también cambian.

Gráfico 2. Proceso cíclico de defensa



Controles de protección compilados bajo el marco NIST de ciberseguridad

Durante muchos años las normas de protección hicieron hincapié en la cuestión de la defensa de la organización, a saber: la prevención frente a una penetración en la organización y sus re-

ursos cibernéticos. La realidad actual es diferente: las organizaciones de todos los tamaños son atacadas, pero estos ataques solo se detectan, si se descubren, después de mucho tiempo. En consecuencia, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST, por sus siglas en inglés) ideó un marco para mejorar la ciberseguridad de infraestructuras críticas, que se centra en la inversión en las fases de preparación y protección tradicionales, y en la detección, contención y recuperación de los ataques cibernéticos.

La presente Metodología de Ciberdefensa adopta el Marco de Seguridad Cibernética del NIST, unificando grupos de control de defensa. Dentro de este marco, **la organización se defiende de los ataques, mientras que aumenta su capacidad para detectar un ataque exitoso, contenerlo y recuperarse con un impacto mínimo.** Estos controles se basan en el conocimiento internacional pero se ajustan a la economía israelí e incluye información destacada y ejemplos para ayudar a las organizaciones a centrar sus esfuerzos de manera más eficaz.

“Solo hay dos tipos de empresas: aquellas que han sido hackeadas y aquellas que lo serán”.

Robert S. Mueller III,
Director del FBI

Cuadro 1. Requisitos de protección

Identificar	Proteger	Detectar	Responder	Recuperar
<ul style="list-style-type: none">Responsabilidad de la Junta Directiva y la DirecciónGestión y evaluación de riesgosMonitoreo, revisión y cumplimiento	<ul style="list-style-type: none">Control de accesoProteger la informaciónProtección de estaciones de trabajo y servidoresEvitar el código maliciosoCifradoSeguridad de la redSeparación de entornosComputación en la nube públicaControles industrialesProteger los teléfonos móvilesGestión del cambioSeguridad de los soportes físicosCadena de suministro y externalizaciónSeguridad en las compras y el desarrolloProtección Física y AmbientalRecursos humanos y sensibilización de los empleadosCapacitación e instrucción	<ul style="list-style-type: none">Registro y monitoreoEvaluación de los controles de seguridadCiberdefensa proactiva	<ul style="list-style-type: none">Gestión de eventos	<ul style="list-style-type: none">Continuidad del negocio <div></div>

/04. Proceso de planificación organizacional

El proceso de planificación se compone de las siguientes etapas intuitivas:

Etapas 1: ¿Qué hay que defender? Identificación de los activos empresariales o procesos sensibles a los ataques cibernéticos.

Etapas 2: Impacto en los objetivos de la organización. Comprensión del impacto de los ciberataques sobre los activos o procesos del negocio mediante la realización de un cuestionario sobre el valor del negocio.

Etapas 3: ¿Cómo proteger correctamente? Controles necesarios que se derivan de los valores definidos en la etapa 2.

Etapas 4: Ideal versus real. Detección de las brechas defensivas en relación con los controles necesarios.

Etapas 5: Diseño de un plan de proyecto. Mejoramiento del nivel de defensa con el fin de alcanzar el nivel de riesgo deseado (incluyendo la comprensión de la exposición al riesgo, en caso de dejar de lado la instalación de los controles requeridos).

Gráfico 3. Etapas de defensa



/05.

Metodología de Ciberdefensa desde la perspectiva de la organización

Esta metodología presenta dos niveles diferentes de recomendaciones, que se derivan del daño potencial que puede sufrir una organización debido a un ciberincidente:

01

Organización de categoría A. Bajo potencial de daño. La organización llevará a cabo un proceso simple de identificación de los objetivos de protección con el fin de entender rápidamente el método de protección requerido.

02

Organización de categoría B. Potencial de daño significativo. Se trata de una organización que depende en gran medida del ciberespacio y que precisa llevar a cabo un proceso más detallado.

La clasificación se realiza después de responder a la pregunta que se plantea a continuación.

Si un ciberincidente ocurriera en su organización, ¿sería el costo de manipulación del incidente superior a NIS 500.000 (nuevos shekels israelíes)?

Dato: el costo de los daños resultantes de un incidente cibernético incluye los daños directos e indirectos para el negocio. Estos costos comprenden: el apagado temporal del servicio, el daño a la reputación, el costo de las sanciones impuestas a la luz de la violación de la ley y los requisitos reglamentarios, entre otros.

Al contestar a la pregunta es necesario tener en cuenta el costo total.

Las organizaciones que respondieron negativamente a la pregunta anterior pertenecen a la categoría A.

Las que respondieron afirmativamente pertenecen a la categoría B.

Requisitos adicionales: en el caso de que obligaciones adicionales se apliquen a la organización, en virtud de estar sujeta a regulaciones existentes, la empresa puede transferirse de la categoría A a la B. Además, una organización puede requerir a sus diversos proveedores satisfacer las necesidades de las organizaciones de categoría B.



Implementación de la Metodología de Ciberdefensa en organizaciones de categoría A

La Metodología de Ciberdefensa para las organizaciones de la categoría A se presenta en las páginas 24 a 29 de esta publicación.

Etapas 1: asignación de activos

Es necesario identificar los principales activos. Debe consultarse con el equipo de apoyo técnico sobre los tipos de equipos informáticos y los activos utilizados en la organización.

Gráfico 4. Identificación de activos

Consejo: asegúrese de que el proceso de asignación aborda los siguientes temas:



Etapas 2 y 3: nivel de protección requerido y cómo proteger correctamente. Los 10 mandamientos para una organización de categoría A

Una organización de categoría A requiere una protección coherente con el poten-

cial de daño. Por lo tanto, se precisa que implemente controles extremadamente costo efectivos.

Un desglose de los requisitos de protección se encuentra en el anexo 3 de la publicación. Estos controles se dividen en las 10 categorías de protección mencionadas en el recuadro 1.

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

- 1. Responsabilidad de la Dirección:** entender las amenazas informáticas existentes y elaborar un plan de trabajo para cerrar las brechas de defensa cibernética.
- 2. Evitar el código malicioso:** utilizar las tecnologías para hacer frente al software malicioso (malware) y actualizar las defensas del sistema de la organización.
- 3. Cifrado:** encriptar el acceso remoto de los empleados y proveedores, utilizando medios de cifrado comerciales. Encriptar el acceso a datos sensibles, utilizar un medio de comunicación encriptado (tanto para la navegación doméstica hacia la organización a través de redes inalámbricas como hacia los clientes y proveedores).
- 4. Computación en la nube y adquisición de software:** solicitar (por contrato) que el proveedor cumpla con los estándares comunes de software y protección de datos.
- 5. Protección de datos:** definir los mecanismos de protección para resguardar los datos existentes en la organización.
- 6. Protección del ordenador:** definir un nivel necesario de defensa del ordenador, incluyendo el cambio de las contraseñas por defecto en los equipos, eliminación de programas de software innecesarios, bloqueo de conexiones redundantes, eliminación de cuentas de administrador innecesarias.
- 7. Recursos humanos:** instruir a los nuevos empleados y retirar las autorizaciones a ex empleados.
- 8. Registro y seguimiento:** registrar y monitorear las actividades excepcionales, que pueden indicar la existencia de amenazas informáticas.
- 9. Seguridad de la red:** garantizar que el acceso a la red está bajo el control de la organización (proveedores y empleados no pueden conectarse remotamente a voluntad) y que la red está preparada para soportar ataques de denegación de servicio (DoS, por sus siglas en inglés).
- 10. Continuidad del negocio:** recuperar las capacidades a partir de fallas en el sitio, eliminación de datos, bloqueo de archivos.

Etapa 4: definición de las brechas de protección

Un examen de la aplicación de los controles se presenta en el anexo 3.

Se debe obtener una recomendación del proveedor de los servicios de tecnologías de la información (TI) sobre un plan de trabajo que priorice el manejo de las brechas.

Etapa 5: plan de trabajo

Todos los controles en la etapa de control protegen contra el riesgo cibernético derivado del daño cibernético. El control reduce el riesgo cibernético que podría perjudicar los objetivos de la organización.



Cuando se prepara un plan de trabajo para cerrar las brechas de control, debe tenerse en cuenta lo siguiente:

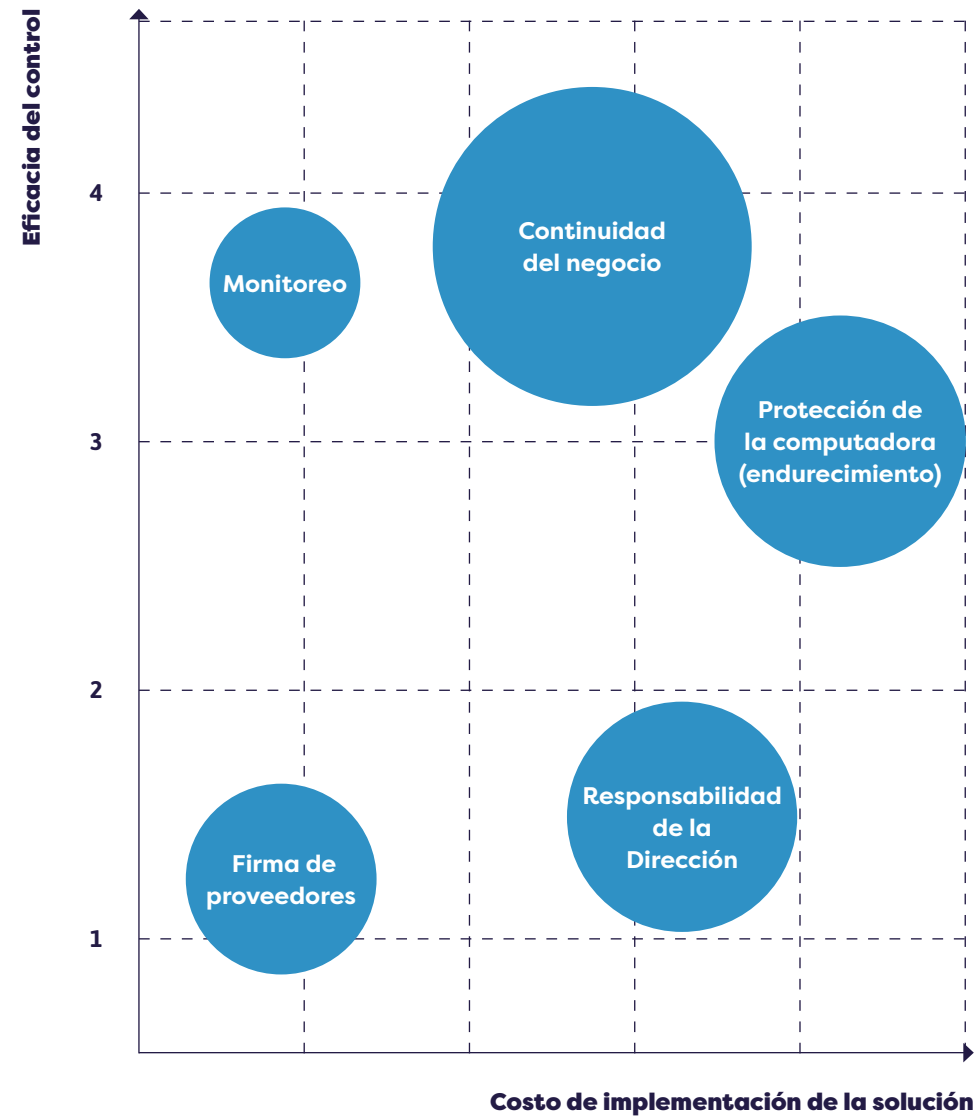
01
Eficacia del control: su contribución a la reducción del riesgo para la organización.

02
Costo de implementación de la solución: se representa en el gráfico 5 a través de un eje “costo de la solución” (duración de la aplicación, complejidad de realización, personal y equipos necesarios).

03
Velocidad de implementación: se representa en el gráfico 5 por el tamaño del círculo.

Un ejemplo de la ponderación de los parámetros mencionados anteriormente en una organización podría tener el aspecto presentado en el gráfico 5.

Gráfico 5. Costo de implementación de la solución versus eficacia del control



Cuadro 2. Cuadro de observaciones

Grupo de control	Existe / no existe	Eficacia del control	Costo de implementación	Ponderación de datos / priorización
Responsabilidad de la Dirección				
Prevención de código malicioso				
Cifrado				
Nube informática y compra de software				
Protección de datos				
Protección del ordenador				
Recursos humanos				
Registro y monitoreo				
Seguridad de la red				
Continuidad del negocio				

El plan de trabajo propuesto deberá ser refrendado o aprobado por el director general de la organización.

La lectura para una organización categoría A culmina aquí

Aplicación de la Metodología de Ciberdefensa en organizaciones de categoría B

Etapa 1: asignación de activos

La organización debe identificar sus activos, sus funciones e interfaces (servicios web, interfaces de programación de aplicaciones [API, por sus siglas en inglés], etc.). Se deben incluir los activos almacenados en la nube (todo como servicio [XaaS, por sus siglas en inglés]).

Esta primera etapa debe vincular los activos de tecnología operativa (OT, por sus siglas en inglés) y de TI a los principales procesos de negocio. Después de hacerlo la organización será capaz de distinguir entre los activos críticos y los secundarios, lo que la ayudará a proteger los activos en función del impacto.

El mapeo de activos incluirá, como mínimo, la lista presentada en el cuadro 3.

Cuadro 3. Identificación de activos

Tipo de activos	Nombre y fabricante	Propósito	Local / nube	Interfaces	Observaciones
Aplicación organizacional					Por ejemplo, almacén de datos (DWH, por sus siglas en inglés), gestión de relaciones con clientes (CRM, por sus siglas en inglés), planificación de recursos empresariales (ERP, por sus siglas en inglés), sistema informatizado de gestión de almacenes (WMS, por sus siglas en inglés), sistema de nómina, portal de la organización, etc.
Infraestructura					Por ejemplo, equipos de comunicación, telefonía, correo electrónico, almacenamiento.
Red					Por ejemplo, red de área local/red de área amplia (LAN/WAN, por sus siglas en inglés). inalámbrica, óptica, satelital.
OT					Por ejemplo, circuitos cerrados de televisión, sistemas de interfaz hombre-máquina (HMI, por sus siglas en inglés) controladores, etc.

Consejo: se debe asumir que todo aquello de lo que la organización no es consciente no está asegurado adecuadamente. Con el fin de llevar a cabo una identificación de todos los activos de TI, se debe obtener una lista completa de los activos del departamento de TI y trabajar con el departamento de compras, el cual tiene una lista completa de productos y servicios.

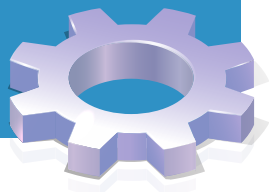
Mapeo de activos OT: se recomienda reunirse con los administradores de operaciones y de seguridad (especialmente en las organizaciones industriales).

Una organización que haya preparado un plan de continuidad del negocio puede utilizar la evaluación de daños y la evaluación de la dependencia de los procesos organizacionales de los activos de datos (uso del análisis de impacto en el negocio [BIA, por sus siglas en inglés]) para realizar el mapeo.

Atención: resolución del mapeo de objetivos

El mapeo de defensa es un proceso que requiere tiempo y recursos. Con el fin de llevarlo a cabo de manera efectiva, **se debe prestar atención a la resolución de mapeo requerida.**

Por ejemplo: por un lado, no es necesario especificar todos los servidores y terminales, pero, por el otro, definir de manera generalizada todos los servidores como un único activo puede resultar en costos desproporcionados de defensa.



Etapa 2: nivel requerido de defensa

El nivel de defensa requerido para cada activo se deriva del valor que la organización le otorga a ese activo. Dentro de la Metodología de Ciberdefensa, los activos se valoran en cuatro niveles: 1 señala un valor bajo mientras que 4 indica el valor más alto.

Consejo: sesgos comunes en la evaluación del valor de los activos. La evaluación de valor de los activos debe llevarse a cabo en cooperación con las unidades de negocio. Un propietario puede sobrevalorar su activo

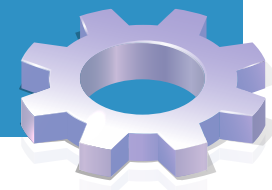
desde el aspecto comercial. Por eso, seguir el criterio del cuestionario para identificar el valor debería ayudar a evaluar correctamente los activos mediante una escala unificada y no sesgada.

Al final de la etapa 2, la organización será capaz de definir los activos más importantes para sus actividades comerciales.

Para completar el cuestionario, se requiere la estrecha colaboración de las entidades de negocio dentro de la organización, que comprenden la importancia de los activos y su influencia en el funcionamiento del negocio.

Atención: En ciberseguridad y seguridad de los datos es común evaluar el impacto potencial en tres categorías:

- C** **Impacto en la confidencialidad de los datos**, por ejemplo, un ataque informático destinado a filtrar detalles de los clientes a Internet.
- I** **Impacto en la integridad de los datos**, por ejemplo, un ataque cibernético con la intención de falsificar informes financieros de una empresa.
- D** **Impacto en la disponibilidad de los datos**, por ejemplo, un ataque cibernético para imposibilitar el acceso a la información de la empresa o de sus clientes (cierre de un sitio web, bloqueo de archivos o introducción de un software de secuestro de datos [ransomware]).



Se debe definir el nivel de valor de cada activo rellenoando el cuestionario incluido en el cuadro 4.

Cuadro 4. Cuestionario para determinar el nivel de valor de los activos

Pregunta	Nivel 1	Nivel 2	Nivel 3	Nivel 4
<p>1. ¿Cuál es el nivel de daño causado a la organización después de la fuga del activo?</p> <p>C</p> <p>Confidencialidad</p>	<p>El daño se estima en:</p> <p>A) el costo de hasta NIS 500.000 para la organización, y/o</p> <p>B) una inversión de hasta dos meses/hombre (<i>man-months</i>) para el manejo del incidente.</p>	<p>El daño se estima en:</p> <p>A) el costo de más de NIS 500.000, pero menos de NIS 5 millones para la organización, y/o</p> <p>B) una inversión de más de seis meses/hombre, pero menos de cinco años/hombre, para el manejo del incidente, y/o</p> <p>C) el activo se define como una base de datos a la que se aplica el nivel de seguridad medio, de acuerdo con la normativa de protección de datos de la Autoridad Israelí de Derecho, Información y Tecnología (ILITA, por sus siglas en inglés), y/o</p> <p>D) existe una clara amenaza para la salud pública.</p>	<p>El daño se estima en:</p> <p>A) el costo de más de NIS 5 millones para la organización, y/o</p> <p>B) una inversión de más de cinco años/hombre para el manejo del incidente, y/o</p> <p>C) el activo se define como una base de datos a la que se aplica el nivel de seguridad medio, de acuerdo con la normativa de protección de datos de ILITA, y/o</p> <p>D) existe un claro peligro para la vida humana.</p>	<p>Se producirá un daño significativo que incluirá uno de los dos escenarios siguientes:</p> <p>A) Existe un peligro claro y presente para la vida de muchas personas.</p> <p>B) El daño económico estimado es de más de NIS 20 millones.</p>
<p>2. ¿Cuál es el nivel de daño causado a la organización por la alteración o interrupción de la información existente en el sistema?</p> <p>I</p> <p>Integridad</p>				
<p>3. ¿Cuál es el nivel de daño causado a la organización debido a un apagado del sistema a largo plazo?</p> <p>D</p> <p>Disponibilidad</p>				



Nota: el valor de cada activo se define por la puntuación más alta recibida por las tres preguntas (impacto = MAX 1-3). Esta puntuación también se llama intensidad del riesgo y define el daño máximo que puede llegar a afectar a la organización en relación con cada activo.

Etapas 3: cómo proteger correctamente

En la etapa 2 se definió para cada activo el valor (intensidad) en una escala de 1 a 4. El grado de protección de cualquier activo deriva directamente de su valor (el valor resultante eleva el nivel de intensidad).

En la sección 6 de esta publicación, se indica en cada control de protección si se requiere para un activo cuyo puntaje de intensidad es 1, 2, 3 o 4.

Para cada activo, es necesario poner en práctica la totalidad de los controles cuyo valor es menor o igual a la puntuación de la intensidad del activo. Así, por ejemplo, para un activo cuya puntuación de intensidad es 3, es necesario poner en práctica todos los controles cuyo valor es 1, 2 y 3. Esta definición ayuda a ajustar los controles necesarios para aplicar la defensa que se precisa contra el daño potencial.

Etapas 4: definición de las brechas de protección

Se debe comprobar qué protección implementa la organización actualmente y qué necesita para llevar a cabo los controles de protección que figuran en el Cuadro 8. Al final de este proceso, la organización recibirá un listado de brechas (análisis de brechas).

Dado que no todos los controles se aplican de la misma manera en una organización, es importante asegurarse de que los objetivos esenciales de protección se examinan individualmente. Esto se debe al hecho de que un control no siempre está incluido en cada objetivo de la organización. La experiencia demuestra que a pesar de que la mayoría de los controles se implementan lateralmente en las organizaciones, existen no pocos casos en los que un control no se ha implementado en un sistema específico.

Debido a que no es necesario implementar todos los controles en todos los activos, tiene que utilizarse el nivel de valor para cada activo que se determinó en la etapa 3, para obtener el listado de brechas. Esta lista será la base para la construcción de plan de trabajo de la organización (etapa 5).

Calcular el nivel de riesgo de un activo: ponderar los datos

Se debe ponderar el impacto potencial (I) con la probabilidad de que tal evento cibernético ocurra.

La probabilidad (P) se calcula mediante la definición de un nivel de exposición de activos (por ejemplo, un activo vinculado a Internet que no tiene mecanismos de defensa está altamente expuesto a ataques cibernéticos, mientras que un activo aislado en una sala asegurada está menos expuesto).

Con el fin de definir el nivel de exposición de los activos, se debe responder al cuestionario incluido en el cuadro 5.



Cuadro 5. Cuestionario para determinar el nivel de exposición de los activos

Pregunta	1	2	3	4
1. ¿Cuántos usuarios existen en el sistema?	Hasta 50.	De 50 a 500.	De 500 a 5.000.	Más de 5.000.
2. ¿Quiénes son los usuarios del sistema?	Solo los empleados internos.	Proveedores externos regulares.	Proveedores externos casuales.	Público en general.
3. ¿Cuántas interfaces existen en el sistema?	Ninguna.	De 1 a 5.	De 5 a 10.	Más de 10.
4. ¿Cuál es la naturaleza de las interfaces del sistema?	Ninguna.	Interfaces dentro de la organización.	Interfaces externas con los proveedores.	Interfaces para el público en general.
5. ¿Qué tipo de información existe en el sistema?	Información no sensible para el negocio.	Información interna de la empresa.	Información médica o de clientes.	Información comercial sensible.
6. ¿Hay un acceso remoto al sistema?	No.	Vía autenticación de dos factores (2FA)	A través de un canal cifrado.	A través de un software de adquisición comercial.
7. ¿Cuál es el nivel de permisos de compartimentación en el sistema?	Compartimentación completa (permisos por grupos/roles).	Compartimentación individual (permisos individuales por empleado).	Compartimentación básica (gerente y usuario).	No existe compartimentación (permisos idénticos para todos).
8. ¿Cuál es el nivel de actualización del sistema?	La versión más reciente.	Hasta tres versiones hacia atrás.	Más de tres versiones hacia atrás.	Versiones que ya no son soportadas por el fabricante.
9. ¿Cuál es la política de actualizaciones y parches de seguridad?	Instalación de actualizaciones completas al menos una vez por trimestre.	Instalación solo de actualizaciones de seguridad al menos una vez por trimestre.	Solo actualizaciones críticas de seguridad, al menos, una vez por trimestre.	No hay un proceso ordenado de actualización.
10. ¿Cuál es el nivel de seguridad física del sistema?	Solo accesible a personas autorizadas.	Accesible a todos los empleados de la organización.	Accesibles a los contratistas externos.	Accesible a todos los visitantes de la organización.

Nota: La puntuación de exposición de cada activo es la media de las 10 preguntas (P = Promedio 1-10), también llamada probabilidad del riesgo (P).

Ponderar el nivel de riesgo, los costos de respuesta de un activo y la complejidad de la implementación

Con el fin de calcular el nivel de protección requerido, se debe multiplicar por tres la clasificación de impacto (I) y luego añadir la clasificación de probabilidad (P), como se muestra a continuación:

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

Nivel de riesgo de un activo = (Ix3) + P.

Un ejemplo de cálculo del riesgo de un activo se presenta en el anexo 1.

Después de esta etapa, la organización poseerá una lista que podría tener un aspecto como el presentado en el cuadro 7.

Cuadro 7. Controles

Control	Toda la organización	Sistema de gestión de relaciones con los clientes (CRM)	Sistema de pago a proveedores
4.30. Implementar una autenticación multifactor (MFA, por sus siglas en inglés) para acceder a cuentas con privilegios altos a través de la red.	Existe parcialmente.	Existe.	Necesario para implementar.
6.4. Configurar y poner en práctica medidas de seguridad para detectar y alertar sobre cambios no autorizados en los ajustes de configuración.	Hay un proceso ordenado en la organización.	El sistema está en la nube y no se tiene control directo sobre este requisito.	Existe.
16.2. Utilizar herramientas contractuales y legales en la compra de un sistema de información o de un servicio a proveedores.	No hay un proceso organizado para firmar con los proveedores.	El proveedor firmó una declaración.	Se trata de un proveedor del exterior con quien no es posible de firmar. Se van a considerar los requisitos del acuerdo genérico con él.

Etapa 5: plan de trabajo

Cada control en los capítulos de controles protege contra el riesgo cibernético derivado del daño cibernético.

En el marco del plan de trabajo, la prioridad de la aplicación de los controles que faltan en una organización se determinará por la ponderación del nivel de riesgo de los activos, el costo de la solución y la complejidad de la implementación. La prioridad de la aplicación de los controles que faltan se establecerá por la ponderación de:

01

El nivel de riesgo de los activos (eje vertical en el gráfico 6).

02

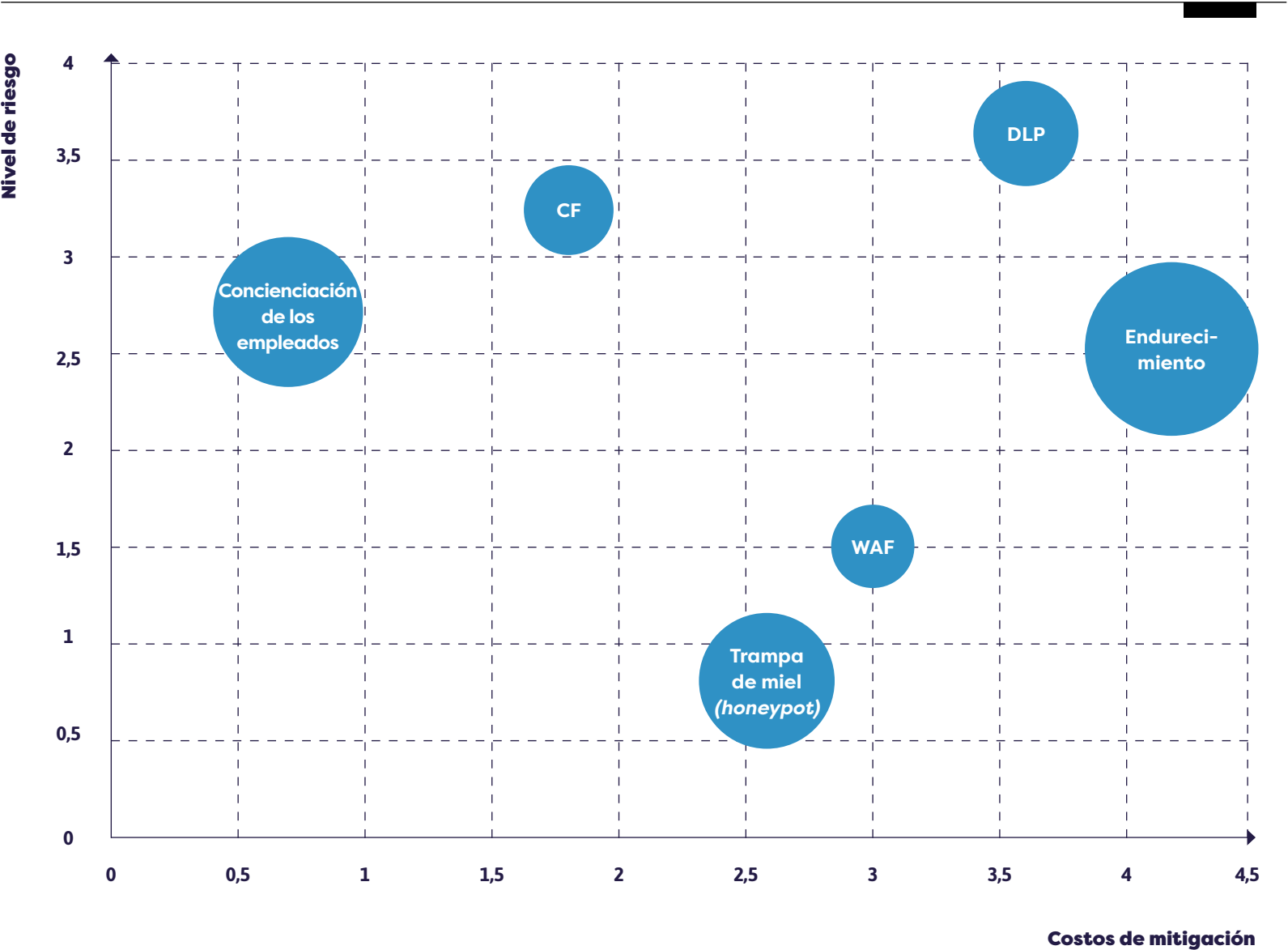
El costo de implementación de la solución (eje horizontal en el gráfico 6).

03

La velocidad de implementación de la solución (expresada por el tamaño de los círculos en el gráfico 6).

Gráfico 6. Ejemplo de ponderación del costo de realización, importancia del activo y velocidad de ejecución

Nota: CF: contafuegos; WAF: cortafuegos de aplicaciones web (siglas en inglés); DLP: prevención de pérdida de datos (siglas en inglés).



/06.

Capítulos de controles: etapas de implementación y control

Introducción

Los requisitos de protección de una organización se llaman profesionalmente controles. Con el fin de proteger a la organización en el campo cibernético, se requiere que la organización implemente controles en varios campos. Estos controles incluyen los procesos, procedimientos, sistemas y tecnologías de defensa que la organización ha implementado para reducir el riesgo de un incidente en el ciberespacio.

Estos controles se presentan divididos en diferentes temas, por ejemplo, de protección de los servidores y las estaciones de trabajo de gestión de usuarios, de seguimiento, entre otros.




Los controles de protección críticos (los que tienen el mayor valor costo-beneficio) se marcaron con un ícono de llave a fin de destacarlos.

A fin de construir una Metodología de Ciberdefensa proporcional, los controles se clasifican en niveles que oscilan sobre un eje de 1 a 4: los de nivel 1 son los más básicos y se requieren para cada organización y cada activo, y los de nivel 4 son los que se precisan para un objetivo de protección cuyo potencial de daño es 4.


Cómo proteger

Cuadro 8. Controles de seguridad para activos cibernéticos según tema y nivel

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
IDENTIFICAR					
1. Responsabilidad de la Junta Directiva de la Dirección Actualmente los activos cibernéticos son activos críticos necesarios para los objetivos de las organizaciones. Protegerlos puede ser tan importante como resguardar los activos físicos, las finanzas y los empleados. La ciberdefensa es responsabilidad de la Dirección de la organización. Esta responsabilidad ha de estar expresamente recogida en la visión acerca de la ciberdefensa de la Junta Directiva, en la política de ciberdefensa de la Dirección y en los procedimientos organizacionales para la ciberdefensa.					
Responsabilidad de la Junta Directiva	1.1	La Junta Directiva de la organización aprobará la política institucional de seguridad de la información y ciberdefensa una vez al año y asignará los recursos necesarios para su implementación.	Una vez al año, se presentará a la Junta la política institucional de seguridad de la información y ciberdefensa, la cual deriva del mapa de riesgo cibernético de la organización.	Al igual que cualquier programa de defensa, la ciberdefensa no es un ámbito herméticamente aislado, y la Dirección debe decidir el nivel de riesgo que está dispuesta a asumir, considerando los costos de los controles frente al precio de que el riesgo se materialice dentro de la organización e impacte en clientes, proveedores y objetivos nacionales. Además, la Dirección de la organización debe implementar mecanismos para manejar los eventos cibernéticos que puedan ocurrir destinados a reducir el daño a la organización. Se recomienda designar un representante entre los miembros de la Junta que concentrará los conocimientos sobre el tema a nivel directivo. En relación con este requisito, es importante asegurarse de que el mapa de riesgos se presente a la Junta Directiva en un lenguaje institucional junto con la respuesta actual de la organización y las medidas para subsanar las deficiencias y alcanzar un nivel aceptable de riesgo. Es importante que la Junta Directiva defina el nivel de riesgo que la organización debería tomar ("apetito de riesgo", por ejemplo, en función de una supuesta amenaza o de una relación de costo-beneficio).	2
Responsabilidad de la Dirección	1.2	Aprobar anualmente el mapa de riesgo actual, tal como surge del estudio de riesgo cibernético organizacional.	La organización trazará los riesgos a los que está expuesta en el campo cibernético. El riesgo se clasificará y se presentará a la Dirección junto con la definición de la respuesta planificada.	Las organizaciones con activos de nivel 2 pueden realizar un estudio independiente en el que se mapeen los activos y procesos operacionales sensibles y trabajar sobre la base del método de evaluación de riesgos de la Metodología de Ciberdefensa. En cuanto a las organizaciones con objetivos de protección de nivel 3 o superior, se recomienda utilizar un agente externo para llevar a cabo el estudio.	2
Responsabilidad de la Dirección	1.3	Identificar la legislación y los reglamentos de conformidad con la ley que sean aplicables a la organización.	Todos los requisitos pertinentes en virtud de la ley, una norma, un contrato con la organización y todas las medidas tomadas por la organización para cumplir con el requisito se definirán, documentarán y actualizarán claramente para todos los sistemas de información y actividades de ciberdefensa de la organización en su conjunto.	1. Preparar una lista de todos los requisitos legales, reglamentos y obligaciones contractuales que se han identificado. Un ejemplo de requisitos legales y reglamentarios puede ser el cumplimiento con el Ministerio de Justicia (registro de bases de datos y protección de la privacidad), la protección de las tarjetas de crédito de acuerdo con los requisitos estándar de la normativa de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés), los requisitos de los proveedores y clientes para el cumplimiento de los procedimientos de ciberdefensa firmados por la organización, manteniendo la propiedad intelectual y trabajando con software que posea una licencia en lugar de uno pirateado, etcétera. 2. Realizar y documentar auditorías de conformidad, indicando que en la organización se cumplen los requisitos anteriores.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
2. Gestión y evaluación de riesgos La Metodología de Ciberdefensa de una organización se basa en el proceso de gestión y evaluación de los riesgos cibernéticos. Se trata de un proceso cíclico que debe realizarse cuando el entorno cibernético de la organización está cambiando, tanto dentro de la organización (implantación de nuevos sistemas, cambios tecnológicos, cambios en los procesos operacionales, etc.) como fuera (cambio constante de las amenazas del ciberespacio para la organización).					
Gestión y evaluación de riesgos	2.1	Diseñar un proceso para establecer límites organizacionales, mapear los objetivos de defensa de la organización y evaluar el nivel de valor de los objetivos de defensa. 	El mapeo de los objetivos de defensa se puede lograr relevando los procesos de trabajo, sistemas, bases de datos e infraestructura tecnológica de la organización. El nivel de valor de los objetivos de defensa se determina de acuerdo con los efectos de la vulneración de la seguridad, la disponibilidad y la integridad de la información.	De acuerdo con esta Metodología, la gestión de riesgos en una organización requiere identificar los objetivos de la defensa, definir qué controles son necesarios para protegerlos y crear un plan de trabajo adecuado. La definición de los objetivos incluirá todos los aspectos en los que la organización debe considerar el nivel de riesgo actual frente al nivel deseado. Tales objetivos pueden incluir, entre otras cosas, una lista de sistemas, infraestructuras, procesos operacionales, personas clave y todo lo que la organización haya definido para sí misma como un objetivo de ciberdefensa. Ha de tenerse en cuenta que hay objetivos de defensa que se agregaron en los últimos años y que, por error, no se han relevado. Un buen mapeo incluirá, por ejemplo, el ámbito de IoT: cámaras de seguridad, ascensores y escaleras eléctricas, ensamblaje y otros componentes “integrados en software”, que a menudo no son administrados por los profesionales de TI de la organización (no constituyen activos de TI clásicos). Estos activos a menudo están en el centro de la acción del funcionamiento de la organización y no son menos vulnerables a los ataques cibernéticos (puede ser una noria en un parque de atracciones, una bomba de combustible, un sistema de aire acondicionado central, un sistema de mando y control para turbinas, etcétera).	2
	2.2	Definir e implementar un proceso periódico de evaluación de riesgos cibernéticos de acuerdo con el perfil de amenazas de la organización, el nivel de exposición a las amenazas de los objetivos de defensa y los controles de protección implementados en la organización.	El propósito del proceso de evaluación de riesgos es proporcionar un mapa actualizado de los riesgos cibernéticos reales (riesgos residuales) a fin de definir un plan para abordar los riesgos. El estudio debe llevarse a cabo periódicamente y actualizarse para tener en cuenta los cambios en los procesos y sistemas de la organización.	Es posible basar el proceso de evaluación de riesgos en la Metodología de Ciberdefensa.	2
3. Monitoreo, revisión y cumplimiento Todas las organizaciones han de proteger sus activos cibernéticos para cumplir con los criterios legales básicos de la protección de los derechos de autor (por ejemplo, no usar software no autorizado), proteger los registros corporativos y la información privada que se encuentra en la base de datos de la compañía. Si hay información codificada, esta se mantiene siguiendo las normas legales específicas.					
Algunas organizaciones deben cumplir requisitos legales adicionales. La organización debe implementar mecanismos de control para verificar de manera continua que cumple con los requisitos de la ley, con la normativa pertinente, de acuerdo con el sector (salud, seguros, mercados de capitales, etc.), así como con esta Metodología de Ciberdefensa, la directiva de la Junta y las decisiones de la Dirección en materia de ciberdefensa.					

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Control, revisión y cumplimiento	3.1	Revisar periódicamente los diversos procesos de información con el fin de garantizar el cumplimiento de las normas y la política de seguridad así como todos los requisitos de seguridad de la información.	Se debe realizar un “estudio de gestión” de los diversos procesos para confirmar que se cumplen las normas y requisitos de seguridad de la información. En ese estudio se examinarán los diversos parámetros en el campo de la ciberdefensa y se ofrecerá a la Dirección un panorama de las fortalezas y puntos débiles de la organización.	Un estudio de gestión proporciona una visión lateral sobre el estado de la organización desde el punto de vista de su nivel actual de protección. Tales estudios presentarán a la organización las áreas a las que debe prestar mayor atención, en comparación con aquellas en las que está más avanzada (como el modelo de madurez de capacidades [CMMI, por sus siglas en inglés]). Las áreas a las que puede referirse el estudio pueden ser, por ejemplo, desarrollo seguro, nivel de sensibilización, capacidades de monitoreo, nivel de madurez de los equipos de respuesta, procedimientos de la organización, etcétera. Es importante asegurarse de que los procesos que se definen como críticos en el marco del programa de continuidad del negocio de la organización reciban una respuesta de protección adecuada.	2
	3.2	La organización garantizará la redacción de una política de protección, que abordará todos los aspectos detallados en este documento.	El propósito del monitoreo es asegurar que la Dirección de la organización haya definido sus pautas con respecto a los aspectos de protección de varias cuestiones, tales como directivas de protección de recursos humanos, directivas de protección de la cadena de suministro, directivas de monitoreo y control, etcétera.		
Control, revisión y cumplimiento	3.3	Asegurarse de que los diversos sistemas de información cumplan con los estándares de seguridad de la información corporativa y de ciberdefensa, y que se implementen de manera segura y regular, de acuerdo con la política de seguridad de la información y de ciberdefensa de la organización.	Se deben realizar revisiones periódicas para garantizar que los diversos sistemas de información cumplan con los requisitos de seguridad de la información y de ciberdefensa que la organización haya establecido, y que sean inmunes a los ataques.	La implementación adecuada de esta labor de monitoreo se llevará a cabo escribiendo un plan corporativo anual o plurianual para realizar estudios cibernéticos periódicos sobre los activos corporativos. Los estudios pueden ser en forma de caja blanca o gris o de caja negra, y se prioriza la revisión de los sistemas que recibieron una puntuación alta en el cuestionario de valores. Con respecto a los sistemas de nivel 3, se recomienda que un organismo independiente fuera de la organización realice la revisión.	2
Monitoreo, auditoría y cumplimiento	3.4	Verificar automáticamente el nivel de protección de la organización.	Utilizar herramientas automatizadas que simulen la actividad del atacante automáticamente.	Dado que realizar pruebas de penetración es una acción que requiere la participación humana en su mayor parte, la capacidad de cubrir muchos sistemas en tiempo real es limitada. A fin de abordar las limitaciones de tiempo y conocimientos, hay algunos productos que permiten al Director de Defensa recibir notificaciones usando herramientas que simulan un “juego de guerra” y un ataque a la organización mediante varios métodos, con el fin de detectar los vectores de ataque y los puntos débiles que se deben abordar.	4

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
PROTEGER					
4. Control de acceso Muchos agentes necesitan acceder a la información de la organización para su correcto funcionamiento, tanto agentes humanos (empleados, clientes y proveedores de la organización) como elementos tecnológicos (aplicaciones). Estos últimos precisan acceder a diferentes sistemas y tipos de información. Para evitar abusos en tal acceso, la organización debe implementar un monitoreo y una protección adecuados, lo que asegurará que todos los agentes puedan acceder exclusivamente a la información que necesitan y que ninguna parte no autorizada pueda utilizarla.					
Control de acceso	4.1	Desarrollar, documentar e implementar una directiva de control de acceso.	La directiva de control de acceso está diseñada para garantizar que solo las partes autorizadas puedan acceder a la información y los sistemas de la organización para ver y realizar cambios, todo de acuerdo con las definiciones de sus funciones y sujeto a supervisión.	La directiva de control de acceso de la organización puede incluirse como un capítulo de su política de seguridad de la información.	2
Control de acceso	4.2	Configurar cuentas de usuario coherentes con las funciones operacionales de la organización. 	Como mínimo, separe las cuentas de “administrador” de las de “usuario”. También es necesario configurar usuarios que administren las funciones de seguridad del sistema (como crear usuarios, administrar el acceso y los privilegios del sistema, administrar los sistemas de seguridad de la información, etcétera).	Creación de usuarios corporativos como usuarios estándar, definiendo usuarios “administradores” solo para determinadas funciones.	1
Control de acceso	4.3	Examinar la lista de usuarios periódicamente y actualizarla en consecuencia.	La organización examinará cada cierto período predefinido la lista de usuarios y eliminará usuarios irrelevantes, según sea necesario.	Los administradores de sistemas realizarán el proceso de revisión periódica de los usuarios y su documentación mediante la organización del procedimiento de control de acceso y el monitoreo continuo a través de una matriz automática o manual.	2
Control de acceso	4.4	Deshabilitar o eliminar cuentas temporales automáticamente después de un tiempo especificado. 	La organización establecerá un período de tiempo fijo después del cual la cuenta temporal se bloqueará automáticamente.	Si es posible, configurar cuentas temporales con una asignación de tiempo para cualquier sistema que interactúe con un directorio activo (Active Directory), un sistema de administración o uno de gestión de identidades (IDM, por sus siglas en inglés). Las cuentas que deben extenderse requieren una aprobación especial.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Control de acceso	4.5	Deshabilitar o eliminar cuentas temporales automáticamente después de un tiempo especificado.	La organización deshabilitará o eliminará cuentas inactivas después de un período de tiempo fijo que se definirá en la política.	Se deben emitir informes periódicos sobre la actividad de inicio de sesión de los usuarios en el sistema que interactúe con un Active Directory, así como con las cuentas que se cerraron hace mucho tiempo (como se define en el procedimiento de control de acceso). Se deben eliminar tales cuentas.	3
Control de acceso	4.6	Documentar en un registro de inicios de sesión automático cualquier actividad de creación, modificación, habilitación, deshabilitación y eliminación de cuentas.	La organización documentará cualquier cambio en las cuentas de usuario y realizará un seguimiento automático o manual de la ejecución de la documentación.	Esto se puede implementar a través del sistema de gestión de información y eventos de seguridad (SIEM, por sus siglas en inglés), que interactuará con los sistemas de administración por tareas en la organización (Active Directory, administración de identidades, servidores, sistemas aplicativos así como equipos de seguridad de la información y la comunicación).	3
Control de acceso	4.7	Monitorear la actividad de la cuenta para detectar cualquier uso anómalo y notificar todo uso inusual a los funcionarios correspondientes.	Ejemplos de uso anómalo son los siguientes: iniciar sesión en el sistema en ciertos días y en ciertos momentos, iniciar sesión desde direcciones incompatibles con el patrón de uso normal.	Se puede aplicar utilizando un sistema SIEM para monitorear usuarios en grupos sensibles. La recopilación de información se realizará a partir de fuentes como Active Directory, comunicaciones y equipos de seguridad de la información (cortafuegos, etcétera).	3
Control de acceso	4.8	Definir y aplicar condiciones para bloquear cuentas.	Ejemplos de condiciones de bloqueo de entrada son el fin de semana u horario nocturno.	Es posible definir en la configuración del usuario una restricción de entrada en la cuenta de Active Directory, de modo que no se permita la conexión durante horas no laborables.	4
Control de acceso	4.9	Definir y aplicar privilegios de acceso lógico al sistema y a la información de acuerdo con la política de control de acceso.	El control de acceso se puede realizar a nivel personal (basado en la identidad) o a nivel de función (basado en la función), y tiene como objetivo controlar el acceso de las entidades (usuarios o procesos informáticos) a los objetos (archivos, registros, dispositivos, etcétera).	Los usuarios se gestionarán de forma centralizada a través de un directorio empresarial de la organización, por ejemplo, Active Directory, protocolo ligero de acceso a directorios abierto (LDAP, por sus siglas en inglés) u otros. El sistema por tareas se asignará al perfil de usuario.	1
Control de acceso	4.10	Limitar los privilegios del usuario al mínimo esencial para realizar sus tareas.	La organización definirá un nivel mínimo de privilegios para cada función, así como un nivel mínimo de privilegios para un usuario básico (sin una función definida) necesario para acceder a los sistemas de la organización.	Los privilegios del usuario dependerán de su función. Se definirá y otorgará un perfil básico al usuario, y se establecerán privilegios adicionales de acuerdo con las necesidades y tras la aprobación de un supervisor directo. Si hay un sistema IDM, se pueden asignar un perfil básico y perfiles de aplicación. Tras mejorar el proceso, se otorgarán privilegios dependiendo de la función.	2


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Control de acceso	4.11	Definir los funcionarios, llevar a cabo una separación de funciones y otorgar los correspondientes privilegios de acceso en el sistema.	El propósito de la separación de funciones es reducir el potencial de abuso de privilegios. En ella se incluye, por ejemplo, separar las funciones operacionales entre empleados o funcionarios y garantizar que el equipo de seguridad de la información que gestiona el control de acceso administre, al mismo tiempo, las funciones de revisión del control de acceso.	Se debe realizar e implementar un mapeo por tareas que admita una separación de poderes dentro de los perfiles de privilegios de los usuarios; por ejemplo, un desarrollador frente a un probador de <i>software</i> (cada uno de ellos tendrá acceso a un entorno diferente: un desarrollador trabajará en un entorno de desarrollo de menor amplitud; un probador trabajará en un entorno superior, de preproducción), etcétera.	3
Control de acceso	4.12	El acceso a sistemas y aplicaciones sensibles se realizará exclusivamente a través de un componente endurecido previamente determinado (terminal).	Con el fin de aplicar una política uniforme “reforzada” a los recursos sensibles, hay que asegurarse de que el acceso a ellos se realizará solo después de pasar por el componente de mediación (como un servidor proxy o un terminal).	Es posible ejercer este control definiendo el acceso en el componente del cortafuegos de modo que la conexión a activos confidenciales se permita solo a través del componente de enlace, incluidas las pruebas y la estricta política corporativa (como evitar que pueda hacerse un copipega, impedir la descarga de archivos, bloquear la interfaz de línea de comandos [CLI, por sus siglas en inglés], etcétera).	4
Control de acceso	4.13	Determinar los empleados autorizados a publicar información en un sistema accesible al público (como un sitio web) e implementar esta autorización en el marco del proceso de otorgamiento de privilegios.	La organización definirá a los usuarios cuyo trabajo requiere publicar información en fuentes públicas y documentará las funciones mencionadas anteriormente como parte del procedimiento de la organización.	En los sistemas de administración de contenido (CMS, por sus siglas en inglés), es necesario otorgar derechos de edición y privilegios de publicación solo a los administradores de contenido.	3
Control de acceso	4.14	Restringir el inicio de sesión de los usuarios en el sistema después de varios intentos fallidos de inicio de sesión, utilizando la opción de bloqueo de inicio de sesión durante un tiempo específico o hasta que un administrador del sistema lo libere.	El propósito de este monitoreo es hacer frente al riesgo de ataques DoS. Este control debe implementarse tanto en el nivel de conexión al sistema operativo como en el de conexión a aplicaciones específicas.	Es posible limitar el número de intentos fallidos de inicio de sesión dentro de la directiva de grupo y la de dominio.	2
Control de acceso	4.15	Limitar el número de conexiones permitidas simultáneamente de un solo usuario.	El propósito de este monitoreo es detectar la conexión desde dos lugares diferentes utilizando la misma identificación. Esa situación podría ser una indicación de un uso no autorizado de la cuenta de un usuario.	Se puede limitar el número de conexiones simultáneas en la directiva de inicio de sesión remoto dentro de la política de grupo.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Control de acceso	4.16	Bloquear las conexiones resultantes de la inactividad temporal y desactivar la conexión continua hasta la identificación y autenticación del usuario. Como parte del bloqueo de la conexión, ocultar la información que ha aparecido en la pantalla antes del bloqueo.	Este control generalmente se aplica a nivel del sistema operativo, pero también se puede implementar a nivel de la aplicación. Cabe señalar que un bloqueo de conexión no es un sustituto regular del cierre de sesión.	Esto se puede lograr configurando un protector de pantalla. Si es posible, asegúrese de que los sistemas de autodesarrollo y los de productos de plataforma incluyan un mecanismo de tiempo de espera de sesión.	3
Control de acceso	4.17	Definir e implementar restricciones de uso y requisitos de configuración para la conexión remota. 	Se requiere una directiva para manejar las conexiones remotas, que defina los límites del uso de la conexión remota a los recursos de la organización. También se han de usar sistemas que brinden acceso remoto seguro a los recursos de la organización.	Es posible implementar un acceso seguro a la organización a través de sistemas como una red privada virtual (VPN, por sus siglas en inglés) o un intérprete de comandos seguro (SSH, por sus siglas en inglés), que son coherentes con las directivas corporativas para la conexión remota a los recursos de la organización.	2
Control de acceso	4.18	Monitorear las conexiones remotas.	El monitoreo automático de las conexiones remotas permite a las organizaciones detectar ciberataques, así como garantizar el cumplimiento de los procedimientos de acceso remoto controlando las actividades realizadas durante la conexión a distancia.	Es posible interconectar los sistemas de acceso remoto con sistemas de monitoreo, como el SIEM, y verificar que los eventos de inicio de sesión estén realmente registrados.	3
Control de acceso	4.19	Dirigir todas las conexiones remotas a través de un número determinado de puntos de control administrados de acceso a la red.	Reducir el número de puntos de control de acceso disminuye la superficie de ataque.	Revisar el mapeo de superficie de ataque de la organización y transferir servicios corporativos sensibles al área de red ubicada detrás del cortafuegos. Redireccionar el tráfico hacia ella desde la red VPN a través del acceso desde el servidor VPN. Eliminar el acceso directo desde fuera de la organización para acceder a estos servicios.	3
Control de acceso	4.20	Implementar salvaguardas adicionales cuando se ejecuten comandos sensibles a través de una conexión remota.	Los comandos sensibles son, por ejemplo, arrancar un servidor o cancelar una transacción. Asegurarse de que sea imposible ejecutar dichos comandos en el marco de un sistema de inicio de sesión normal.	El acceso a servidores confidenciales y a la administración de sistemas se llevará a cabo mediante una red de administración fuera de banda, a la que se puede acceder a través de un servidor de administración dedicado (que requiera identificación y autenticación).	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Control de acceso	4.21	Prohibir el inicio de sesión remoto para administrar el sistema y limitar el acceso al sistema desde redes que no sean administradas por la organización.	La organización no permitirá el acceso remoto directo a las interfaces de administración, a menos que sea de forma segura, y solo después de la verificación y la conexión a una red de administración.	Se debe evitar el inicio de sesión del administrador cuando se conecta de forma remota a los sistemas (también se puede hacer en Linux eliminando PermitRootLogin).	4
Control de acceso	4.22	Proteger la conexión a un sistema desde una red inalámbrica utilizando autenticación de usuarios y dispositivos, cifrado y configuración de límites de uso.	La organización permitirá la conexión a una red inalámbrica solo para dispositivos administrados y autenticados por ella, y solo para usuarios identificados.	El acceso a la red inalámbrica se permitirá solo después de la identificación frente al punto de acceso.	2
Control de acceso	4.23	Calibrar la intensidad de la señal inalámbrica para reducir las posibilidades de que se reciba fuera de las instalaciones de la organización.	La organización revisará las señales de transmisión de las redes inalámbricas y se asegurará de que la señal no exceda un rango predefinido.	El mapeo del rango de recepción puede llevarse a cabo utilizando una visión general espacial y un equipo especial (radio) en coordinación con el proveedor del sistema inalámbrico. También se puede hacer de forma independiente a través de un analizador de radio y tomando medidas alrededor del área del edificio.	4
Control de acceso	4.24	Prohibir la conexión a los sistemas de la organización desde una red inalámbrica.	El acceso a los sistemas de la empresa se permitirá solo a equipos informáticos conectados por cable a la red de la organización.	No se han de conectar redes inalámbricas a la red de la organización, sino únicamente en un enrutador de Internet dedicado solo para navegar. También es posible implementar un servidor proxy de la red inalámbrica.	2
Control de acceso	4.25	Definir e implementar restricciones de uso y requisitos de configuración para la conexión a través de dispositivos móviles.	La organización definirá e implementará una directiva para monitorear la seguridad de la información para los dispositivos móviles que accedan a los sistemas de la organización. Esta directiva debe abordar tanto los dispositivos proporcionados y administrados por la organización como los dispositivos personales de los empleados o invitados de la organización.	Definir una directiva de dispositivos móviles que determine los límites del uso de esos dispositivos (como teléfonos celulares y tabletas): qué contenido puede guardarse y a qué contenido se puede acceder en la organización a través de un dispositivo móvil.	2
Control de acceso	4.26	Implementar un cifrado completo de la información almacenada en los dispositivos móviles para proteger la confidencialidad e integridad de la información.	La organización cifrará el espacio en disco de los dispositivos móviles que se conectan para conducir sus sistemas.	Esto se puede realizar a través de una directiva que se distribuirá a los dispositivos móviles mediante la administración de tales dispositivos y será compatible con la mayoría de los dispositivos de Android y Apple.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Control de acceso	4.27	Prohibir el inicio de sesión en un sistema sensible mediante dispositivos móviles.	La organización bloqueará y ejecutará mediante controles tecnológicos el acceso a sistemas organizacionales sensibles mediante dispositivos móviles.	Esto puede hacerse identificando el navegador del dispositivo móvil o no permitiendo la exposición de sistemas sensibles a las redes a las que acceden los dispositivos móviles (ni detrás del segmento de VPN o, alternativamente, conectando dispositivos móviles a un segmento de VPN que sea diferente al de las otras computadoras).	4
Control de acceso	4.28	Identificar y validar únicamente a los usuarios del sistema.	La organización verificará de manera inequívoca a un usuario que se conecta a los sistemas de la organización.	Cada usuario del sistema tendrá un nombre de usuario único (que se asigna a una persona en particular). En cuanto al usuario genérico, se indicará quién tiene el nombre de usuario genérico y los usuarios aplicativos serán propiedad del administrador del sistema.	2
Control de acceso	4.29	Implementar una MFA para iniciar sesión en cuentas con privilegios excesivos en toda la red.	La organización implementará la identificación local por varios medios de identificación (dos o más) en cuentas sensibles.	Se puede realizar, por ejemplo, mediante el uso de tarjetas magnéticas, huellas digitales u otros mecanismos compatibles con Active Directory.	2
Control de acceso	4.30	Implementar la MFA para el inicio de sesión local de cuentas con privilegios excesivos.	La organización implementará la identificación por varios medios (dos o más) en cuentas sensibles en el inicio de sesión local.	Se puede realizar, por ejemplo, mediante el uso de tarjetas magnéticas, huellas digitales u otros mecanismos compatibles con Active Directory.	3
Control de acceso	4.31	Establecer un mecanismo de autenticación que resista a los ataques de reproducción para conectar cada cuenta (con énfasis en un mecanismo de verificación por medios de cifrado).	La organización implementará un mecanismo de identificación a prueba de escuchas (como un mecanismo de identidad que emite una identificación única) para todas las cuentas.	Se puede realizar a través de mecanismos como tarjetas inteligentes o contraseña de un solo uso (OTP, por sus siglas en inglés).	4
Control de acceso	4.32	Implementar la MFA para conectarse de forma remota al sistema.	La organización implementará la identificación remota por varios medios (dos o más) para los sistemas de la organización.	Se puede realizar a través de mecanismos como tarjetas inteligentes u OTP en el acceso remoto a sistemas como VPN.	2
Control de acceso	4.33	Identificar y validar dispositivos únicos que están en proceso de conexión.	La organización reconocerá inequívocamente los dispositivos que se conectan a la red corporativa.	Esto se puede hacer usando certificados digitales emitidos para un punto de conexión y una computadora portátil.	3




Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Control de acceso	4.34	Gestionar medios de identificación para el sistema, como por ejemplo, seleccionar los medios de identificación de un empleado o titular de la oficina y su ubicación y bloquearlos tras un tiempo sin uso.	Administrar un conjunto de métodos de identificación y su emisión. Además, es posible cancelar los medios de identificación a través de un sistema central.	Se puede realizar a través del sistema de gestión de OTP si se requiere un medio de identificación más robusto que el sistema existente.	2
Control de acceso	4.35	Aplicar una política de contraseña mediante medios tecnológicos.	La aplicación de la política debe incluir, al menos, establecer una complejidad mínima, variar las contraseñas anteriores, establecer el tiempo de vencimiento, fijar un requisito para definir una nueva contraseña después de un inicio de sesión inicial.	Se puede realizar utilizando la directiva de grupo y la de dominio.	2
Control de acceso	4.36	Asegurarse de que los comentarios del sistema de información a lo largo del proceso de verificación no brinden información que pueda causar daño si se descubre o si llegara a ser utilizada por partes no autorizadas.	Camuflar los campos de autenticación ocultando la contraseña.	Se puede hacer mediante mecanismos integrados en los sistemas operativos. También se puede implementar en páginas web definiendo el campo como una contraseña.	2
Control de acceso	4.37	Implementar un mecanismo de autenticación cifrada.	El objetivo es que la información de identificación no quede expuesta (contraseñas no cifradas). La información de identificación expuesta se puede robar si se transfiere a través de un medio de comunicación no cifrado, por ejemplo, en caso de un ataque de intermediario (MITM, por sus siglas en inglés).	Se puede realizar a través de mecanismos como tarjetas inteligentes u OTP.	2
5. Proteger la información En la era digital actual la información es uno de los activos más importantes para la mayoría de organizaciones, ya sea información comercial, datos de clientes o cualquier información recopilada y mantenida por la organización para sus operaciones.				En consecuencia, la organización debe actuar para proteger su información contra el robo, manipulación o eliminación, y a veces incluso está obligada a hacerlo en virtud de la legislación vigente. Estos controles se aplican para proteger la información en sí misma: su clasificación, almacenamiento, portabilidad, etcétera.	

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Proteger la información	5.1	Evitar la transferencia de datos no autorizada o no intencional a través de recursos compartidos del sistema. 	La organización debe evitar la transferencia de información de manera no autorizada, por ejemplo, mediante el uso de carpetas compartidas, correo electrónico, medios extraíbles, etcétera.	Restringir el uso de carpetas compartidas para transferir información, especialmente cuando hay tareas para partes no autorizadas. Es posible utilizar un sistema de prevención de pérdida de datos para evitar que se transfiera la información almacenada en carpetas compartidas.	1
	5.2	Crear e implementar políticas y procedimientos para proteger la información y actualizarlos periódicamente.	La política debe incluir, al menos, una referencia a varios tipos de información en la organización o sistema. También debe contener definiciones claras sobre la obtención de información más allá de los límites de la organización y el método de divulgación de esa información. Además, es necesario hacer referencia a todos los canales y equipos terminales de la organización: estaciones de trabajo, servidores, equipos móviles, incluidas computadoras, tabletas, teléfonos móviles y equipos informáticos portátiles (relojes inteligentes, etcétera).	Este control puede implementarse redactando un documento de política sobre la protección de la información en la organización. En él deben incluirse definiciones para los diversos tipos de información en la organización y qué tipos de información se pueden enviar fuera de la organización. Además, es necesario elaborar procedimientos complementarios sobre cómo se envía la información de forma segura.	2
Proteger la información	5.3	Elaborar e implementar una directiva de clasificación de la información organizacional y procedimientos de implementación para los empleados de la organización con el propósito de clasificar la información.	La directiva de clasificación debe incluir definiciones claras sobre cómo y de qué manera clasificar cada tipo de información específica. También se debe agregar un procedimiento para guiar la manera de manejar cada clasificación de información.	1. Describir los tipos de información disponibles en la organización de acuerdo con su importancia, según las necesidades de la organización o las normas y reglamentos aplicables a la organización. 2. Crear una matriz que contenga todas las categorías de clasificación: lo que se incluye en cada clasificación (es decir, qué tipos de información: privada, comercial, sanitaria, de seguridad pública, etc.) y los diferentes tipos de manejo de la información (almacenamiento, transferencia, destrucción, protección física y lógica, etcétera).	3
Proteger la información	5.4	Implementar salvaguardas para evitar la filtración de información al transferirla a partes internas o externas.	La organización debe implementar mecanismos para proteger la información cuando se mueva entre sistemas de la organización y cuando la envíe a terceros fuera de la organización, de acuerdo con la política de protección de la información corporativa.	Se puede realizar utilizando varias tecnologías, cada una de las cuales puede evitar ciertos escenarios: 1. Un sistema de prevención de fugas de información. 2. Un sistema seguro para transferir información, como correo electrónico seguro o cifrado, caja fuerte electrónica, etcétera.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Proteger la información	5.5	Implementar mecanismos de protección para monitorear y evitar el acceso, uso o eliminación de información definida como sensible por la organización a entidades no autorizadas dentro y fuera de la organización.	La organización debe implementar mecanismos para proteger la información mientras la guarda en las matrices de almacenamiento de la organización, que pueden ser servidores físicos, virtuales y en la nube, así como al proteger las estaciones de trabajo de la organización. Asegurarse de que los mecanismos de protección no permitan la replicación, impresión, envío, eliminación, etc., de información definida como confidencial según la política establecida con respecto a esa información.	Eso se puede realizar utilizando tecnologías para evitar la filtración de información con el fin de monitorear, advertir y prevenir estas acciones. También se puede llevar a cabo utilizando soluciones de protección de documentos (seguridad de los documentos), así como mediante el monitoreo y la restricción del acceso a archivos confidenciales (de lo que se trata en detalle en los apartados sobre control de acceso y monitoreo).	3
Proteger la información	5.6	Evitar la operación remota de accesorios informáticos (cámaras web, micrófonos, altavoces, auriculares o cualquier accesorio que pueda estar conectado a una PC) y establecer una indicación explícita de que los accesorios están físicamente activos con el usuario.	Bloquear o deshabilitar la operación remota de cámaras, micrófonos, etcétera.	Es preferible bloquear permanentemente los accesorios informáticos que no se utilizan para reducir este riesgo.	3
6. Protección de estaciones de trabajo y servidores Las estaciones de trabajo y los servidores son el equipo informático básico en cualquier organización. Su protección es fundamental para evitar ataques a la organización y resguardar la información corporativa.				Las estaciones de trabajo y los controles de protección del servidor tienen varias capas de protección: servicios de endurecimiento (lista blanca y negra), evitar la aparición de brechas de seguridad de forma maliciosa o accidental, etcétera.	
Protección de estaciones de trabajo y servidores	6.1	Definir, documentar e implementar una directiva de endurecimiento para estaciones de trabajo y servidores, que cumpla con los requisitos de seguridad de la información de la organización.	La organización definirá los requisitos de endurecimiento para los sistemas dentro de la organización con énfasis en cuáles son los requisitos básicos, la frecuencia de las actualizaciones y el nivel de clasificación. Luego documentará los requisitos en un marco general que servirá como base para los procedimientos de endurecimiento.	Es posible utilizar documentos de referencia de los fabricantes oficiales y las organizaciones normativas, como la Agencia de Sistemas de Información de Defensa (DISA, por sus siglas en inglés), el Instituto de Administración de Sistemas, Auditorías, Redes y Seguridad (SANS, por sus siglas en inglés), etc. Además, en los procedimientos de la organización se ha de definir quién es responsable de implementar el endurecimiento real y cómo se lleva a cabo la prueba continua de los controles. La documentación sobre el endurecimiento incluirá, entre otras cosas, una referencia al uso de servicios no autorizados y servicios seguros, los puertos aprobados, la eliminación de cuentas inactivas, etcétera. Es importante asegurarse de que el endurecimiento se llevará a cabo de acuerdo con la funcionalidad relevante de la aplicación (como el endurecimiento de los servidores Internet Information Services [IIS] frente a Tomcat, el endurecimiento del servidor web frente a un endurecimiento del servidor de base de datos, etcétera).	1

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Protección de estaciones de trabajo y servidores	6.2	Establecer mecanismos para la gestión, implementación y validación centralizadas de la configuración del sistema.		En sistemas Windows es posible usar herramientas de directiva de grupo como Active Directory; en sistemas Linux se puede recurrir, por ejemplo, a herramientas de Red Hat o, alternativamente, a una herramienta de administración y distribución de configuración automática como Chef.	3
Protección de estaciones de trabajo y servidores	6.3	Implementar una directiva para controlar, aplicar y monitorear la instalación de <i>software</i> en las PC de la organización.	El propósito de ese control es asegurarse de que el <i>software</i> se instale en los dispositivos y servidores solo con aprobación y después de examinar la necesidad y riesgo involucrado en el uso del <i>software</i> .	Este control se puede realizar restringiendo las cuentas de usuario para la instalación y modificación de los dispositivos de <i>software</i> , así como mediante el uso de una herramienta de control de aplicaciones.	2
Protección de estaciones de trabajo y servidores	6.4	Configurar e implementar medidas de seguridad para detectar y alertar sobre cambios no autorizados en la configuración.	Los cambios en la configuración del sistema pueden reducir el nivel de protección del activo. Así pues, por ejemplo, un cambio en la configuración de la longitud de la contraseña o una tarea para instalar <i>software</i> que no está de acuerdo con la directiva de la organización lo expone al riesgo.	Esto puede lograrse definiendo leyes relevantes en el sistema SIEM, comparando informes periódicos (configuración actual en relación con la configuración anterior), mediante herramientas de monitoreo y control o de mando y control que proporcionen una indicación de los cambios en la configuración, etcétera. Se recomienda adoptar las herramientas de monitoreo continuo de controles (CCM, por sus siglas en inglés) para recibir notificaciones en tiempo real.	3
Protección de estaciones de trabajo y servidores	6.5	Definir la configuración del sistema para proporcionar la funcionalidad mínima requerida (y bloquear funciones, puertos y protocolos innecesarios).	La organización definirá procedimientos de endurecimiento para cada tipo de sistema y servidor según las prácticas aceptadas para incluir, como mínimo, lo siguiente: 1. reducir la superficie de ataque del sistema mediante el bloqueo de puertos innecesarios; 2. desactivar servicios innecesarios; 3. eliminar cuentas de usuario invitado; 4. usar preferentemente un protocolo de comunicación seguro entre servidores; 5. recibir actualizaciones por correo electrónico de manera ordenada; 6. bloquear funciones sensibles del sistema; 7. enviar registros de eventos del sistema a un servidor de monitoreo; y 8. bloquear la instalación de <i>software</i> por usuarios no autorizados.	Las organizaciones de nivel 1 pueden llevarlo a cabo mediante una cláusula contractual con el proveedor de <i>software</i> o del servicio de productos resistentes de acuerdo con la práctica común. Las organizaciones de nivel 2 y niveles superiores han de realizar pruebas de efectividad del producto o servicio de acuerdo con el nivel de endurecimiento necesario. Las organizaciones de nivel 3 deben realizar una prueba de la efectividad del endurecimiento. Puede recurrirse a procedimientos de endurecimiento en torno a prácticas aceptadas, como las del NIST, las publicaciones del equipo nacional de respuesta ante emergencias informáticas y del Centro para la Seguridad en Internet (CIS, por sus siglas en inglés), o a servicios de expertos que prepararán procedimientos de endurecimiento de acuerdo con la tecnología conveniente.	1


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Protección de estaciones de trabajo y servidores	6.6	Evitar la ejecución de aplicaciones según lo definido por la organización (lista negra).	La organización definirá una lista de <i>software</i> prohibido (lista negra).	La organización bloqueará determinados programas, tales como herramientas de ataque, <i>spyware</i> , herramientas de almacenamiento en la nube, herramientas para compartir archivos y otros. Es posible configurar una lista de <i>software</i> prohibido usando Active Directory o herramientas de administración de configuración. Algunos de los servidores y herramientas de protección de dispositivos admiten las capacidades anteriores.	2
Protección de estaciones de trabajo y servidores	6.7	Configurar y usar una lista blanca de <i>software</i> permitido para usar y bloquear cualquier otro <i>software</i> .	La organización definirá una lista de <i>software</i> permitido para usar y bloqueará la instalación y el uso de cualquier otro <i>software</i> que utilice el sistema de administración de la configuración de la organización, o mediante el uso de una herramienta de terceros, y bloqueará la instalación de estos programas de <i>software</i> .	Es posible configurar una lista de <i>software</i> permitido con Active Directory o con herramientas de administración de configuración. Algunos de los servidores y herramientas de protección de dispositivos admiten las capacidades anteriores.	3
Protección de estaciones de trabajo y servidores	6.8	Supervisar los servidores y sistemas que hayan sido excluidos (y cuya exclusión fue aprobada) de la implementación de una configuración reforzada.	A veces, por razones operacionales, no se puede aplicar el nivel de protección para todos los activos de la misma manera. En tales casos, se requiere que la organización implemente un proceso que necesitará una tarea especial para excluir a un servidor o sistema particular de los requisitos de seguridad de la información después de una determinada necesidad y, al hacerlo, la organización será responsable de proporcionar controles compensatorios en lugar de exclusión.	Es posible nombrar a un responsable de sector o un funcionario que haga las veces de “autoridad de aprobación” para definir las necesidades de exclusión, quien examinará las necesidades operativas y organizativas de exclusión y recomendará controles compensatorios.	3
7. Evitar el código malicioso El código malicioso lo utilizan agentes hostiles a la organización y está diseñado para penetrar sin la aprobación de esta con el fin de producir daños a través del ciberespacio (robo o manipulación de datos, daño a los sistemas informáticos, etcétera). La expresión “código malicioso” es un término amplio, que incluye muchos tipos de <i>software</i> abusivo: virus, gusanos, troyanos, <i>rootkits</i> , <i>software</i> publicitario (<i>adware</i>) y otros.				La protección del sistema contra el código malicioso es de suma importancia en la ciberdefensa de una organización. La matriz de defensa incluye, por un lado, la prevención de la intrusión de código malicioso (en los puntos de entrada y salida de comunicaciones corporativas, servidores y dispositivos conectados) y, por otro lado, la detección y el proceso de manejo del código malicioso que se ha infiltrado en la organización.	


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Evitar el código malicioso	7.1	<p>Activar herramientas y sistemas en los puntos de comunicación externos a la organización. Estas herramientas escanearán y detectarán códigos maliciosos. También operarán en comunicación con terceros, correo electrónico y servicios de navegación.</p> 	El propósito de este monitoreo es detectar código malicioso antes de que penetre en la organización, aún a nivel de pasarela.	Puede realizarse utilizando servidores proxy, sistemas de cortafuegos de nueva generación (NGFW, por sus siglas en inglés) y herramientas dedicadas a diferentes protocolos de comunicación, como el correo electrónico.	2
	7.2	<p>Definir procedimientos para la gestión de estaciones, servidores o redes infectadas por código malicioso.</p> 	La finalidad de este monitoreo es asegurar que la organización esté preparada para hacer frente a los casos de infiltración de código malicioso.	Ejemplos de procedimientos: detección y eliminación de código malicioso, reinstalación del sistema operativo, identificación de tendencias y generación de conclusiones en el caso de una propagación masiva e infección en la organización.	2
	7.3	<p>Implementar herramientas para detectar y prevenir el código malicioso en los dispositivos conectados y servidores de la organización. Estas herramientas se ejecutarán en un modo de protección activa y también se realizarán exploraciones periódicas.</p> 	Dado que algún software abusivo podría penetrar en los mecanismos de seguridad, hay que asegurarse de que los controles para manejar el código malicioso también se aplicarán a nivel de estación de trabajo.	Es posible utilizar cualquier herramienta de detección y bloqueo de código malicioso (como antivirus) de fabricantes reconocidos.	1
Evitar el código malicioso	7.4	<p>Implementar y administrar estas capacidades como parte de las herramientas de protección de los dispositivos, o integrar herramientas con estas capacidades además de los antivirus existentes.</p>	El propósito de este monitoreo es elevar el nivel de detección y manejo de los dispositivos más allá de las capacidades básicas de un sistema antivirus en funcionamiento.	Los productos de sistemas de prevención de intrusiones basado en el host (HIPS, por sus siglas en inglés) se pueden usar de forma independiente o como capacidades adicionales de protección de software de productos antivirus.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Evitar el código malicioso	7.5	Activar controles avanzados para evitar códigos maliciosos en los sistemas operativos de los servidores y los dispositivos conectados.	La organización activará en el sistema operativo mecanismos que dificulten el acceso de código malicioso a la memoria o las funciones del sistema operativo.	Se puede lograr con soluciones para identificar anomalías en el nivel del sistema operativo.	4
Evitar el código malicioso	7.6	Implementar una herramienta para identificar el código malicioso a nivel de red.	La organización activará herramientas que se implementarán en la red de la organización con el objetivo de identificar y alertar sobre la propagación de código malicioso en línea.	Ejemplos de estas herramientas son <i>honeypots</i> o redes trampa, tecnologías contra bots, componentes del sistema de prevención de intrusiones (IDS, por sus siglas en inglés), etcétera.	3
Evitar el código malicioso	7.7	Administrar la herramienta de prevención de códigos maliciosos en la organización a través de un sistema central. Las principales herramientas de gestión permitirán una notificación importante de incidentes sospechosos y la identificación de eventos del sistema (actualización de problemas, protección inactiva, eliminación de componentes, etcétera).	El objetivo de este monitoreo es administrar efectivamente el sistema de protección frente al código malicioso. Trabajar mediante una configuración instalada localmente hace que sea difícil distribuir actualizaciones, garantizar una cobertura completa y controlar la situación general de defensa.	La mayoría de los sistemas de prevención de códigos maliciosos permiten el uso de herramientas de gestión con una interfaz de administración centralizada.	2
Evitar el código malicioso	7.8	Activar medidas de detección y prevención, basadas en la detección de comportamientos que se desvíen del comportamiento razonable y aceptable, además del uso de herramientas basadas en firmas electrónicas.	El propósito de este monitoreo es detectar actividades que se desvíen de la norma. El cifrado de múltiples archivos, documentos que intentan acceder a los archivos de registro, etc., son ejemplos de hechos que se supone que deben provocar una alerta roja en la organización.	Es posible utilizar herramientas que analicen la heurística, el comportamiento de un usuario o de un sistema.	3
Evitar el código malicioso	7.9	Ejecutar una actualización automática de todos los sistemas para identificar y evitar el código malicioso dentro de la organización.	La organización activará las actualizaciones automáticas desde un servidor central, administrado por la organización o por un proveedor de servicios reconocido. Estas actualizaciones mantendrán las herramientas de protección actualizadas constantemente.	Pueden usarse servidores de actualización, integrados en los servidores de administración de la organización como parte de estos sistemas o, alternativamente, utilizar los servidores del fabricante si no hay un servidor central de actualizaciones en la red de la organización (también se aplica a los servicios en la nube).	1



Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
8. Cifrado El uso inteligente del cifrado es de gran ayuda para proteger la información y evitar su exposición, incluso cuando esta se ha filtrado, ya que reduce buena parte de las consecuencias para la organización frente a la filtración de información. Por lo tanto, es importante definir las aplicaciones que requieren cifrado y el tipo de cifrado necesario, de acuerdo con las leyes, directrices, procedimientos, normativas, compromisos organizacionales y la viabilidad económica en el marco de la gestión de riesgos.					
Cifrado	8.1	Definir los usos que precisan cifrado y el tipo de cifrado requerido, de acuerdo con las leyes, directrices, procedimientos, regulaciones y compromisos de la organización.	La organización definirá qué información y sistemas deben cifrarse y registrará la configuración del cifrado de la información. Los requisitos se derivarán de las normas aplicables a la organización o de las necesidades de retención de información.	Es imprescindible configurar el cifrado en diferentes medios de los que se puede filtrar información (memorias, <i>middleware</i> de comunicación, etc.) y definir mecanismos para administrar y monitorear el cifrado (como la administración de claves criptográficas y certificados digitales en varias etapas). De particular importancia es el cifrado de medios en los dispositivos móviles (computadoras portátiles, teléfonos móviles, tabletas, etcétera).	1
Cifrado	8.2	Administrar y proteger las claves de cifrado durante la producción, distribución, almacenamiento, acceso y destrucción.	La organización definirá procedimientos y procesos para la emisión de claves de cifrado, protegiendo las claves de cifrado privadas y los servidores para emitir claves y certificados, endureciendo los procedimientos y definiendo procedimientos para la regeneración de claves.	Endurecimiento y preservación de los servidores de la autoridad certificadora raíz, protección mediante un módulo de seguridad <i>hardware</i> (HSM, por sus siglas en inglés), distribución de claves criptográficas a sistemas y empleados, operación de la matriz de infraestructura de clave pública (PKI, por sus siglas en inglés).	1
Cifrado	8.3	Garantizar la disponibilidad de información incluso en caso de pérdida de las claves de cifrado.	La organización establecerá un sistema de recuperación de datos cifrados mediante la implementación de procesos administrados y herramientas apropiadas.	Por ejemplo, una matriz de recuperación de cifrado de disco de computadoras portátiles usando las herramientas de cifrado de disco del fabricante y procesos de recuperación administrados.	3
Cifrado	8.4	Implementar el cifrado de la información confidencial transmitida entre los sistemas de la organización y las interfaces de usuario final en el <i>middleware</i> de comunicación pública.	La organización implementará matrices de cifrado de datos para la información confidencial que se muestra al usuario a través de un navegador, una aplicación móvil u otros sistemas que brindan acceso a la información mediante redes públicas como Internet.	Uso de certificados de capa de conexión segura (SSL, por sus siglas en inglés) aprobados y actualizados en el navegador.	Por determinar
Cifrado	8.5	Implementar el cifrado de información confidencial transmitida entre sistemas dentro de la organización.	La organización implementará el tráfico cifrado en las interfaces entre servidores y servicios que transmitan información confidencial y dará prioridad a protocolos que codifiquen el tráfico.	Eso puede lograrse utilizando protocolos como SSL, SSH, el protocolo seguro de transferencia de hipertexto (HTTPS, por sus siglas en inglés) y otros.	Por determinar

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Cifrado	8.6	<p>Establecer el cifrado de la información confidencial transmitida entre la organización y las interfaces externas, proveedores y sistemas externos.</p> 	La organización implementará una comunicación cifrada con proveedores y sistemas que se encuentren fuera de la organización.	Se puede realizar utilizando protocolos como SSL, SSH, HTTPS, el protocolo seguro de transferencia de archivos (SFTP, por sus siglas en inglés), etcétera.	2
Cifrado	8.7	Implementar mecanismos de cifrado en los dispositivos portátiles (computadoras portátiles, teléfonos móviles, tabletas, etcétera).	La organización implementará el cifrado del disco duro de dispositivos móviles y dispositivos multimedia portátiles.	Los dispositivos móviles y las tabletas pueden usar el sistema de cifrado de discos del fabricante. Otros sistemas operativos pueden usar las herramientas de los proveedores que permiten el cifrado del disco.	2
Cifrado	8.8	Utilizar mecanismos de cifrado basados en algoritmos de cifrado reconocidos y tamaños de clave correspondientes con el perfil de la amenaza.	La organización no utilizará mecanismos de cifrado con deficiencias y vulnerabilidades conocidas, y hará coincidir la intensidad del cifrado, incluidos los tamaños de las claves de cifrado, con el perfil de la amenaza.	Por ejemplo, no se deben utilizar métodos de cifrado obsoletos, como SHA1, SSLv1, SSLv2 o claves de cifrado de menos de 128 bits, etcétera.	2
Cifrado	8.9	Administrar una matriz de certificados digitales para la emisión y revocación de certificados digitales y usar certificados digitales solo de fuentes confiables.	La organización administrará una matriz para la emisión de certificados digitales y una matriz para la revocación de certificados (CRL, por sus siglas en inglés). Además, también utilizará certificados externos emitidos únicamente por fuentes confiables (autoridad de certificación de confianza).	Se puede realizar mediante una matriz de servidores CRL ordenada y actualizada, y usando certificados externos de servicios aprobados (autoridad de certificación de confianza).	2
Cifrado	8.10	Definir un proceso para la renovación de certificados digitales antes de su vencimiento.	La organización se asegurará de que los certificados digitales en uso se renueven antes de su vencimiento. Si se reemplazan los certificados, los más antiguos se distribuyen a los servidores de revocación de certificados (CRL).		2



Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
9. Seguridad de la red La infraestructura de comunicaciones de la organización es un factor clave que conecta todos los recursos informáticos a su disposición, tanto entre ellos como con Internet y otras organizaciones. La infraestructura de las comunicaciones es fundamental para las actividades cotidianas en muchas organizaciones, y su cierre o daño tiene considerables repercusiones para la organización. Por lo tanto, en la red de la organización se originan muchos tipos de ataques contra ella y, en consecuencia, es imprescindible protegerla contra amenazas internas y externas.					
Seguridad de la red	9.1	Definir e implementar una directiva de protección de las redes de comunicación, y revisarla y actualizarla periódicamente. 	La organización debe definir e implementar una política de seguridad de la red, que debe incluir una referencia a temas como los canales de acceso a la red pública de Internet y la configuración de su protección. Además, debe abordar los aspectos centrales de las comunicaciones internas y de la comunicación externa.	Redactar un documento de política o integrarlo como un capítulo en la política de seguridad de la información de la organización.	2
	9.2	Separar la funcionalidad de los usuarios de los servicios de administración de la red.	Las interfaces de administración se deben separar de otras interfaces de usuario para reducir su exposición a un posible acceso no autorizado a las interfaces de administración.	Ello puede hacerse mediante una página de inicio de sesión diferente para usuarios y administradores; una red de comunicación separada utilizada para conectarse a las interfaces de gestión de equipos; la restricción de la dirección IP autorizada para acceder a la interfaz de administración, etcétera.	3
	9.3	Operar dispositivos tecnológicos para proteger los servicios contra ataques DoS.	Defenderse de los ataques DoS de varios tipos, como sobrecargar los recursos informáticos para que colapsen, sobrecargar el ancho de banda de la comunicación, sobrecargar el sitio web para bloquearlo y otros.	El control se puede implementar usando diversas herramientas, como sistemas de cortafuegos (usando un módulo de prevención de intrusiones), sistemas de detección de intrusiones (IPS, por sus siglas en inglés), cortafuegos de aplicaciones web (WAF, por sus siglas en inglés), así como restricciones en el volumen de tráfico hacia ciertos sistemas, o limitando el número de consultas realizadas en el sistema.	1
	9.4	Desconectar la conexión de red vinculada a la sesión al concluir, o después de un tiempo determinado de inactividad.	La organización aplicará límites a la duración de la conexión y supervisará e interrumpirá la comunicación cuando no se realicen tareas de transmisión.	El control se puede implementar usando un cortafuegos y configurándolo para que las conexiones de red reciban un tiempo de expiración tras un período de inactividad determinado.	2


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad de la red	9.5	Establecer pautas para el uso de la tecnología de telefonía IP (VoIP, por sus siglas en inglés) y monitorear su uso.	La organización definirá cuándo y cómo se permite o prohíbe el uso de los servicios de VoIP (integrados en los sistemas de la organización o como un servicio externo) y aplicará medidas de seguridad de la información para implantar esa configuración.	Se puede aplicar separando la red VoIP de la red estándar, limitando el equipo de conectividad que no sea de telefonía a la red utilizando medidas como el control de acceso a la red (NAC, por sus siglas en inglés), la identificación del equipo opuesto a los servidores VoIP o el uso de cifrado e identificación mediante SSL.	2
Seguridad de la red	9.6	Asegurarse de que el servicio de traducción de direcciones de red (DNS, por sus siglas en inglés) sea proporcionado por un servidor confiable (dentro y fuera de la empresa).	La organización permitirá obtener el servicio de traducción de direcciones solo de un servidor interno seguro para evitar el enrutamiento erróneo de comunicaciones (intencionalmente o no) a objetivos hostiles.	Se configurarán servidores DNS internos que proporcionarán una respuesta a los servidores de la organización. También es posible configurar servidores DNS dedicados para áreas más seguras de la red. Los servidores de la empresa se configurarán de modo que cualquier solicitud a un servicio DNS se realice únicamente a través de esos servidores.	1
Seguridad de la red	9.7	Asegurarse de que las respuestas recibidas del servidor de traducción de direcciones sean confiables y no hayan sido alteradas durante la tarea de transmisión.	La organización se asegurará de que las respuestas devueltas desde el servidor de traducción de direcciones no puedan modificarse mediante mecanismos tales como las respuestas de aseguramiento enviadas por un certificado digital.	Se puede aplicar usando extensiones de seguridad para el sistema de nombres de dominio (DNSSEC, por sus siglas en inglés) del servicio DNS.	2
Seguridad de la red	9.8	Proteger la credibilidad de las comunicaciones a nivel de sesión, de modo que ambos extremos de la sesión estén seguros de la exactitud de la identidad de la otra parte (protección frente a ataques MITM, secuestro de sesión, etcétera).	La organización activará el monitoreo de la fiabilidad mediante opciones tecnológicas como los certificados digitales mientras establece la comunicación entre varios servicios del sistema.	Se pueden usar certificados SSL para identificar el servicio y un servidor de la autoridad de certificación interno seguro que emita certificados para los diversos servicios de la organización. El servicio es compatible con una infraestructura de Active Directory y el servicio Kerberos de Microsoft. El monitoreo de la administración de la sesión se puede realizar utilizando el monitoreo de la sesión en el nivel del servidor (como IIS o Apache) o en el nivel de la red con un equilibrador de carga (<i>load balancer</i>).	2
Seguridad de la red	9.9	Monitorear el tráfico de red saliente y entrante de la organización.	El propósito de este monitoreo es asegurar que solo se permita el tráfico dentro y fuera de la organización que respete la directiva definida (acceso a través de protocolos autorizados, servicio aprobado, desde destinos y hacia destinos aprobados, etcétera).	Se puede realizar mediante la aplicación de cortafuegos que distinga entre la red de la empresa y las redes externas.	2




Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad de la red	9.10	Monitorear y controlar los principales enlaces de comunicación dentro de la red de la organización.	La organización dividirá su red en subredes, según el nivel de riesgo y la clasificación de los datos de los sistemas.	Las redes se pueden separar mediante un cortafuegos corporativo entre entornos, configurando entornos tales como una zona de amortiguación (DMZ, por sus siglas en inglés) para servicios salientes a Internet, redes de administración que se conectarán tras una conexión segura, redes que contienen servicios sensibles y sistemas sensibles.	3
Seguridad de la red	9.11	Limitar el número de canales de comunicación fuera del sistema.	La organización reducirá y agrupará los canales de comunicación para garantizar un mejor control sobre las conexiones al sistema.	Se usa un servidor terminal para conectarse al sistema.	2
Seguridad de la red	9.12	Bloquear de manera predeterminada todo el tráfico de red y permitir de manera manual cualquier tráfico deseable mediante reglas de excepción.	La organización definirá las reglas de filtrado del tráfico de red para bloquear de manera predeterminada todo el tráfico que no esté explícitamente definido como permitido.	Configurar una “regla cero” en el cortafuegos para bloquear todo el tráfico no explícitamente habilitado. Hay que asegurarse de que las rutas estén configuradas para que todo el tráfico se enrute a través del cortafuegos.	1
					
Seguridad de la red	9.13	Evitar que los dispositivos creen una comunicación local sobre el sistema en paralelo a la comunicación a través de una conexión externa.	El propósito de este monitoreo es prevenir una situación en la que la computadora actúe como un puente que conecta el mundo externo con la red interna de la organización.	Es posible configurar la estación de trabajo mediante una directiva que determina que solo una tarjeta de red esté activa en cualquier momento en el servidor –las conexiones se configurarán solo al concentrador de la organización, detrás de un cortafuegos– y eliminar otras tarjetas de red que no estén conectadas a una red requerida por definición (por ejemplo, la red de almacenamiento), como las tarjetas de red cableadas e inalámbricas.	2
Seguridad de la red	9.14	Enrutar la comunicación dentro de la organización a redes externas a través de servidores proxy autenticados y administrados.	La organización determinará que todas las comunicaciones a redes externas se realizarán solo a través de servidores proxy. Esto se hará con el fin de crear un medio que evite la comunicación directa que exponga los recursos de la organización a Internet y para facilitar la implementación de controles concentrados y protecciones de los canales de comunicación frente a Internet.	Se puede aplicar a través de un servidor proxy conectado al mundo, en el que la navegación se realiza solo a través de él. El servidor proxy se configurará con la opción de restringir las conexiones a sitios y categorías no autorizados. Además, los servidores se configurarán de modo que el acceso a Internet esté habilitado solo para actualizaciones a través del servidor proxy (si no resulta posible usar un servidor de actualizaciones específico del fabricante del sistema).	3
Seguridad de la red	9.15	Implementar mecanismos para evitar conexiones físicas no autorizadas a la red corporativa.	La conexión de equipos no autorizados a la red de la empresa expone sus recursos a potenciales daños a la confidencialidad e integridad de la información y a los recursos informáticos y su disponibilidad.	Se puede implementar mediante el uso de sistemas NAC.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad de la red	9.16	Aplicar mecanismos que filtren la comunicación que no coincida con la estructura del protocolo o la información esperados.	Estos mecanismos deben implementarse para defenderse contra el uso malicioso de protocolos inseguros o no autorizados. Además, hay que asegurarse de que los paquetes de comunicaciones lleguen en la configuración correcta y no hayan sido alterados antes de llegar al destino.	Por ejemplo, el filtrado de tráfico que no cumpla con los estándares de cortafuegos, una aplicación de cortafuegos para XML.	3
Seguridad de la red	9.17	Asegurarse de que, en caso de falla operativa de uno de los dispositivos de protección del perímetro (cortafuegos, etc.), el nivel de seguridad del sistema no se vea comprometido.	El equipo de seguridad de la información debe configurarse para bloquear la comunicación en caso de falla.	La mayoría de los equipos de seguridad de la información se pueden configurar para dar redundancia hacia el equipo secundario (cortafuegos secundario para la redundancia, otra ruta de comunicación segura, etc.); si no hay redundancia, la falla moverá el sistema a un estado de error y cierre.	2
Seguridad de la red	9.18	Usar los dispositivos de protección del perímetro para separar los componentes del sistema que admiten tareas o servicios de la organización que esta determine que requieren una separación.	La organización determinará que la separación de redes en áreas seguras se llevará a cabo a través de equipos de seguridad de la información dedicados.	Es posible utilizar herramientas como un cortafuegos, una herramienta VPN que permita conectarse de forma segura a redes de administración, control de acceso a nivel de enrutador, servidores proxy.	2
Seguridad de la red	9.19	Utilizar direcciones de red separadas (diferentes subredes) para conectarse a distintas zonas de seguridad.	La organización determinará que cada subred tendrá un rango de direcciones separado, que se informará al cortafuegos y los enrutadores.	Se puede realizar a través de la administración centralizada de direcciones en la interfaz de administración del cortafuegos central, o mediante el registro manual (administrado y controlado) de las diferentes direcciones de red.	1
Seguridad de la red	9.20	Implementar mecanismos para mantener la integridad y confidencialidad del tráfico de red en un medio público.		Por ejemplo, cifrar el tráfico saliente fuera de la organización, cifrar las líneas de comunicación en un medio público.	2


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad de la red	9.21	Definir, documentar e implementar una directiva de endurecimiento para el equipo de comunicaciones que cumpla con los requisitos de seguridad de la información de la organización.	La organización definirá los requisitos de endurecimiento para los sistemas de comunicación dentro de la organización con énfasis en los requisitos básicos, la frecuencia de las actualizaciones y el nivel de clasificación y luego documentará los requisitos en un marco general que servirá como base para los procedimientos de endurecimiento.	Documentos de referencia y referencias a los requisitos de endurecimiento en los documentos de política. Además, se ha de definir quién es responsable de la implementación del endurecimiento real y cómo se lleva a cabo la prueba continua de los controles. La documentación sobre el endurecimiento incluirá, entre otras cosas, una referencia al uso de servicios no autorizados y servicios seguros, los puertos aprobados, la eliminación de cuentas inactivas, etcétera. Es importante asegurarse de que el endurecimiento se lleve a cabo siguiendo las recomendaciones del fabricante. Se pueden encontrar recomendaciones de endurecimiento en las normas aceptadas en el sector, como DISA, SANS y el sitio web oficial del fabricante.	3
Seguridad de la red	9.22	Implementar mecanismos para la gestión centralizada, implementación y validación de los equipos de comunicaciones.		Se puede aplicar por tipo de equipo de telecomunicaciones y de acuerdo con el mecanismo de gestión central de cualquier fabricante. Además, es posible realizar el endurecimiento de los diferentes componentes de medios manualmente, utilizando la interfaz de administración de cada componente por separado.	3
Seguridad de la red	9.23	Definir un mecanismo (central o local) para administrar la directiva del cortafuegos.	La organización definirá la directiva de administración de los sistemas de cortafuegos, que incluirá referencias al proceso de agregar y eliminar reglas de enrutamiento ilegales en el sistema, incluido un proceso de aprobación para agregar y eliminar reglas. También es necesario establecer la manera de documentar y detallar cualquier regla que se haya abierto en el cortafuegos para su manejo adecuado.	Se puede implementar directamente en la interfaz de administración del sistema. Es posible aplicar un proceso de aprobación para la apertura y eliminación de reglas, así como la creación y eliminación real de reglas en el sistema mediante el uso de sistemas automatizados de gestión de cambios.	2
Seguridad de la red	9.24	Mejorar las reglas del cortafuegos. 	La organización llevará a cabo un proceso de revisión de las reglas del sistema de cortafuegos con vistas a su mejora, mantener su integridad y confirmar que no hay reglas que puedan exponer a la organización a riesgos innecesarios.	Se puede aplicar mecánicamente utilizando sistemas automatizados para gestionar los cambios o, alternativamente, realizar un proceso manual de revisión de reglas y definiciones.	3
Seguridad de la red	9.25	Escanear periódicamente la red. 		Se puede realizar utilizando herramientas de escaneo gratuitas, como NMAP, Superscan, entre otras.	2


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
10. Separación de entornos Una red empresarial puede incluir varios entornos, como un entorno de producción, uno de desarrollo, uno de prueba, uno de administración, etc. Estos entornos a menudo están vinculados entre sí, pero difieren en el tipo de información que hay en ellos, el nivel de disponibilidad requerido, en su gestión y en el nivel de defensas y controles de seguridad de la información integrados en ellos.					
Separación de entornos	10.1	Definir e implementar una directiva de separación de entornos, revisarla y actualizarla periódicamente.	La organización definirá e implementará una directiva de separación de entornos, como producción, desarrollo, prueba, soporte, Internet, entornos de red de invitados, etc. El propósito de la separación es evitar la capacidad de moverse entre entornos mediante el uso de acceso por tareas o de infraestructura compartida.	La directiva debe contener una definición de los tipos de separación entre entornos, el nivel de separación requerido (por ejemplo, separación lógica o física) y la derivación a los procedimientos apropiados.	2
Separación de entornos	10.2	Configurar entornos separados para desarrollo, pruebas y producción. 	El equipo de seguridad de la información debe configurarse para bloquear la comunicación en caso de falla.	Definición de diferentes entornos, sistemas de mapeo y demarcación tecnológica (redes, servidores y bases de datos) de cada entorno.	2
Separación de entornos	10.3	Restringir el uso de datos confidenciales de producción (datos del cliente o datos definidos por la organización como confidenciales) en entornos que no sean de producción si no están protegidos al mismo nivel que en un entorno de producción.	Dado que los desarrolladores y el personal de control de calidad acceden a los entornos inferiores de manera menos controlada, existe la preocupación de que se puedan filtrar datos confidenciales. Además, el nivel de seguridad en estos entornos generalmente es menor que en el entorno de producción. Para reducir la exposición debido al acceso de los desarrolladores y otros a los entornos de prueba e integración, es necesario evitar la transferencia de datos confidenciales a estos entornos.	Es posible utilizar procesos de anonimización (identificadores de codificación de datos o tareas) o datos de prueba sintéticos para entornos de desarrollo y prueba.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Separación de entornos	10.4	Separar los privilegios de usuario para diversos entornos y definir privilegios para cada entorno por separado. 	Es necesario administrar usuarios y privilegios en un solo sistema de administración de usuarios, pero también se precisa establecer un registro de privilegios diferente para cada entorno por separado, de modo que los entornos que contengan información confidencial no estén expuestos a un acceso no autorizado en caso de que se piratee una cuenta de usuario o se den privilegios abusivos.	Configurar una cuenta de usuario separada para el empleado para cualquier entorno en el que deba operar. Los privilegios de acceso también se definirán por separado para cada cuenta, dependiendo de las necesidades de operación del empleado.	2
	10.5	Configurar un proceso de aprobación para la transferencia de datos desde el entorno de producción a otros entornos y un proceso para la transferencia segura de datos.	A veces se requiere la transferencia de datos confidenciales del entorno de producción a otros entornos como parte de los procesos de desarrollo y prueba. Para evitar el abuso de estos procesos, es necesario implementar un proceso controlado de transferencia de datos que requiera las aprobaciones apropiadas antes de la ejecución.	Se puede aplicar mediante un proceso automatizado, incluida la aprobación por los responsables de seguridad de la información.	2
Separación de entornos	10.6	Configurar un proceso controlado de transferencia de componentes de <i>software</i> desde los entornos de desarrollo y prueba al entorno de producción.	Implementar el proceso de transferencia de componentes de <i>software</i> al entorno de producción, diseñado para garantizar la finalización de los procedimientos de prueba y obtener las aprobaciones necesarias antes de ejecutar la transferencia.	Se puede aplicar en el marco del Comité de preparación para la producción, que concentra los cambios en el entorno de producción y su aprobación antes de ejecutar la transferencia.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Separación de entornos	10.7	Establecer entornos separados que implementen diferentes niveles de seguridad de manera que tenga en cuenta el nivel de amenaza que se plantea para el entorno “más seguro” respecto del “menos seguro”.	Los entornos de producción tienden a manejarse cuidadosamente y tienen amplios controles y salvaguardas, mientras que los entornos de desarrollo y prueba tienden a tener una gestión más flexible y contienen menos controles y salvaguardas. Para evitar daños al entorno de producción debido a la utilización de puntos débiles en entornos bajos, se deben establecer los distintos sistemas y niveles de seguridad del entorno y entornos separados que implementen diferentes niveles de seguridad.		2
Separación de entornos	10.8	Aplicar la separación entre entornos en la red de telecomunicaciones, sistemas de almacenamiento, virtualización, procesos de identificación y gestión de claves de cifrado.	Una separación completa entre entornos requiere la aplicación de redes físicas e infraestructuras separadas. El uso de infraestructuras compartidas requiere la implementación de mecanismos de separación de los proveedores, adaptados al nivel de amenaza y la naturaleza de los riesgos planteados al entorno tecnológico.		3
Separación de entornos	10.9	Implementar mecanismos de filtrado bidireccional en las comunicaciones y las interfaces de transferencia de datos entre entornos para evitar el paso de código malicioso, el ataque a puntos débiles, la explotación de interfaces de aplicación y la liberación no controlada de información.	Una separación completa entre entornos requiere la aplicación de redes físicas e infraestructuras separadas. El uso de infraestructuras compartidas requiere la implementación de mecanismos de separación de los proveedores, adaptados al nivel de amenaza y la naturaleza de los riesgos planteados al entorno tecnológico.	Se puede realizar mediante tecnologías avanzadas de filtrado que permiten el filtrado de contenido y mediante reglas de filtrado avanzadas.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
11. Computación en la nube pública <p>Muchas organizaciones confían cada vez más en los servicios en la nube para procesar y almacenar información. Junto con las ventajas del cambio, se requiere que la organización administre el riesgo resultante de que una información valiosa para la organización se transfiera a un tercero (el proveedor de servicios en la nube). Por lo tanto, es deber de la organización asegurarse de que los servicios en la nube no afecten al nivel de su ciberdefensa, estableciendo los requisitos adecuados para el proveedor de servicios en la nube. La organización debe comprender la división de responsabilidades de los servicios de seguridad entre el proveedor de servicios y la organización, e implementar el monitoreo de la protección en consecuencia, tanto a nivel de la empresa como del proveedor.</p>					
Computación en la nube pública	11.1	Comprender la división de responsabilidades entre el proveedor de servicios y la organización, e implementar un monitoreo de protección en consecuencia.	Cuando se utilizan servicios en la nube pública, existe una división de responsabilidad de la protección cibernética entre las cuestiones que están bajo la responsabilidad del proveedor y las que quedan bajo la responsabilidad del cliente. Esta división de responsabilidades depende de la naturaleza del servicio y del modelo de implementación. La organización tiene que entender cuáles son las cuestiones que están bajo su responsabilidad y aplicar las consecuencias de esta responsabilidad.	En el caso de servicios como la plataforma como servicio (PaaS, por sus siglas en inglés) o la infraestructura como servicio (IaaS, por sus siglas en inglés), la responsabilidad del cliente es administrar a los usuarios, monitorear el uso por parte de ellos, administrar los datos y garantizar su seguridad, mantener aplicaciones e interfaces seguras y, a menudo también, sistemas operativos e infraestructuras seguros, todo dependiendo de la naturaleza del servicio, según se defina en el acuerdo con el proveedor. Estos controles pueden implementarse usando herramientas de monitoreo y control proporcionadas como parte del servicio, usando las herramientas disponibles en la organización o a través de proveedores externos que proporcionan servicios de seguridad en la nube.	1
Computación en la nube pública	11.2	Definir e implementar una directiva para el uso y la protección de los servicios en la nube pública, revisarla y actualizarla periódicamente.	La Dirección de la organización debe definir una directiva y pautas con respecto a las condiciones y reglas para el uso de servicios en la nube pública y la manera en que la organización implementa la ciberdefensa en caso de que utilice servicios en la nube pública.	Una directiva sobre el uso de servicios en la nube suele enfrentarse a las siguientes cuestiones: cuáles son los servicios que pueden usarse en la organización, cuáles los requisitos específicos de la organización, cuestiones en torno a la contratación con proveedores, la gestión de riesgos de privacidad, la supervisión y el control.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Computación en la nube pública	11.3	Asegurarse de que el proveedor de servicios en la nube se compromete a cumplir con los estándares y regulaciones requeridos, en función de las obligaciones y estándares de la organización acordados con el proveedor.	Varias organizaciones están sujetas a pautas regulatorias relacionadas con el uso de servicios en la nube, como la protección de la privacidad, las normativas sectoriales o la responsabilidad contractual frente a terceros. Tales obligaciones suelen dictar reglas estrictas para el uso de servicios en la nube.	Por ejemplo, la implementación de las directivas del Banco de Israel, la supervisión del mercado de capitales, las directrices de ILITA, las directivas de la autoridad gubernamental para las tecnologías de la información y las comunicaciones (TIC) y otras. Al hacer esta comparación, es necesario examinar todas las aplicaciones activas en la nube en la organización. Este mapeo se puede hacer, entre otras formas, examinando el historial de navegación de los usuarios y comparándolo con la lista de proveedores de <i>software</i> y examinando las reglas existentes en los componentes de comunicación relevantes (como cortafuegos, filtrado, etcétera). En muchos casos el <i>software</i> para la gestión de la nómina, el intercambio de documentos, la creación de formularios y encuestas y otros tareas se encuentra en la nube, y la organización no lo sabe (<i>Shadow IT</i>).	2
	11.4	Definir e implementar procesos para la supervisión periódica y el control del cumplimiento del proveedor con sus obligaciones. 	Se debe aplicar la protección cibernética en servicios en la nube basada en el cumplimiento estricto de sus obligaciones por parte del proveedor de servicios. Es necesario tomar medidas de supervisión para garantizar que el proveedor cumpla sus obligaciones, ya sea por supervisión directa o por un tercero independiente que revise periódicamente el cumplimiento de las obligaciones del proveedor.	Por ejemplo, enviando cuestionarios al proveedor, auditándolo, utilizando servicios de revisión externos y objetivos, indicando que el proveedor cumple con sus obligaciones. El proveedor de servicios y <i>software</i> enviará al cliente un registro detallado de su cumplimiento con los requisitos definidos en el acuerdo y su implementación. Las desviaciones del acuerdo por parte de un proveedor deben ser aprobadas por el director de ciberdefensa de la organización. Por ejemplo, en caso de un requisito fundamental por parte de la organización para el cumplimiento de directivas específicas del acuerdo de nivel de servicio, o una directiva sobre contraseñas que el proveedor no puede cumplir, se requiere un procedimiento formal, en el que el proveedor explica por qué no puede cumplir ese requisito y si espera subsanar esa deficiencia. Estos datos se transferirán al director de ciberdefensa de la organización para su aprobación y para definir controles compensatorios para reducir el riesgo.	2
	11.5	Realizar verificaciones independientes de seguridad de la información de las interfaces a los servicios en la nube que están expuestos a Internet.	La prueba de los servicios en la nube por parte de la organización, por un tercero contratado para este propósito o por algún otro objetivo, permite identificar las exposiciones de seguridad de la información y manejarlas sin tener que depender exclusivamente del proveedor.	Las pruebas relevantes pueden incluir pruebas de penetración de interfaces de usuario, interfaces de gestión e interfaces de aplicación, auditorías de acuerdo con estándares generalmente aceptados o auditorías que cubran temas específicos definidos con el proveedor en el contrato.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Computación en la nube pública	11.6	Asegurarse de que no se transfiera a los servicios en la nube ningún dato que según la normativa y las responsabilidades de la organización no deba transferirse. 	Hay datos que la organización no puede transferir para su almacenamiento o procesamiento en servicios en la nube pública debido a restricciones de la normativa o a compromisos con terceros. Antes de transferir datos a la nube, asegurarse de que dichos datos no se guarden en la nube o se transfieran a servicios en la nube.	Por ejemplo, hacer un examen de los campos de datos que la organización planea transferir a los servicios en la nube antes de tomar una decisión al respecto. También se puede realizar mediante la eliminación o sustitución de dichos datos en los registros transferidos a los servicios en la nube. Habrá que consultar a una entidad jurídica calificada cuando se realiza un examen y evaluación de la sensibilidad de los datos y la posibilidad de transferirlos para su almacenamiento en la nube.	1
	11.7	Incluir en el plan de continuidad del negocio de la organización las situaciones de revocación de la capacidad de acceder a los servicios en la nube.	Los servicios en la nube son externos a la organización, y la conexión a ellos suele ser a través de una infraestructura pública, como Internet. Es necesario considerar, como parte del plan de continuidad del negocio, situaciones en las que no hay acceso a la nube, ya sea debido a un mal funcionamiento del proveedor o a una falla en la infraestructura de acceso al proveedor.	Por ejemplo, hay que prever métodos alternativos para proporcionar servicios a los clientes en caso de desconexión de los servicios en la nube, contar con archivos de datos actualizados en la organización que contengan la información presente en los servicios en la nube.	2
	11.8	Configurar e implementar mecanismos para el control de acceso, que sean adecuados para las interfaces de acceso a los servicios en la nube, en función de las amenazas y exposiciones relevantes para cada interfaz.	Los servicios en la nube suelen tener varios tipos de interfaces: interfaces de usuario, de gestión y mantenimiento, y de aplicación. En general, estas interfaces están expuestas a Internet y a las redes públicas y, por lo tanto, es imprescindible establecer sólidos mecanismos de control de acceso, adecuados a la naturaleza de las amenazas relevantes para la interfaz, al nivel de exposición tecnológica y al perfil de las amenazas.	Por ejemplo, una interfaz de administración de autenticación fuerte que limite el acceso a interfaces sensibles a ciertas direcciones de Internet.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Computación en la nube pública	11.9	Asegurarse de que el proveedor de servicios en la nube implemente procesos de desarrollo seguros e integre pruebas de seguridad de la información en las etapas de desarrollo y mantenimiento.	Las principales áreas de exposición del <i>software</i> como servicio (SaaS, por sus siglas en inglés) en la nube son las interfaces de usuario y aplicación. Para reducir esa exposición, el proveedor de servicios en la nube debe implementar procesos de desarrollo seguros e integrar controles de seguridad apropiados durante las etapas de desarrollo y mantenimiento. La organización debe asegurarse de que el proveedor implemente adecuadamente estos procesos.	Por ejemplo, exigir la declaración del proveedor de que está implementando procesos de desarrollo seguros o la presentación de los resultados de las pruebas periódicas de seguridad de la información realizadas en los sistemas del proveedor.	3
Computación en la nube pública	11.10	Asegurarse de que el proveedor de servicios en la nube implemente mecanismos para el monitoreo de la seguridad de la información e informes a la organización sobre eventos excepcionales.	Hay áreas en el campo de la ciberdefensa que son responsabilidad del proveedor de servicios en la nube. La organización debe asegurarse de que el proveedor realice un monitoreo de estas áreas e informe a la organización (el cliente del servicio) sobre presuntos incidentes cibernéticos, para que la organización pueda tomar medidas de protección por su lado: contención y recuperación.	Se puede aplicar incluyendo ese problema en el contrato con el proveedor y en el informe periódico por parte del proveedor sobre el número de incidentes que han ocurrido y su análisis.	2
Computación en la nube pública	11.11	Implementar un mecanismo de monitoreo de incidentes de seguridad para detectar incidentes cibernéticos en los servicios en la nube.	A fin de obtener una imagen completa de los incidentes cibernéticos y los eventos sospechosos, la organización debe monitorear las actividades del servicio en la nube. Este monitoreo puede llevarse a cabo utilizando los sistemas del proveedor de servicios en la nube o conectando los sistemas de monitoreo de la organización a los registros producidos por los sistemas del proveedor de servicios en la nube.	Puede realizarse recibiendo un informe (<i>feed</i>) de los incidentes del sistema del proveedor a los sistemas de monitoreo de la organización, o accediendo a las interfaces de monitoreo del proveedor.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Computación en la nube pública	11.12	Definir e implementar un mecanismo que permita la continuidad funcional completa y la eliminación de los datos almacenados por el proveedor de servicios en la nube en caso de la finalización del acuerdo de servicio con el proveedor.	Al finalizar el contrato con el proveedor de servicios en la nube, la organización debe permitir la continuidad funcional y la retención de los registros que le pertenecen que se hayan conservado o procesado mediante los servicios en la nube. Además, debe asegurarse de eliminar los datos que han permanecido con el proveedor y que son propiedad de la organización o están bajo su responsabilidad.	Eso puede hacerse incluyendo esa cuestión en el contrato con el proveedor.	2
12. Controles industriales Los sistemas de control industrial (ICS, por sus siglas en inglés) son responsables de controlar líneas de ensamblaje, sistemas de atención médica, sistemas eléctricos, sistemas de gestión de inmuebles (ascensores, escaleras mecánicas, etc.), infraestructura del agua, etc. Debido a la simplicidad de estos componentes, lo habitual en el pasado era no incluirlos entre los sistemas que la organización debía proteger frente a las amenazas cibernéticas. Sin embargo, estos componentes son un objetivo favorito de los atacantes, pues su daño podría ocasionar graves daños a la organización y a sus clientes.				En consecuencia, la organización ha de atribuir gran importancia a la protección de estos componentes y tener especial cuidado en separarlos y aislarlos de las redes de comunicación tanto como sea posible. Para este propósito, se debe establecer una política corporativa en materia de controles, a fin de proteger sus comunicaciones, administrar el acceso físico, el personal autorizado y las potenciales operaciones a realizar (actualizaciones de software, conectar medios extraíbles, etc.) e implementar mecanismos que controlen la interferencia en sus actividades en caso de ciberataque. Estos controles también son adecuados para sistemas integrados (entorno OT) en general.	
Controles industriales	12.1	Definir, gestionar y supervisar la política corporativa para la protección del entorno del ICS.		Puede realizarse elaborando directivas y procedimientos de apoyo que definan requisitos únicos para el entorno del ICS con respecto a la naturaleza del entorno de los controles (fabricación/logística/control del entorno/producción de energía, etcétera). Se debe hacer referencia a los aspectos reglamentarios disponibles para estos entornos (por ejemplo, de la Administración Nacional de Alimentos y Fármacos de los Estados Unidos [FDA, por sus siglas en inglés], buenas prácticas en clínica, laboratorio y manufactura [GxP, por sus siglas en inglés], autoridad cibernética).	2
Controles industriales	12.2	Definir reglas para el uso adecuado de los equipos en el entorno de producción y señalar lugares que expliquen esas reglas.	La organización definirá una señalización que explique las prácticas en materia de seguridad de datos en las estaciones de trabajo que controlan y supervisan el entorno de producción.	La señalización puede referirse, entre otras cosas, al uso de estaciones de trabajo compartidas, a la utilización de dispositivos de medios extraíbles, al cierre de sesión de los usuarios, etcétera.	1
Controles industriales	12.3	Especificar los procesos sensibles donde existen entornos de control industrial según su grado de sensibilidad.	La organización mapeará los procesos donde existen entornos de control y definirá los principales procesos operacionales en que se dan estos controles a fin de comprender el nivel de daño a la organización que podría proceder de dichos entornos.	Documentar los procesos de mapeo y los entornos según la gravedad.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Controles industriales	124	Separar las redes de control de otros sistemas y redes externas.	La organización establecerá redes de control, redes de usuarios o servidores en redes separadas para restringir el acceso directo entre redes.	La separación se puede llevar a cabo utilizando cortafuegos y redes de área local virtual (VLAN, por sus siglas en inglés) separadas para cada red de monitoreo. Si se da la opción, es preferible realizar la separación por un diodo unidireccional y permitir solo la divulgación de información fuera de la organización.	1
Controles industriales	125	Separar el sistema de gestión de los controladores de equipos industriales y los componentes operativos del sistema.	Implementar una separación adecuada entre la red de controles operativos y el sistema de gestión de los controles.		2
Controles industriales	126	No conectar dispositivos que no sean controles del entorno de producción a la red de controles de producción.	La organización no instalará equipos que no formen parte del ICS en la red de controles. Si un equipo debe conectarse, se utilizará una red separada y la comunicación se habilitará individualmente.	Si es necesario conectar diferentes equipos para interfaces con sistemas de producción, debe conectarse por un segmento de red separado detrás del cortafuegos.	1
Controles industriales	127	Permitir el acceso de los proveedores de soporte a la red de producción únicamente mediante autorización previa, así como a través de una comunicación segura e identificada que permita registrar las acciones del proveedor.	La organización implementará una red de comunicaciones segura para el acceso de los proveedores y revisará el acceso del proveedor a la organización al proporcionar una autorización previa para cualquier conexión del proveedor a la red de control.	Esto puede aplicarse utilizando un sistema de administración de servidor VPN para usuarios dedicados para cada proveedor (prioridad del usuario para cada empleado del proveedor), que generalmente se bloqueará y solo se abrirá cuando sea necesario.	2
Controles industriales	128	Impedir el acceso directo a Internet desde el entorno de controles industriales y desde el entorno de HMI.		Es posible limitar las redes de control en el cortafuegos y deshabilitar el acceso de comunicación directa de estas redes a Internet. Se permitirán actualizaciones desde una red de búfer individualmente, solo después de pasar a través de equipos tales como un proxy.	2
Controles industriales	129	Limitar los servicios innecesarios en el entorno de producción y los sistemas de soporte, como las HMI y los sensores inteligentes.	La organización cancelará o limitará los servicios innecesarios para todos los sistemas en el entorno de control, ya sea a nivel de sistema operativo, de comunicaciones o de aplicación.	Es posible basarse en los documentos de endurecimiento de los fabricantes del sistema operativo y las aplicaciones, y cerrar servicios, bloquear puertos, limitar el acceso de aplicación a ciertas funciones, etcétera.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Controles industriales	12.10	Utilizar una comunicación segura entre controles industriales y equipos terminales, si es posible.	Utilizar protocolos que permitan la autenticación y el cifrado de origen y destino del medio que admite el equipo.	En el caso de que sea posible usar versiones seguras de estos protocolos, emplear tales versiones (SFTP, HTTPS, SNMPv3, etcétera).	2
Controles industriales	12.11	Establecer un equipo de comunicación unidireccional desde la fabricación hasta los sistemas sensoriales.		Configurar herramientas para la transferencia de comunicación unidireccional entre sensores y sistemas en entornos sensibles.	4
Controles industriales	12.12	Separar las redes inalámbricas en el entorno de producción de las redes inalámbricas de la empresa.	La organización implementará una red inalámbrica específica separada de la red inalámbrica empresarial, que se utilizará únicamente para controlar las comunicaciones de red. Esta red no redirigirá a la red empresarial ni viceversa.	Es preferible evitar el uso de una red inalámbrica en las redes de control, pero si fuera necesario para el funcionamiento del negocio, esta red se configurará por separado y su administración también estará separada y no estará vinculada a ninguna red interna de VLAN.	1
Controles industriales	12.13	Limitar la comunicación inalámbrica en el entorno de producción mediante el uso de protocolos seguros.		Se ha de usar el protocolo de acceso wifi protegido-clave previamente compartida (WPA-PSK 2, por sus siglas en inglés) y, si es posible, se recomienda usar una versión certificada digitalmente para estas redes inalámbricas.	1
Controles industriales	12.14	Definir un usuario separado para cada cliente final que utilice una red inalámbrica en el entorno de producción.	La organización establecerá un usuario específico para todos y para cada equipo de red inalámbrica.	Se recomienda conectar la red inalámbrica a un servidor Radius dedicado, que autentificará a los usuarios de esta red y permitirá su administración.	2
Controles industriales	12.15	Permitir el acceso a las HMI por medio de usuarios personales para cada operador.	La organización definirá un usuario personal para cualquier persona que trabaje con la HMI. Si se comparte el puesto, se puede utilizar la identificación mediante tarjeta inteligente.		2
Controles industriales	12.16	Permitir el acceso a las HMI mediante el uso de una autenticación robusta.	La organización definirá una autenticación robusta para acceder a la HMI.	Es posible utilizar diversos medios, como biometría, tarjetas inteligentes, OTP, etcétera.	4

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Controles industriales	12.17	Instalar sistemas de monitoreo y registrar la actividad en los servidores de administración.	La organización establecerá un sistema para grabar los registros de actividad en los servidores de administración del entorno de control.	Se pueden utilizar diversos medios, como herramientas para grabar pantallas y actividades de usuarios, grabar registros de aplicaciones, etcétera.	2
Controles industriales	12.18	Instalar utilidades tales como herramientas de detección de intrusiones en el entorno de redes de administración del entorno de producción.		Puede realizarse mediante el uso de IPS, la HIPS y herramientas similares, como los <i>honeypots</i> o redes trampa.	3
Controles industriales	12.19	Instalar herramientas para la verificación de la firma de los archivos (verificación de integridad) a fin de escanear los archivos que se transfieren al entorno de administración o se instalan en él.		Se puede realizar utilizando diversas herramientas de comprobación de la integridad de los archivos.	3
Controles industriales	12.20	Instalar herramientas anticódigo malicioso específicas en las HMI.		Se puede implementar utilizando herramientas anticódigo malicioso específicas, según el tipo de sistema.	1
Controles industriales	12.21	Instalar las actualizaciones de software del fabricante en los entornos inferiores (entornos de prueba) antes de instalarlas en el entorno de producción.	La organización velará por la instalación de actualizaciones en un entorno de prueba y las ejecutará paulatinamente a fin de probar la estabilidad del sistema y el proceso.	Puede realizarse estableciendo un entorno inferior (al menos parcialmente), desviando la comunicación a este entorno durante un período de mantenimiento en el entorno de producción y probando el proceso.	2
Controles industriales	12.22	Instalar actualizaciones del sistema operativo en el entorno de producción que sean compatibles con el proveedor.	La organización implementará en un plazo razonable el sistema operativo y las actualizaciones de la aplicación tal como se reciben del proveedor del sistema y exigirá al proveedor actualizaciones de seguridad para fallas graves a medida que se publiquen.		1

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Controles industriales	12.23	Instalar las herramientas de “Configuración de bloqueo” en los sistemas de fin de vida, incluidos los sistemas operativos obsoletos.	La organización implementará herramientas que bloquean la configuración del sistema en una configuración “limpia” si no hay una opción para actualizar el equipo.		3
Controles industriales	12.24	Limitar la capacidad de conectar medios extraíbles a los equipos de producción, incluidos controladores, HMI y sensores.		Puede realizarse eliminando físicamente los dispositivos USB (bloqueo de puerto) o lógicamente mediante la política del sistema operativo: directiva de grupo (GPO, por sus siglas en inglés).	2
Controles industriales	12.25	Llevar a cabo la transferencia de archivos de medios extraíbles a los sistemas de producción después del “lavado” de los archivos transmitidos.	La organización implementará un sistema de “lavado” de archivos y los probará exhaustivamente sirviéndose de algunas herramientas antes de transferirlos al entorno de control.	Se puede realizar mediante la adquisición de una estación de lavado especializada o, alternativamente, mediante el establecimiento de una estación dedicada, que incluya varios motores de escaneo diferentes.	2
Controles industriales	12.26	Instalar un sistema de redundancia para los componentes esenciales del entorno de producción.	La organización implementará un sistema de redundancia de servidores y sensores críticos en el entorno de control de cara a la continuidad del proceso.	Para generar redundancia, se recomienda consultar con el proveedor del sistema de control.	2
Controles industriales	12.27	Limitar el acceso físico para las necesidades de funcionamiento de la organización solo al entorno de controles industriales, así como a los equipos de comunicaciones de este entorno.	La organización limitará el acceso físico a los bastidores (racks) de comunicación, concentradores y estaciones de administración del entorno de los controles.	Se puede realizar mediante la conversión de salas dedicadas a comunicaciones y servidores concentrados, y realizar el control de acceso utilizando etiquetas de acceso o biometría para este entorno.	2
Controles industriales	12.28	Limitar el acceso lógico para las necesidades de funcionamiento de la organización solo al entorno de controles industriales, así como a los equipos de comunicaciones de este entorno.	La organización limitará el acceso de los usuarios de la organización que no tengan relevancia institucional al sistema de control y evitará su acceso a estas redes y equipos.		2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Controles industriales	12.29	Limitar el acceso lógico, siempre posibilitando el funcionamiento de la organización, a los sistemas de producción, incluidas las interfaces de control, las de muestra y las HMI.	El acceso a los sistemas de gestión estará limitado según los perfiles de usuario. Un controlador del sistema no cambiará la configuración ni los parámetros de un sistema. El cambio de los parámetros será realizado por un usuario administrador.	Es posible verificar con el fabricante del sistema si este soporta el uso de diferentes perfiles de usuario.	3
Controles industriales	12.30	Realizar pruebas de seguridad de la información en los entornos y la interfaz de producción y gestión, incluidas las pruebas de penetración.	La organización definirá un esquema exhaustivo de pruebas, también para la variedad de componentes de la red de control, con énfasis en pruebas de seguridad de la información integrales para todos los componentes, a fin de mantener la continuidad del proceso de la organización.	Puede realizarse comprobando la configuración del entorno, ejecutando simulaciones durante los períodos de tiempo de inactividad y realizando pruebas de penetración en estas redes si es posible o durante las operaciones de mantenimiento.	2
Controles industriales	12.31	Configurar escenarios de monitoreo únicos en el entorno de producción y hacer un seguimiento de ellos mediante una matriz de monitoreo organizacional.	La organización definirá un rango de escenarios de monitoreo para el entorno de control en función del perfil de las amenazas y la importancia del sistema para el proceso organizacional.	El monitoreo de red en las redes de control es diferente del de los sistemas ordinarios, ya que el umbral de sensibilidad es más bajo. Cualquier desviación en la cantidad de comunicación normal entre los controles y las interfaces y sensores de gestión puede indicar un posible ciberincidente, pues la actividad en estos entornos es continua y constante.	2
13. Proteger los teléfonos móviles Los teléfonos celulares se han convertido en importantes herramientas profesionales: contienen los contactos, la correspondencia por correo electrónico, diversas aplicaciones empresariales, contraseñas, etc. En muchos casos, permiten el acceso a redes corporativas y la navegación web.				Por lo tanto, es fundamental para la ciberdefensa de la organización una definición correcta de los privilegios de los teléfonos, de su uso en la empresa y su protección. Se necesita establecer el control de su acceso y la seguridad de la configuración, implementar herramientas de protección específicas, asegurar canales de comunicación con la organización, disponer una administración centralizada, incluido el control remoto en caso de pérdida, etcétera.	
Proteger los teléfonos móviles	13.1	Configurar la política de uso del teléfono móvil y actualizarla periódicamente.	La organización ha de establecer una política de uso de teléfonos móviles de acuerdo con sus necesidades, incluido el acceso a las aplicaciones empresariales y el mantenimiento de los datos confidenciales de la organización en el teléfono móvil.		2
Proteger los teléfonos móviles	13.2	Implementar mecanismos de protección para controlar el acceso a los teléfonos móviles, como contraseñas o medidas biométricas.	La organización debe fijar los parámetros para controlar el acceso a los dispositivos móviles, como una contraseña de cierta longitud y el bloqueo automático.	Eso puede realizarse utilizando configuraciones de directivas automatizadas, que se apliquen a un dispositivo cuando esté conectado a una red de la organización.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Proteger los teléfonos móviles	13.3	Aplicar una configuración de seguridad en los teléfonos, que restrinja el acceso al teléfono, mantenga el software actualizado, limite los riesgos de instalar aplicaciones peligrosas, etcétera.	La organización debe establecer la aplicación de varios parámetros en los sistemas operativos de los teléfonos móviles y su efectiva implementación en los dispositivos. Estas configuraciones incluyen la aplicación de actualizaciones de software, la restricción de servicios peligrosos, la limitación de la instalación de software desconocido o arriesgado, etcétera.	Eso puede hacerse utilizando configuraciones de directivas automatizadas, que se apliquen a los dispositivos cuando estén conectados a la red empresarial o mediante un sistema de administración centralizado.	3
Proteger los teléfonos móviles	13.4	Implementar el cifrado de los datos confidenciales almacenados en los dispositivos móviles.	Los datos confidenciales de la organización, almacenados en el dispositivo móvil, como el correo electrónico corporativo, los archivos confidenciales y las aplicaciones confidenciales, se cifrarán utilizando el sistema operativo del dispositivo o mediante aplicaciones específicas.	Esa configuración se puede hacer mediante aplicaciones de cifrado de datos (aplicación de correo electrónico seguro, por ejemplo) o particiones cifradas que utilizan el sistema operativo.	2
Proteger los teléfonos móviles	13.5	Implementar herramientas de protección específicas que detecten y bloqueen el acceso no autorizado y las aplicaciones hostiles en los dispositivos móviles.	Los dispositivos móviles, especialmente los que son propiedad de los empleados de la organización, están expuestos a la infiltración de programas hostiles, ya sea insertados en un dispositivo sin el conocimiento de su propietario o disfrazados como una aplicación inocente. Para bloquear el código malicioso que podría llevar a la exposición de información confidencial de la empresa, se deben ejecutar aplicaciones especializadas que detecten y eviten la ejecución del código hostil.	Ello se puede aplicar usando sistemas comerciales diseñados para proteger dispositivos móviles, o mediante dispositivos comerciales que implementan este tipo de funciones de defensa.	3
Proteger los teléfonos móviles	13.6	Implementar el cifrado de datos confidenciales en la comunicación entrante y saliente de los dispositivos móviles.	Las comunicaciones de datos entrantes y salientes desde teléfonos móviles utilizan redes públicas no seguras. Para proteger la información frente a la posibilidad de una exposición es necesario cifrarla.	Eso puede hacerse utilizando protocolos de cifrado convencionales y aplicaciones que realizan operaciones de cifrado mientras acceden a la red de la organización.	2


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Proteger los teléfonos móviles	13.7	Implementar medidas de control de acceso en la red móvil de la organización.	Los dispositivos móviles que se conectan a la red corporativa están utilizando interfaces de acceso remoto a la red. Para asegurar esta interfaz, se debe implementar el control de acceso, por ejemplo, mediante el uso de tecnologías de certificados digitales y contraseñas.		3
Proteger los teléfonos móviles	13.8	Disponer un sistema de administración centralizado, que administre la configuración de los dispositivos móviles y permita la eliminación remota de datos del dispositivo.	La aplicación de una configuración segura en los teléfonos móviles y el control remoto de los datos confidenciales almacenados en ellos es posible gracias a un sistema de administración central y a componentes de administración que se instalan en los dispositivos.		2
Proteger los teléfonos móviles	13.9	Implementar un sistema central de monitoreo de la seguridad de la información, que reciba alertas sobre eventos inusuales en dispositivos móviles y permita la contención y la respuesta a incidentes.	Para detectar incidentes de ataque en los dispositivos móviles y permitir su contención y una respuesta adecuada, es necesario implementar un sistema de monitoreo centralizado, que reciba alertas de los componentes instalados en los dispositivos móviles.		3
Proteger los teléfonos móviles	13.10	Establecer una directiva para la protección o restricción de llamadas realizadas en los teléfonos móviles.	Los dispositivos móviles utilizan redes públicas no seguras: la organización debe establecer reglas de etiqueta y precaución al hacer llamadas telefónicas sensibles.		4
14. Gestión del cambio El entorno cibernético de la organización también necesita realizar cambios y actualizaciones periódicas, como parte del proceso de desarrollo y actualización de la organización. Estos incluyen la adquisición de empresas y su integración dentro de la infraestructura de la organización, las actualizaciones tecnológicas, la adición o el cambio de los procesos operacionales (por ejemplo, en la cadena de suministro), etc.				Estos procesos de cambios o actualizaciones conllevan un gran riesgo de dañar los sistemas de la organización y la información que contienen. En consecuencia, la organización debe gestionar los cambios con el fin de reducir el riesgo, incluyendo una política de gestión de la configuración para el entorno cibernético en la organización, su documentación y actualización continua.	
Gestión del cambio	14.1	Definir e implementar una política de administración de la configuración, revisarla y actualizarla periódicamente.		El capítulo de gestión del cambio se encuentra en la política de seguridad de la información corporativa y en los procedimientos de apoyo.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Gestión del cambio	142	Configurar, registrar y actualizar la configuración básica del sistema de información cuando sea necesario.	La organización registrará la configuración del sistema de información durante su establecimiento, incluida la documentación de los componentes, la comunicación, la configuración del sistema, así como su procedimiento de instalación.	Puede aplicarse definiendo una cartera del sistema.	2
Gestión del cambio	143	Examinar la configuración existente de los sistemas de información periódicamente y cuando ocurran incidentes que fueron definidos por la organización y son parte integral del proceso de instalación y actualización de una versión.	La organización registrará los cambios en los sistemas de información cuando se produzca una reconfiguración importante o una vez cada cierto período de tiempo determinado (lo que suceda primero).	Se puede realizar a través de un proceso de documentación de los cambios.	2
Gestión del cambio	144	Implementar mecanismos automáticos para mantener actualizada la configuración básica del sistema de información, incluida su integridad y la preparación de la configuración.	La organización implementará un conjunto de respaldo y restauración para la configuración del sistema de información y sus componentes.		3
Gestión del cambio	145	Mantener las versiones anteriores de la configuración del sistema para permitir una reversión.	La organización se asegurará de que existan herramientas y métodos de reversión para deshacer los cambios ineficaces.	Esto se puede aplicar utilizando un respaldo completo del sistema antes del cambio y mediante la actualización gradual de los componentes (entorno de prueba o entorno de recuperación ante desastres, etcétera).	2
Gestión del cambio	146	Determinar qué cambios en el sistema se definen como cambios de configuración, solicitudes de cambio de configuración de documentos y su estado (aprobado/ejecutado/rechazado) y guardarlos durante un período de tiempo determinado.	La organización gestionará un proceso de ratificación de cambios antes de aplicarlos.	Esto se puede aplicar mediante la celebración de reuniones semanales de gestión de cambios y la ratificación de cambios mientras se explica la naturaleza de los mismos.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Gestión del cambio	14.7	Implementar un mecanismo automático para documentar las solicitudes de cambios de configuración, alertar a la autoridad de certificación y prohibir hacer cambios hasta recibir todas las aprobaciones necesarias.	La organización operará un sistema de información que coordinará el proceso de gestión de cambios en general y el proceso de ratificación de cambios en particular.		4
Gestión del cambio	14.8	Analizar los cambios en el sistema de información a fin de determinar las posibles consecuencias en materia de seguridad antes de implementar el cambio (debido a puntos débiles, falta de conformidad, mala intención, etcétera).	La organización gestionará un proceso de evaluación de riesgos como parte de la gestión del cambio organizacional. Se documentarán los posibles impactos en la disponibilidad y fiabilidad del sistema, como parte de las etapas de presentación de una solicitud de cambios.	Se puede aplicar a través de un cuestionario complementario para la solicitud de cambios de gestión, que enumerará sus riesgos al realizar los cambios.	2
Gestión del cambio	14.9	Analizar los cambios de configuración en el entorno de información en un entorno de prueba separado antes de su implementación en el entorno de producción.	La organización examinará los cambios en un entorno de prueba separado antes de implementar cambios en el entorno de producción.	Esto puede realizarse mediante el mantenimiento de un entorno de prueba, en una versión similar al entorno de producción.	2
Gestión del cambio	14.10	Después de realizar cambios de configuración en el sistema de información, verificar las funciones de seguridad para asegurarse de que funcionen correctamente.	La organización verificará todo el sistema y sus componentes en relación con los aspectos de seguridad de la información, que incluyen autenticación, autorización, cifrado, endurecimiento y cualquier otra funcionalidad de seguridad de la información en el sistema.	Se debe ejecutar a través del panorama general del monitoreo requerido y, de ser necesario, incluso mediante pruebas tales como estudios de controles y pruebas de penetración.	3
15. Seguridad de los soportes físicos Los soportes físicos (magnéticos, extraíbles, ópticos, mecánicos) se utilizan para introducir y extraer información de la organización. Los soportes físicos se emplean para el almacenamiento y la portabilidad de la información tanto dentro de la organización como fuera de ella.				Esta información puede ser sensible para la organización, sus clientes o sus proveedores y, por lo tanto, es necesario protegerla de la posibilidad de caer en manos de cualquier agente no autorizado. Los soportes físicos también pueden usarse para introducir software abusivo dentro de la organización. Por consiguiente, es necesario definir e implementar una política de manejo y protección de los soportes físicos que contemple también su desguace.	

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad de los soportes físicos	15.1	Definir e implementar una directiva de protección de soportes físicos (magnéticos, extraíbles, ópticos, mecánicos), y revisarla y actualizarla de manera periódica.	La organización redactará e implementará una política de uso y protección para los soportes físicos, que incluirá la referencia a su uso, la manera en que almacenarán la información y cómo se destruirá la información almacenada o los propios soportes al final de su uso (o tras el fin de la vida de los soportes).	La política considerará, por ejemplo, los tipos de dispositivos aprobados frente a los prohibidos, el uso de cuáles soportes está permitido o prohibido (como una computadora portátil, una memoria removible, un teléfono de trabajo) para fines privados, si está permitido salir con estos soportes físicos fuera de la organización, y qué hacer con los soportes físicos cuando están defectuosos o se dejan de usar. De esta política surgirán los procedimientos relevantes para la organización, tales como los procesos de mapeo de los soportes físicos y los medios de distribución (como la compra de discos magnéticos para los servidores, medios ópticos, etc.) y el acceso a los medios antes mencionados de acuerdo con los procedimientos de la organización para los funcionarios relevantes (como acceso a discos duros solo para personal de TI, acceso a medios extraíbles para los funcionarios pertinentes, etcétera).	2
	15.2	Identificar cada soporte de acuerdo con el nivel de seguridad de los datos almacenados, y señalar su tratamiento en relación con la seguridad de los datos y los aspectos acerca de las limitaciones de distribución.	La organización definirá los procedimientos y procesos de identificación de los soportes, y los identificará de acuerdo con el nivel de seguridad de los datos almacenados.	Los soportes se pueden identificar con adhesivos pegados a las cintas de respaldo, los cables de salida de los discos duros y los discos ópticos.	2
	15.3	Almacenar los soportes de forma segura.	La organización definirá los métodos de seguridad de almacenamiento de datos, de acuerdo con varios tipos de soportes (magnéticos, ópticos, extraíbles).	Se puede implementar mediante la protección física de áreas de almacenamiento de medios físicos, la codificación de las copias de respaldo y el almacenamiento de los soportes magnéticos en una instalación de almacenamiento con licencia, la protección de los gabinetes de comunicación que alojen servidores y el almacenamiento de dispositivos y discos duros, y el almacenamiento de soportes ópticos y componentes de dispositivos de codificación (HSM) en cajas de seguridad.	2
	15.4	Definir procesos de “oscurecimiento” (<i>blackening</i>) o destrucción de soportes físicos.	La organización definirá procedimientos y procesos para el oscurecimiento (que consiste en eliminar todos los datos confidenciales de un componente antes de que salga de la organización o se asigne a un uso diferente) y la destrucción de los soportes, así como para llevar a cabo una vigilancia continua de la implementación de estos procedimientos de oscurecimiento y destrucción. Asegurarse de que los datos confidenciales no salgan de la organización sin control.	El “oscurecimiento” de los medios se puede realizar manualmente (como la eliminación individual de datos confidenciales: detalles de la tarjeta de crédito, detalles que pueden servir para identificar a clientes, etc.) o de manera tecnológica (eliminación sistemática de patrones conocidos). La destrucción de los soportes se puede hacer por trituración, magnetización o restablecimiento por sobrescritura.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad de los soportes físicos	15.5	Limpiar los medios extraíbles al conectarlos a la red de la organización, para asegurarse de que no contengan código malicioso u otros componentes maliciosos.	La organización definirá un proceso de “blanqueamiento” de datos (escaneo y limpieza de amenazas de código malicioso), antes de incorporar los soportes al interior de los sistemas de la organización.	Eso puede implementarse definiendo estaciones especiales de blanqueamiento, para escanear los medios antes de su conexión a los sistemas de la organización.	2
Seguridad de los soportes físicos	15.6	Definir e implementar limitaciones al uso de los soportes, utilizando medios de seguridad.	La organización definirá e implementará tecnologías y métodos para limitar el uso de los soportes. Eso se hace para minimizar la filtración de datos o las amenazas de penetración de código malicioso a la red de la organización, a través de medios extraíbles.	Puede implementarse endureciendo las estaciones de trabajo de acuerdo con el tipo de sistema o estación, o las autorizaciones de los empleados, permitiendo que solo los empleados autorizados conecten dispositivos de memoria extraíbles (como una memoria USB) a la computadora. Se puede implementar una definición por la cual se cifren los datos que se transfieran de una estación a un dispositivo extraíble.	2
Seguridad de los soportes físicos	15.7	Implementar un mecanismo de cifrado para asegurar los medios digitales transferidos fuera de la organización.	La organización implementará tecnologías de cifrado para los soportes destinados a salir de la organización, o que se usen constantemente fuera de la organización (medios extraíbles).	Puede implementarse mediante herramientas de cifrado de datos extraíbles, cifrado de cintas de respaldo, durante el respaldo, etcétera.	3
Seguridad de los soportes físicos	15.8	Inspeccionar periódicamente los equipos de blanqueamiento y destrucción de medios para validar su efectividad.	La organización definirá un proceso de inspección de los equipos de destrucción y blanqueamiento de medios, incluida la verificación de la efectividad de los procesos y tecnologías implementados.	Los sistemas de blanqueamiento o destrucción pueden inspeccionarse periódicamente por muestreo, como intentar insertar un archivo “ficticio”, intentar leer o recuperar un archivo confidencial de un soporte obsoleto.	3
16. Cadena de suministro y externalización Muchas organizaciones dependen de servicios comprados a proveedores externos. Estos pueden ser subcontratistas que producen componentes computarizados, proveedores de servicios informáticos, diversas aplicaciones compradas a proveedores externos, etc.				Dichos servicios pueden estar vinculados a los sistemas de las organizaciones, por lo que constituyen posibles canales de ataque. Por ello, la organización tiene que defenderse de ser dañada por sus proveedores, algo que hace mediante demandas legales y contractuales con sus proveedores, informándose sobre los mecanismos de ciberdefensa de los proveedores, diseñando procedimientos de trabajo, etcétera.	
Cadena de suministro y externalización	16.1	Defenderse de las potenciales amenazas de la cadena de suministro para el sistema, como parte de una defensa en general.	La organización mapeará y detectará amenazas y riesgos derivados de los sistemas y servicios, tecnologías y procesos de los proveedores, y mapeará los riesgos como parte de la gestión de riesgos y amenazas de la organización.	El proceso de mapeo puede contar con el apoyo de una recopilación de datos de inteligencia cibernética sobre el proveedor, a fin de tener en cuenta dicha información al considerar y decidir sobre la gestión de riesgos. Se deben considerar los mecanismos, controles y procesos existentes del proveedor, y su influencia en los procesos operacionales respaldados por el sistema o servicio. Por ejemplo, los controles de automatización y los servidores virtuales instalados por el proveedor en una plataforma en la nube y su método de endurecimiento pueden influir en la organización si estos entornos no se endurecen lo suficiente o si el proveedor de servicios en la nube no está asegurado o está situado en un país hostil, etcétera.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Cadena de suministro y externalización	16.2	Usar herramientas legales y contractuales al comprar un sistema de datos o un servicio de proveedores externos. 	La organización utilizará mecanismos contractuales, como los de responsabilidad limitada y otros mecanismos legales, para minimizar los riesgos derivados de la compra.	Además de las cláusulas de responsabilidad limitada e indemnización, el cumplimiento de los requisitos legales y reglamentarios, se pueden estipular cláusulas referentes a alertas tempranas, apoyo técnico durante el servicio o apoyo ampliado en caso de interrupción más allá del fin de la vida útil del sistema, acuerdos de confidencialidad y almacenamiento seguro de datos, o cualquier otra cláusula que constituya un factor de control, que compense los riesgos incorporados en el establecimiento del sistema o la compra del servicio.	2
Cadena de suministro y externalización	16.3	Realizar un estudio de proveedores antes de firmar un contrato de compra de servicios o productos	La organización estudiará el carácter y la conducta de los proveedores antes de firmar el contrato.	El estudio de proveedores puede examinar los siguientes aspectos acerca de ellos: la madurez, la integración o el número de clientes, la estabilidad, la capacidad de servicio, el mecanismo de seguridad de los datos, la continuidad del negocio, etcétera.	3
Cadena de suministro y externalización	16.4	Implementar controles preventivos para minimizar los daños causados por las infraestructuras del proveedor en casos de conexión a la red del proveedor.	La organización utilizará sus propios controles u otros controles designados para minimizar los daños causados por las infraestructuras del proveedor.	Dichos controles pueden ser la separación del entorno o la interfaz, la sanitización del producto del proveedor, la separación de la comunicación por un servidor proxy, etcétera.	3
Cadena de suministro y externalización	16.5	Inspeccionar el aspecto de la seguridad de los datos del sistema o servicio antes de la instalación.	La organización inspeccionará el sistema o servicio con sus propias herramientas, y también tratará de penetrarlo antes de pasar a la producción.	El sistema puede ser examinado mediante herramientas de gestión de vulnerabilidades o mediante encuestas de riesgo y pruebas de penetración, con el fin de garantizar la inexistencia de hallazgos graves que puedan dañar a la organización y sus procesos.	4
Cadena de suministro y externalización	16.6	Definir el nivel de importancia del sistema o servicio en relación con los procesos operacionales dependientes.	La organización definirá un determinado sistema como crítico si cualquier daño que sufra influye en un proceso organizacional esencial.	Agregar el sistema o servicio a la lista de sistemas críticos. Vigilarlo para verificar su continuidad.	3
17. Seguridad en las compras y el desarrollo En los procesos de compra y desarrollo, la organización introduce componentes cibernéticos en sus sistemas (compra de un nuevo sistema de software o desarrollo de una herramienta especializada). El código malicioso puede penetrar en la red de la organización a través de los procesos de compra y desarrollo. Por otro lado, se pueden integrar varias defensas durante el desarrollo de un producto, lo que ayudará a la organización en el futuro a hacer frente a las amenazas cibernéticas.				Los controles están destinados a minimizar los riesgos de que una compra o un sistema o software desarrollado introduzcan riesgos cibernéticos en la organización. Los controles incluyen definir una política para todas las entidades dentro de la organización (compras, legales, gerentes de proyectos, desarrolladores, etc.), que incluye requisitos de defensa frente a entidades de compra o desarrollo, y la gestión de riesgos en la compra o el desarrollo, las defensas a lo largo del ciclo de vida del software o sistema.	
Seguridad en las compras y el desarrollo	17.1	Elaborar, implementar y revisar periódicamente la política de compra y desarrollo.	Estos controles están destinados a verificar que todos los sistemas cumplan con la referencia de seguridad definida por la organización, tanto los desarrollados internamente como los comprados o como un servicio en la nube.	Esta política incluirá, entre otras cosas, una referencia al acuerdo sobre el nivel de servicio deseado, cumpliendo los requisitos de protección en todos los niveles (política de contraseñas, registros, cifrado, etc.), acceso remoto, acceso de los desarrolladores a la producción, etcétera.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad en las compras y el desarrollo	17.2	Para sistemas con un nivel 3, garantizar el cumplimiento de las normas por parte de entidades externas e independientes.	La organización se asegurará de que los activos clasificados en el cuestionario de valor como de nivel 3 o superior cumplan con todos los requisitos de la Metodología de Ciberdefensa. Esto lo realizará un perito externo a la organización desarrolladora o compradora.	En casos de desarrollo interno, se puede ser asistido por una empresa de asesoramiento o registro para examinar que la protección del sistema cumpla la Metodología de Ciberdefensa. En casos de compra externa, asegurarse de que el sistema cumpla con los requisitos de nivel 3 de la Metodología o, alternativamente, solicitar al proveedor que presente certificados de cumplimiento de estándares comunes, como los controles para organizaciones y sistemas (SOC1/SOC2, por sus siglas en inglés), así como otros requisitos (como la conformidad con la PCI, la Ley de Portabilidad y Responsabilidad de los Seguros de Salud [HIPAA, por sus siglas en inglés], etc., de acuerdo con el tipo de datos almacenados o procesados por el sistema), unos certificados que se almacenarán y respaldarán en el acuerdo de compra o desarrollo (incluido el compromiso de notificar si el certificado se anula o caduca).	4
Seguridad en las compras y el desarrollo	17.3	Gestión del riesgo cibernético: evaluar los riesgos de seguridad informática y cibernética que implica el desarrollo o compra de un nuevo sistema o servicio. Administrarlos de acuerdo con los procesos de gestión de riesgos existentes.	El control está destinado a verificar que los aspectos de protección se tienen en cuenta desde el principio y planificación hasta las fases de desarrollo y producción. Asegurarse de que la iniciación, la compra o el desarrollo se basen en un estudio de los riesgos incurridos y su integración dentro de la gestión de riesgos de la organización.	Se recomienda iniciar la gestión de riesgos en la fase de iniciación, a fin de estar preparado para integrar los controles dentro del proceso de desarrollo o listo para vivir con los riesgos detectados. Se puede recibir asistencia en la gestión de riesgos con métodos conocidos, como las publicaciones sobre ciclo de vida de desarrollo de sistemas seguro (SSDLC, por sus siglas en inglés), publicaciones del SANS o del proyecto abierto de seguridad de aplicaciones web (OWASP, por sus siglas en inglés). Considere que la externalización y los sistemas en la nube incorporan riesgos específicos, algunos de los cuales se describen en esta publicación. Se recomienda familiarizarse con las recomendaciones de estándares específicos, como ISO 27017, CSA, etcétera.	3
Seguridad en las compras y el desarrollo	17.4	Protección cibernética como parte del ciclo de vida del desarrollo: tener en cuenta las consideraciones de seguridad en cada etapa del ciclo de vida del desarrollo del sistema y definir qué empleados se ocuparán de los aspectos de seguridad en cada etapa.	La organización promoverá un proceso ordenado de desarrollo seguro, definiendo las etapas de implementación de la seguridad de la información en cada etapa del proceso de desarrollo, y se asegurará de que los principales agentes responsables de las etapas del proceso de desarrollo acepten la responsabilidad de sus roles en la seguridad del sistema y cuenten con los conocimientos necesarios para hacerlo.	Es posible definir requisitos de seguridad de la información en la fase de iniciación, en la fase de diseño (la fase de prueba de concepto), en la fase de implementación (fase de adquisición, desarrollo e implementación) y en la etapa de presentación (pruebas y ensayos de seguridad de la información antes de pasar a producción). En estas etapas, es necesario definir las pautas y la responsabilidad para asegurarse de que se cumplen las consideraciones y requisitos de seguridad en el proceso. Las consideraciones de seguridad en el proyecto también incluirán aspectos que no son tecnológicos, o no directamente relacionados con el desarrollo y la presentación, como el almacenamiento de información con el proveedor al final del desarrollo, la compartimentación en las instalaciones del proveedor, los procedimientos de acceso remoto, el acuerdo de nivel de servicio, el compromiso de dar soporte para el producto durante un período específico, el método de transferencia de archivos y la información del cliente al proveedor, etc. Utilizar los controles incluidos en el apartado sobre externalización de este documento.	




Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad en las compras y el desarrollo	17.5	Incluir los siguientes requisitos y criterios para cerrar el contrato de compra del sistema, componente o servicio: requisitos de seguridad funcional, de protección, de monitoreo, de documentación, configuración de un entorno de producción, requisitos de admisión.	El objetivo es una definición formal de los requisitos de protección para cada proyecto y contratación a nivel contractual.	Es posible definir una colección de plantillas de documentos de requisitos de seguridad de la información para usar al caracterizar sistemas en desarrollo o adquisición. El documento incluirá los controles que se espera que el proveedor aborde en función del nivel de valores esperados del sistema planificado de acuerdo con los criterios de la Metodología de Ciberdefensa.	
Seguridad en las compras y el desarrollo	17.6	Exigir a los desarrolladores del sistema que proporcionen una descripción funcional de los controles de seguridad que se implementarán, así como información sobre el diseño y la implementación de estos controles.	La organización exigirá la documentación completa de los controles de seguridad de los datos integrados en el sistema para garantizar el cumplimiento de los requisitos de seguridad en materia de datos y por el bien del proceso de gestión de riesgos y amenazas de la organización.	Se recomienda que como parte de la documentación completa del sistema se obtengan los documentos de diseño de nivel funcional, de alto nivel y de la implantación o de bajo nivel, incluida la documentación de los controles. Dicha documentación tratará, entre otros asuntos, del tipo de cifrado, las pruebas de entrada, los <i>scripts</i> de ciberdefensa, etc. En la documentación el proveedor se referirá a su propio desarrollo y a aplicaciones externas (bibliotecas, complementos, <i>software</i> de terceros, interfaces externas, etcétera). Este control no pretende verificar la mera implementación de los requisitos de seguridad, sino cómo se hace (protocolos, procesos, herramientas de soporte, etcétera).	3
Seguridad en las compras y el desarrollo	17.7	Arquitectura de seguridad: implementar principios de arquitectura de seguridad dentro de la caracterización, diseño, desarrollo, implementación y alteración de un sistema de datos.	La organización garantizará que se implemente una arquitectura de seguridad en la planificación del sistema, ya sea internamente o mientras controla los procesos de un proveedor externo.	Los principios de arquitectura de seguridad se pueden derivar de los controles descritos en el presente documento, de estándares comunes, etcétera.	2
Seguridad en las compras y el desarrollo	17.8	Arquitectura de seguridad: implementar principios de arquitectura de seguridad en un marco de especificación, diseño, desarrollo, realización y cambio en el sistema de información.	La organización se asegurará de que, al diseñar sistemas y servicios, se implemente una arquitectura de seguridad; la organización podrá llevarla a cabo, coordinarla o supervisarla, o controlar el trabajo de un proveedor externo.	Los principios de la arquitectura de seguridad pueden derivarse de los controles citados en las secciones de esta publicación y otros estándares aceptados.	
Seguridad en las compras y el desarrollo	17.9	Desarrollo seguro: garantizar que los desarrolladores de sistemas empleen herramientas y métodos de desarrollo seguros, como parte integral del proceso de desarrollo.	La organización integrará metodologías de desarrollo seguras y garantizará su asimilación dentro de los proveedores de sistemas y servicios que realizan procesos de desarrollo.	Un proveedor de <i>software</i> entregará la documentación de su implementación de los principios de desarrollo seguro, detallando las herramientas y métodos utilizados, los controles que se suministrarán para el nivel de protección del sistema.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad en las compras y el desarrollo	17.10	Operación segura: mantener un manual de administración del sistema de datos, incluido el mejor método de configuración de seguridad.	El manual de instalación y operación incluirá la información necesaria para una configuración segura.	Dentro de la documentación de configuración se incluyen un manual de instalación, el endurecimiento de infraestructura y aplicaciones, la implementación recomendada, etc. Para sistemas de nivel 3 y superiores, se ha de reafirmar previamente la configuración del sistema recomendada, como puertos abiertos, uso de la red, empleo de protocolos verificados, cambio de la contraseña predeterminada, etc., ya que la gestión del cambio de configuración es difícil de controlar y seguir manualmente. Los activos de nivel 3 y superiores incluirán un mecanismo de compensación para probar los cambios de la configuración automática (reglas dentro del sistema SIEM, un sistema de gestión de configuración central, monitoreo de control de continuidad).	2
Seguridad en las compras y el desarrollo	17.11	Seguridad en la cadena de suministro: exigir a los proveedores que cumplan con los requisitos de seguridad de la organización, con las regulaciones, estándares y direcciones.	La organización se asegurará de que sus proveedores cumplan con sus directivas, así como con las regulaciones de los estados donde esté activa.	Los requisitos reglamentarios de la organización se pueden definir como parte de un conjunto de requisitos de seguridad de datos estándar, designado para todos los proveedores de servicios externos.	1
Seguridad en las compras y el desarrollo	17.12	Realizar las pruebas y correcciones de la seguridad de los datos antes de integrarlas en sistemas y servicios. Dichas pruebas incluirán, al menos, pruebas de funcionalidad (cumplimiento de los requisitos) y exposición a la seguridad.	La organización se asegurará de que se realicen pruebas de seguridad antes de que un nuevo sistema o servicio esté operativo, y después de cada actualización.	En los casos de servicios prestados por proveedores externos, uno puede confiar en las pruebas realizadas por el proveedor o para el proveedor.	2
Seguridad en las compras y el desarrollo	17.13	Documentar las fallas de seguridad de los datos y el proceso de corrección de vulnerabilidades.	La documentación está destinada a garantizar la integridad y eficacia del proceso.	El control tiene el objetivo de verificar que los flujos se traten de acuerdo con la política de la organización. Este seguimiento localizará flujos graves de larga data, flujos no resueltos de toda la empresa, ayudará al gerente de ciberdefensa a diseñar planes de trabajo periódicos y se presentará periódicamente a la Dirección.	2
Seguridad en las compras y el desarrollo	17.14	Realizar un análisis de código estático como parte de la prueba de seguridad de datos de un nuevo sistema o servicio.	La organización probará los sistemas de nivel 3 con herramientas automáticas que reemplazarán las encuestas manuales (revisión de código).	El análisis de código se puede realizar mediante herramientas automáticas, probando varias configuraciones de código (código fuente, compilado, URL, etc.) e identificando así las lagunas. Realizar un análisis de código antes de comprar un sistema y tras cualquier cambio en su entorno.	3
Seguridad en las compras y el desarrollo	17.15	Validar la evaluación de riesgos y vulnerabilidades del sistema tras la finalización de su desarrollo.	La validación de la evaluación de riesgos tiene por objeto garantizar que la evaluación de riesgos realizada en la etapa de análisis coincida con la del sistema desarrollado.	Realizar una encuesta de riesgos después de la finalización del desarrollo y antes de la producción.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad en las compras y el desarrollo	17.16	Realizar las pruebas de seguridad de los datos por medio de una entidad externa, independiente.	La organización definirá el alcance del estudio que realizará el proveedor y su tipo (de sombrero blanco, gris o negro). La encuesta la realiza una entidad externa e independiente.	La realización de una prueba de penetración a nivel interno puede generar conflictos de intereses dentro de la organización. Recurrir a una entidad externa mejorará la defensa del producto. Al usar herramientas automáticas, un tercero puede validar que la herramienta está realizando pruebas de penetración que cubren el alcance del sistema. La misma parte hará que los resultados sean accesibles para la organización (redacción del informe final). Las pruebas se realizarán en un entorno lo más similar posible al de producción.	3
Seguridad en las compras y el desarrollo	17.17	Realizar pruebas de penetración al sistema o servicio.	El propósito de este control es examinar la efectividad de los controles y las protecciones en la práctica. Esto se logra mediante desafíos e intentos de penetrar en el sistema o la infraestructura.	Estas pruebas pueden llevarse a cabo mediante la aplicación de herramientas de ataque automáticas o por una persona. Pueden incluir intentos de obtener acceso no autorizado, introducir código malicioso en la base de datos e implementar ataques conocidos, como inyección de código de lenguaje de consulta estructurado (SQLI, por sus siglas en inglés), secuencia de comandos en sitios cruzados (XSS, por sus siglas en inglés), falsificación de petición en sitios cruzados (CSRF, por sus siglas en inglés), etcétera.	3
Seguridad en las compras y el desarrollo	17.18	Verificar que las pruebas del sistema incluyen verificación y que los controles de seguridad de datos definidos se implementan de acuerdo con el diseño original.	Mantener una lista de etiquetado de los requisitos de defensa definidos para el sistema y verificar que todos los requisitos se cumplan internamente y sean cumplidos por el proveedor.	En la fase de entrega, verificar que todos los requisitos definidos en el diseño de bajo nivel se implementen realmente. Documentar la naturaleza y los resultados de la prueba.	3
Seguridad en las compras y el desarrollo	17.19	Requerir al proveedor que realice un análisis de código dinámico de un nuevo sistema o servicio.	Requerir al proveedor que realice un análisis de código dinámico de un nuevo sistema o servicio.	El análisis de código dinámico se realizará mediante las herramientas existentes, disponibles en el mercado, o mediante <i>fuzzing</i> , así como mediante una herramienta de escaneo automático durante la ejecución del sistema. La organización inspeccionará periódicamente muestras de informes o hallazgos para verificar la corrección de los flujos en consecuencia.	3
Seguridad en las compras y el desarrollo	17.20	Implementar un mecanismo de resistencia a la manipulación dentro del sistema.	La organización verificará que los desarrolladores implementaron dentro del sistema una capacidad de resistencia a la manipulación.	Los mecanismos de resistencia a la manipulación se pueden implementar mediante firmas digitales, cifrado, creación de copias, etcétera.	4
Seguridad en las compras y el desarrollo	17.21	Implementar métodos para evitar la intrusión de falsos componentes del sistema.	Dichos mecanismos están destinados a evitar la intrusión de <i>software</i> falso de componentes de <i>hardware</i> en la organización, intencionalmente o engañando a un elemento de la cadena de suministro.	Dichos mecanismos pueden ser la verificación de componentes de <i>software</i> , inspección y verificación de archivos de <i>software</i> entrantes, etc. Tales mecanismos pueden consistir en varios niveles de seguridad, desde la compartimentación del acceso físico a las computadoras, la contraseña de BIOS, el cifrado de disco, limitar al sistema operativo a arrancar solo desde el disco duro, las reglas dentro el sistema SIEM, etcétera.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Seguridad en las compras y el desarrollo	17.22	Constatar que los sistemas adquiridos o desarrollados implementen mecanismos de verificación de entrada.	Los sistemas desarrollados implementarán mecanismos de filtrado de entradas inesperadas, como longitudes o formatos inesperados. Estos pueden dar lugar a resultados imprevistos y tener un impacto negativo en la inmunidad, integridad o disponibilidad del sistema, de acuerdo con su nivel de valor.	Se puede hacer para sistemas de nivel 2 con una declaración del proveedor con respecto a la verificación de entrada y el uso de bibliotecas de <i>software</i> estándar que filtran las entradas de acuerdo con sus características esperadas. Para los sistemas de nivel 3 se requiere una solución tecnológica (como WAF) a nivel de red, o un mecanismo similar a nivel de aplicación. Al delimitar las pruebas de penetración, verificar que las pruebas de entrada estén completamente cubiertas (OWASP puede ser un buen punto de referencia) y que cumplan la política de la organización.	2
Seguridad en las compras y el desarrollo	17.23	Verificar que los sistemas adquiridos o desarrollados implementan mecanismos de gestión de errores.	El sistema desarrollado implementará mecanismos para detectar errores y presentar errores del sistema sin exponer datos confidenciales. En cualquier caso, se ha de verificar que el mecanismo de error no exponga datos confidenciales del sistema, como una tabla o nombres de usuario, idioma y versiones de <i>software</i> , etcétera.	Esto puede hacerse implementando un mecanismo de gestión de errores que presente errores estándar.	2
Seguridad en las compras y el desarrollo	17.24	Comprobar que los sistemas adquiridos o desarrollados implementen mecanismos de verificación de salida.	Los sistemas desarrollados implementarán mecanismos para filtrar salidas inesperadas, que pueden resultar de un ataque al sistema, y exponer datos confidenciales.	Se puede implementar mediante el uso de bibliotecas de <i>software</i> estándar, que filtran la salida de acuerdo con sus formatos esperados. O mediante sistemas de identificación de anomalías, basados en el comportamiento del sistema, el usuario o el sistema operativo, etcétera.	3
Seguridad en las compras y el desarrollo	17.25	Verificar que los sistemas desarrollados o comprados implementen mecanismos de fiabilidad de la sesión.	Los sistemas desarrollados implementarán mecanismos destinados a prevenir el secuestro de sesiones, los ataques MITM, etcétera.	Eso puede hacerse mediante una gestión de sesión adecuada, eliminando conexiones al final de las actividades de los usuarios, aleatoriedad de <i>tokens</i> , etcétera.	2
18. Protección física y ambiental La protección física y ambiental es una importante capa de ciberdefensa de la organización, destinada a bloquear la penetración física del entorno cibernético. Entre las actividades preventivas se incluyen las siguientes: el acceso físico a las instalaciones de la organización permitido solo a personas autorizadas,				la protección física de las ciberinfraestructuras, como electricidad o aire acondicionado, daños por agua, etc. Además, una protección física eficaz evita que se produzcan daños maliciosos en el equipo, e informa a las autoridades si se producen tales intentos. Este apartado cubre solo aspectos de la protección física de los componentes cibernéticos.	
Protección física y ambiental	18.1	Definir, implementar y controlar y actualizar periódicamente la política de protección física y ambiental.	Este control tiene como objetivo definir la política de la organización con respecto al cierre de puertas al final del día, cámaras de seguridad, visitantes y entrada de empleados externos en las instalaciones y áreas sensibles de la compañía, la protección adecuada del servidor y las salas de control, etcétera.		2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Protección física y ambiental	18.2	Definir e implementar procedimientos para integrar una política de protección física y ambiental y controles relevantes.	Preparar los procedimientos de control de acceso físico a las instalaciones, que incluyen: 1. procedimiento de acceso físico; 2. procedimiento para los invitados; 3. procedimiento de acceso a las computadoras o la sala de comunicación.		2
Protección física y ambiental	18.3	Definir y mantener una lista de todas las personas autorizadas a ingresar a las instalaciones donde se encuentra el activo. Emitir medios de identificación para las personas autorizadas, examinar la lista periódicamente y borrar de ella a las personas cuyo acceso ya no sea necesario.	Mantener y actualizar la lista de personas autorizadas.	Emitir tarjetas de identificación para los empleados y visitantes.	2
Protección física y ambiental	18.4	Realizar controles de acceso físico en los puntos de entrada y salida de las instalaciones.	Realizar controles de acceso físico en todas las instalaciones de la organización.	Pueden utilizarse un lector de tarjetas de puerta, cerraduras, lectores biométricos, guardias de seguridad, códigos de combinación, etcétera.	2
Protección física y ambiental	18.5	Mantener registros de los accesos físicos a la instalación.	Conservar y almacenar registros de todas las entradas y salidas de todos los visitantes.	Registrar todas las entradas y salidas manualmente, por un guardia, o en una base de datos.	3
Protección física y ambiental	18.6	Controlar, registrar, asegurar y aplicar el control de acceso físico a las áreas de comunicación e informática (salas de servidores y gabinetes de comunicación). 	Limitar el acceso físico de elementos no autorizados a las áreas de comunicación e informática (salas de servidores y gabinetes de comunicación). La organización definirá una lista de personas autorizadas y hará cumplir el acceso de acuerdo con sus procedimientos.	1. Definir permisos de acceso físico y lógico para personas autorizadas. 2. Asentar mediante un registro o libros de registro todos los accesos a las salas de computadoras. En los casos en que no sea posible registrar el acceso a gabinetes de comunicación y salas de servidores, conviene considerar una protección física mediante cerraduras, evitando el acceso a personas no autorizadas.	2
Protección física y ambiental	18.7	Tener control físico sobre los dispositivos de salida de información del sistema a fin de evitar la salida de elementos no autorizados (impresoras, máquinas de fax, etcétera).	Ese control asegura que los productos del sistema lleguen solo a sus propietarios originales. Esto es especialmente importante para los productos que contienen información personal, como datos médicos o de seguros, detalles de empleados privados, etc. En tales casos, hay que asegurarse de que la información llegue solo a las personas que estén autorizadas a verla.	Eso puede lograrse mediante varias vías: 1. mediante el sistema de control de impresión, que requiera un código o una tarjeta de empleado; 2. colocando las impresoras en salas cerradas con acceso limitado; 3. usando los servicios de fax2mail o, al menos, asegurándose de que el receptor adecuado esté cerca de una máquina de fax antes de imprimir un mensaje; 4. finalmente, asegurándose de que todos los dispositivos de salida ubicados en lugares públicos estén "limpios", de modo que no llegue información privada a personas no autorizadas.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Protección física y ambiental	18.8	Supervisar el acceso físico a la instalación donde se encuentra el activo, para detectar incidentes de seguridad y responder a ellos, y para examinar periódicamente los registros de actividad.	Este control está destinado a bloquear el acceso de elementos no autorizados a áreas sensibles. El acceso podría permitirles actuar de manera maliciosa, como instalar dispositivos de escucha, conectarse a la red, robar <i>hardware</i> , etcétera. Un control adecuado significa que solo las personas autorizadas por la organización tienen acceso a esas áreas.	Monitorear todas las entradas físicas a áreas sensibles, como salas de servidores, gabinetes de comunicación, etc., mediante el registro de todas las entradas y salidas.	3
Protección física y ambiental	18.9	Monitorear y activar la alarma en cualquier acceso físico a un activo fuera de las horas y días normales de trabajo.	Usar tecnologías de monitoreo y alarma para detectar intentos de acceso no autorizados fuera de las horas y días normales de trabajo.	Utilizar sistemas de alarma o recurrir a una compañía de seguridad para monitorear y alertar de accesos no autorizados a la instalación.	3
Protección física y ambiental	18.10	Definir y mantener una matriz de respuesta a los accesos no autorizados a la instalación.		Puede hacerse mediante un oficial de seguridad organizacional, una compañía de seguridad, etcétera.	3
Protección física y ambiental	18.11	Instalar un sistema de circuito cerrado de televisión para monitorear cualquier acceso físico al activo. Almacenar las grabaciones por un período predefinido.	Instalar un sistema de circuito cerrado de televisión (CCT) para monitorear cualquier acceso físico al activo. Una persona de seguridad debe monitorear el CCT continuamente.		4
Protección física y ambiental	18.12	Registrar los datos de todos los visitantes de las instalaciones.	Registrar todos los visitantes a las instalaciones de la organización.	Mantener un registro de visitantes, en un sistema determinado, que indique todos los visitantes de una instalación específica.	2
Protección física y ambiental	18.13	Evitar daños de los equipos y cables eléctricos del sistema.	Hay que ser puntilloso al instalar y etiquetar todos los cables eléctricos en las salas de servidores y gabinetes de comunicación.	Se deben etiquetar todas las terminaciones de cable para que los empleados puedan detectar fácilmente su vinculación con servidores o sistemas, y así evitar desconexiones indebidas.	2
Protección física y ambiental	18.14	Garantizar la posibilidad de suministrar electricidad de forma segura durante períodos cortos, a fin de permitir un apagado ordenado de un sistema o su transferencia a una fuente de energía alternativa.		Instalar una matriz de sistema de alimentación ininterrumpida a fin de asegurar un apagado ordenado de los sistemas, en caso de falta de energía.	2


Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Protección física y ambiental	18.15	Garantizar la posibilidad de suministrar electricidad de forma segura durante períodos más largos, a fin de lograr una continuidad de sus actividades.		Un generador eléctrico es una buena opción.	3
Protección física y ambiental	18.16	Implementar y mantener un sistema automático de iluminación de emergencia, que indique las salidas de emergencia y las rutas de evacuación.			1
Protección física y ambiental	18.17	Implementar y mantener sistemas de extinción de incendios, específicamente para sistemas de datos, suministrados por una fuente de energía autónoma.			1
Protección física y ambiental	18.18	Mantener y controlar un nivel aceptable de temperatura y humedad en la instalación del activo.		Especialmente en salas de servidores.	2
Protección física y ambiental	18.19	Proteger el activo de fugas de agua, ya sea por un cierre maestro o por válvulas aislantes.			2
Protección física y ambiental	18.20	Verificar y monitorear los elementos del sistema que ingresan y salen de la instalación.		Puede usarse, por ejemplo, un procedimiento de eliminación de elementos de software y hardware de la organización, especialmente aquellos que pueden almacenar datos confidenciales. El monitoreo y control de la información que sale de la organización se puede realizar haciendo un seguimiento del hardware que salga (computadoras portátiles entregadas a proveedores, memorias USB, etcétera). El registro y monitoreo periódicos incluirán información sobre quién recibió el hardware, por cuánto tiempo, con qué propósito y la fecha estimada de devolución.	2
Protección física y ambiental	18.21	Implementar controles de seguridad en centros de trabajo alternativos (como los de recuperación ante desastres), evaluando su efectividad.		El nivel de seguridad física en un sitio alternativo, como el centro de recuperación ante desastres, será aceptable y adecuado para los datos almacenados allí. La implementación del control se contemplará en el contrato con la dirección del centro alternativo y se revisará periódicamente.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Protección física y ambiental	18.22	Colocar los elementos del sistema donde el potencial de impacto del daño y la probabilidad de acceso no autorizado sean mínimos.	Si es posible, coloque los sistemas (salas de servidores y de comunicación) en la ubicación mejor protegida, en el centro del edificio, lejos de paredes externas y fuentes de agua (también de tuberías).		3
19. Recursos humanos Los empleados de la organización son una capa de protección organizacional importante. Por un lado, pueden detectar eventos sospechosos y advertir de ellos en tiempo real y, por otro, pueden constituir vulnerabilidades, que pueden conducir a incidentes cibernéticos, ya sea por error o por engaño de los atacantes.				Por lo tanto, al reclutar, la organización debe hacer una doble verificación de los empleados potenciales en relación con la sensibilidad de sus funciones, informar a sus empleados sobre las amenazas cibernéticas, las posibles defensas y reportes al respecto. La organización definirá las reglas de conducta de los empleados en el ciberespacio externo (redes sociales, exposición de información interna en el ciberespacio, etc.), lo que puede dañar su nivel de protección. Se deben cancelar todas las autorizaciones de seguridad de los empleados que abandonan la organización.	
Recursos humanos y sensibilización de los empleados	19.1	Evaluar los niveles de sensibilidad de varias funciones en la organización y definir criterios de clasificación adecuados en la contratación de empleados.	Definir requisitos mínimos en el reclutamiento y requisitos más altos para las funciones sensibles.	Los requisitos mínimos pueden incluir, por ejemplo, pruebas de antecedentes y verificación de datos, una prueba de confidencialidad o una prueba de detector de mentiras. Se recomienda diseñar una matriz que defina varias pruebas para funciones específicas. Por ejemplo, la inexistencia de antecedentes penales, la realización de pruebas de clasificación de seguridad cuando sea necesario, las pruebas de confidencialidad y de detección de mentiras, la verificación de los datos presentados por aspirantes a empleados, las credenciales emitidas por antiguos empleadores, los empleados de soporte técnico deben aprobar una prueba de confidencialidad computarizada, los que tienen autorizaciones superiores (Admin) deben someterse a una prueba externa, etcétera.	2
Recursos humanos y sensibilización de los empleados	19.2	Realizar pruebas de antecedentes en la contratación y promoción a funciones de mayor sensibilidad.	Realizar pruebas de antecedentes a los candidatos o empleados antes de autorizar el acceso a los sistemas de datos.	Las pruebas de antecedentes pueden incluir la verificación de datos de fondo, una consulta a antiguos empleadores, pruebas de confidencialidad o de detector de mentiras, verificación de los antecedentes económicos, autorización de seguridad, etcétera.	3
Recursos humanos y sensibilización de los empleados	19.3	Hacer que los empleados firmen un compromiso con los requisitos cibernéticos de la organización.	El empleado firmará documentos, dando fe de su conocimiento del hecho de que los sistemas de la organización contienen datos secretos que no deben divulgarse sin una autorización específica de acuerdo con las reglas de la organización.	Puede implementarse mediante la inscripción de todos los empleados en acuerdos de confidencialidad, guardados en sus archivos; mediante un sistema de gestión de identidades (IdM, por sus siglas en inglés) que controla la información sobre los usuarios en las computadoras y permite la ratificación periódica de cada empleado.	2
Recursos humanos y sensibilización de los empleados	19.4	Hacer firmar a todos los empleados acuerdos de confidencialidad más allá de su empleo.	Cada empleado firmará un acuerdo de confidencialidad y declarará que no posee ningún documento u otro dispositivo de almacenamiento de datos que contenga información de la organización.	Puede implementarse haciendo que todos los empleados firmen acuerdos de confidencialidad y realizando pruebas en una muestra de empleados. Dichas revisiones se pueden hacer monitoreando las actividades de los usuarios en la red para localizar anomalías (tratando de acceder a archivos no autorizados, copiar grandes cantidades de datos, etcétera).	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Recursos humanos y sensibilización de los empleados	19.5	Definir los requisitos de seguridad de proveedores y terceros.	La organización definirá los requisitos de seguridad de datos como parte de su política de relaciones con los proveedores; por ejemplo, limitaciones en el intercambio de datos, acuerdos de confidencialidad, instrucciones en las normas de seguridad de la organización, instrucciones de los proveedores, etcétera.	Puede implementarse mediante un folleto de reglas y mediante la adhesión de los proveedores al comienzo de su empleo. Realizar una actualización periódica.	2
Recursos humanos y sensibilización de los empleados	19.6	Definir reglas sobre el uso de los sistemas de datos en el trabajo. Estas reglas definen las responsabilidades y el uso adecuado de los sistemas de datos, haciendo hincapié en los sistemas sensibles.	La organización definirá reglas de conducta en relación con los sistemas de datos, y las difundirá entre sus empleados.	Puede implementarse mediante procedimientos que definan la política de descarga, la navegación por sitios web de intercambio de datos, la utilización de direcciones privadas o de la empresa, etc. También mediante el registro de la conducta de los usuarios, cursos para nuevos empleados y herramientas tales como las aplicaciones de control y filtrado de URL.	1
Recursos humanos y sensibilización de los empleados	19.7	Definir reglas y limitaciones en el uso de las redes sociales.	Definir reglas y limitaciones en el uso de las redes sociales: limitaciones en la publicación de información sobre la organización en las redes sociales y sitios públicos, representación de la organización en las redes sociales, y acceso a redes sociales desde los sistemas de la organización.	La conducta del usuario en las redes sociales puede definir pautas sobre la representación de la organización en estas redes, la divulgación de información y las precauciones al acceder a las redes sociales desde los sistemas de la organización.	2
Recursos humanos y sensibilización de los empleados	19.8	Definir e implementar un procedimiento de sanción cuando se incumplan las reglas de seguridad de los datos.	La organización definirá procedimientos disciplinarios para hacer frente a las violaciones de seguridad por parte de empleados o contratistas, y hará un registro de las medidas disciplinarias tomadas.	Por ejemplo, se convocará a un empleado que violó instrucciones claras, junto con su superior, para aclarar asuntos con elementos de seguridad. Las consecuencias podrían ir desde medidas disciplinarias hasta el despido. Prestar atención a los casos que requieren la participación de asesores jurídicos o autoridades.	3
Recursos humanos y sensibilización de los empleados	19.9	Examinar y actualizar las autorizaciones de los empleados al cambiar las funciones.	Definir los procedimientos de movilidad de los trabajadores, incluidas la actualización de las autorizaciones en consonancia con las nuevas funciones (eliminar autorizaciones innecesarias y definir otras nuevas según sea necesario para la nueva función).	La actualización de las autorizaciones puede realizarse manualmente, notificando los elementos de autorización en la organización, o automáticamente, cuando las interfaces de autorización están integradas en los sistemas de recursos humanos (un sistema de gestión de identificación computarizado). En cuanto a la movilidad de los trabajadores, es preferible eliminar todas las autorizaciones existentes y definir un nuevo conjunto.	1

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Recursos humanos y sensibilización de los empleados	19.10	Eliminar todas las autorizaciones y bloquear las cuentas de usuario al finalizar el empleo.	Definir un proceso de actualización para aplicar cuando finalice un contrato, incluida la eliminación de autorizaciones y cuentas de usuario.	La actualización de las autorizaciones puede realizarse manualmente, notificando los elementos de autorización en la organización, o automáticamente, cuando las interfaces de autorización están integradas en los sistemas de recursos humanos (un sistema de gestión de identificación computarizado). Cuando finalice el contrato, se deben eliminar todas las autorizaciones existentes y posteriormente las cuentas de usuario.	2
20. Capacitación e instrucción Una política de ciberdefensa es importante para minimizar los ataques cibernéticos en la organización. Muchos ataques actuales se realizan mediante ingeniería social, por ejemplo, ataques de penetración o <i>ransomware</i> , suplantación de identidad (<i>phishing</i>) por correo electrónico para realizar actividades autorizadas (transferencias de dinero), etc.				Los empleados de la organización son herramientas importantes en manos de un atacante, por lo tanto, la realización de seminarios y actividades de concientización son herramientas organizativas importantes para hacer frente a tales riesgos. Se requiere que la organización instruya periódicamente a los empleados en todos los niveles en torno a la ciberdefensa (seminarios generales para crear conciencia, así como seminarios específicos para funcionarios en puestos sensibles) y que los empleados pongan esos conocimientos en práctica de manera regular.	
Capacitación e instrucción	20.1	Desarrollar, registrar e implementar una política de concientización sobre la seguridad de datos.	La organización definirá la política de concientización en materia de seguridad de datos, que incluirá actualizaciones periódicas, el tipo de personal a ser instruido en varios temas y los medios de seguimiento.	Se puede implementar elaborando una directiva sobre seminarios que trate cuestiones de contenido, desempeño y responsabilidades de seguimiento. Esta política definirá varios públicos objetivo (nuevos empleados, personal clave, empleados cuyo empleo ha terminado, proveedores, agentes externos, etc.), quiénes están a cargo de los seminarios, el control y la supervisión (firma de una declaración, un examen, etc.), los logros requeridos, la frecuencia de la instrucción y las materias esenciales.	2
Capacitación e instrucción	20.2	Realizar una capacitación básica para los empleados en materia de seguridad de datos.	La organización llevará a cabo una capacitación básica, relacionada con el uso adecuado de la información, las reglas de seguridad de los datos, las amenazas internas y externas, incluidas las señales de amenaza.	Puede implementarse mediante cursos internos o externos, adecuados para las políticas y necesidades de la organización.	2
Capacitación e instrucción	20.3	Realizar una capacitación específica en materia de seguridad de los datos para los empleados que acceden a datos confidenciales.	La organización llevará a cabo seminarios iniciales y periódicos que incluyan los siguientes temas, según la función de los empleados: la aplicación de controles de seguridad del entorno, la aplicación de controles de seguridad física, la práctica de comportamientos durante incidentes relacionados con los datos y la ciberseguridad, comportamientos sospechosos de los sistemas, identificación de código malicioso.	Puede llevarse a cabo mediante cursos internos o externos, adecuados para las definiciones de trabajo y la política y las necesidades de la organización.	3




Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Capacitación e instrucción	20.4	Sensibilizar a los empleados sobre la ingeniería social.	Verificar que los funcionarios sean conscientes de los intentos de engaño y suplantación de posibles atacantes.	Puede hacerse internamente o por una empresa externa. Tales intentos pueden incluir solicitudes “ilegítimas” del personal de soporte, solicitudes de información en nombre de otra persona, intentos de actuar sin verificación del usuario, solicitudes en las redes sociales o por correo electrónico, etcétera.	4
DETECTAR					
21. Registro y monitoreo		<p>La Metodología de Ciberdefensa asume que, independientemente de todas las defensas, algunos atacantes lograrán penetrar en la organización. Como parte de la estrategia para hacer frente a un incidente cibernético, la organización debe ser capaz de identificar dichos eventos y hacerles frente.</p> <p>Se requiere que la organización registre actividades relevantes en sus sistemas, que pueden ser indicativas de incidentes cibernéticos. Además, la organización debe monitorear esta documentación de una manera que le permita detectar los incidentes lo antes posible, para reaccionar de manera rápida y minimizar los daños. Los controles están destinados a definir eventos y crear documentación eficaz e infraestructuras de monitoreo.</p>			
Registro y monitoreo	21.1	Definir, implementar y revisar periódicamente la política de registro y monitoreo.		Registrar y monitorear la política organizacional y las reglas de apoyo, como un centro de monitoreo de seguridad de los datos, reglas de registro de eventos, etcétera.	2
					
Registro y monitoreo	21.2	Determinar los eventos que el sistema registrará y para qué períodos lo hará. Estos registros de control deben ser la base de los informes sobre incidentes de seguridad. Definir qué sistemas deben auditarse (servidores, componentes de comunicación, aplicaciones, bases de datos, etcétera).	La organización determinará qué eventos que se produzcan en sus sistemas se registrarán en sus sistemas de seguridad de datos, así como las reglas de monitoreo utilizadas en tales eventos. Definirá un período mínimo de tiempo para mantener estos registros, cumpliendo con las regulaciones estatales.	Se puede implementar mediante la caracterización posterior a los hechos de eventos comunes.	2
Registro y monitoreo	21.3	Examinar periódicamente las definiciones de eventos registrados y la efectividad del sistema de registro.	Examinar periódicamente las instalaciones de trabajo en relación con los cambios en los sistemas de la organización, para asegurar la integridad del registro. Además, examinar periódicamente la normalidad de los eventos registrados y su coherencia con las definiciones y necesidades de la organización.	Un examen periódico de los mecanismos de registro y su coherencia con los sistemas de la organización. Para un sistema de control central, se pueden usar mecanismos automáticos para verificar las actividades y la normalidad del sistema de registro de eventos.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Registro y monitoreo	21.4	Emplear un mecanismo que produzca registros de control de eventos. Al menos registre eventos de los sistemas que contengan datos confidenciales de los clientes, de sistemas críticos para el funcionamiento de la organización y de sistemas centrales (servidores, elementos de comunicación, aplicaciones, bases de datos, etcétera).	La organización se asegurará de que la infraestructura y los sistemas de funcionamiento empleen registros, y que estos se almacenen por el período de tiempo definido por la organización. Los registros de control contendrán información como el tipo de evento, el momento en que se dio, la fuente o el nombre de usuario. En cualquier caso, la organización monitoreará los sistemas sensibles, partes de su infraestructura crítica y aquellos que administran procesos centrales.	Por lo general, los sistemas de infraestructura contienen mecanismos de registro. En el caso de las aplicaciones, verificar las opciones de registro existentes. Es posible utilizar mecanismos de registro central, vinculados a los sistemas de la organización, y registrar eventos en una base de datos central.	1
Registro y monitoreo	21.5	Definir los datos adicionales necesarios para el registro de sus sistemas, incluido un identificador único de cada actividad, comando y consulta.	Un registro básico del sistema no necesariamente registra todos los datos requeridos para investigar un evento. Por lo tanto, la organización debe definir los eventos o datos necesarios que se han de registrar. Los sistemas sensibles requieren un registro de actividades profundo y detallado para crear alertas de calidad.	Determinar campos para ser monitoreados en varios sistemas. Ocasionalmente es necesario definir el monitoreo en las etapas de desarrollo, o expandir las bases de datos de monitoreo para recopilar dicha información detallada.	3
Registro y monitoreo	21.6	Implementar un sistema central de monitoreo y alerta.	Definir e implementar un sistema central de monitoreo y alerta para recopilar datos de varios sistemas y centralizar el análisis, alerta y manejo de eventos sospechosos.	Por ejemplo, un sistema SIEM que combina la gestión de la información de seguridad y la gestión de incidentes de seguridad, y proporciona un análisis en tiempo real de las alertas de seguridad generadas por el <i>hardware</i> y las aplicaciones de la red.	3
Registro y monitoreo	21.7	Incluir en el mecanismo de registro, al menos, lo siguiente: datos sobre el evento, una marca temporal, el origen y destino de la actividad, el identificador de usuario, el identificador de proceso, el éxito o fracaso y el nombre de archivo.	Requerir al proveedor que realice un análisis de código dinámico de un nuevo sistema o servicio.	Para las organizaciones de nivel 2 y superiores, verificar que el registro de actividad registre todos los datos requeridos. En la mayoría de los casos, es posible utilizar mecanismos de registro ya existentes en los sistemas de infraestructura. En los sistemas aplicables, verificar la existencia de un registro que funcione.	1

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Registro y monitoreo	21.8	Asignar suficiente espacio de almacenamiento de registro.	La organización asignará suficiente espacio de almacenamiento para sus necesidades de registro y monitoreo a largo plazo.	Planificar previamente los requisitos de almacenamiento de datos. Realizar la planificación periódica de la capacidad.	2
Registro y monitoreo	21.9	Crear un mecanismo de alerta para casos de fallos de registro.		La organización controlará su sistema de monitoreo de la seguridad de los datos con el fin de recibir alertas cuando no se registren eventos por un determinado período de tiempo desde un sistema de información que normalmente se monitorea. Tales casos se pueden definir como reglas en la mayoría de los sistemas de registro y monitoreo (SIEM, Log Management).	2
Registro y monitoreo	21.10	Definir actividades sensibles que la organización desea monitorear.	Este control tiene la intención de garantizar que la organización defina escenarios que deban ser monitoreados, y puede obtener dicha información.	Se puede hacer preguntando a las personas de la organización sobre los procesos de trabajo y las actividades no autorizadas. Los siguientes eventos y escenarios que se deben monitorear se pueden obtener del personal de TI: actividades irregulares en la red, como el acceso a archivos confidenciales, múltiples intentos fallidos de identificación, copia de múltiples archivos a espacios de almacenamiento local, comportamiento ilegítimo de un proveedor o empleado externo, etc. Para monitorear tales eventos, se puede usar un sistema SIEM así como informes locales, productos de varios sistemas, cámaras de seguridad, preguntas a los empleados, etcétera.	2
Registro y monitoreo	21.11	Revisar y analizar periódicamente los registros de control. Informar de los hallazgos a empleados específicos.	La organización extraerá informes de seguridad de los datos y de tendencias, e informará de ello a la Dirección o a un funcionario específico.	Se pueden extraer dichos informes de cualquier sistema de monitoreo de seguridad de datos como el SIEM.	2
Registro y monitoreo	21.12	Utilizar mecanismos automatizados para identificar presuntos incidentes cibernéticos fuera de los registros de monitoreo.	Para detectar eventos sospechosos, es necesario generar alertas e indicaciones a partir del monitoreo de los datos recopilados de los sistemas de la organización. Los eventos que la organización haya definido como sospechosos deben manejarse de acuerdo con el perfil de las amenazas de la organización.	Se puede implementar utilizando informes, consultas y reglas aplicables a la base de datos de monitoreo, o mediante un sistema de monitoreo dedicado como el SIEM.	2
Registro y monitoreo	21.13	Implementar un sistema de monitoreo que recopile registros de control de varias fuentes de datos para obtener una imagen completa de la organización.	La organización implementará un “motor de correlación”, destinado a integrar datos de diferentes fuentes de información (distintos sistemas), permitiendo identificar eventos laterales y ataques avanzados en los sistemas empresariales.	Por ejemplo, combinar datos del sistema y de los sistemas de comunicación, de infraestructura y de aplicación, de varios sistemas de control de acceso físico, examinar vulnerabilidades e integrar entradas de fuentes de inteligencia cibernética.	4

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Registro y monitoreo	21.14	Proteger los registros de control frente a un acceso, un cambio o una eliminación no autorizados.	La organización asegurará el área de almacenamiento y endurecerá la matriz de monitoreo para evitar la actualización de los registros.	Se puede implementar limitando el acceso al almacenamiento de registros de monitoreo y a los servidores.	2
Registro y monitoreo	21.15	Respalidar los registros de control periódicamente y almacenar los archivos de respaldo lejos del sistema de monitoreo.		La organización definirá métodos de respaldo continuo de las definiciones de la matriz de monitoreo (reglas y configuraciones de monitoreo de respaldo), así como de los registros recopilados.	3
Registro y monitoreo	21.16	Utilizar mecanismos criptográficos para proteger la integridad de los registros y las herramientas de control.	Los archivos de registro se sellarán mediante sellado digital y <i>hashing</i> para verificar que no se modifiquen.	La mayoría de los sistemas SIEM admiten estas funciones. Se debe verificar su correcto funcionamiento.	3
Registro y monitoreo	21.17	Asegurarse de que sea posible recuperar o buscar registros almacenados que sean lo más antiguos posible.	Periódicamente, la organización se asegurará de que se puedan recuperar los registros de control antiguos (lo más antiguos posible).	Por ejemplo, es posible extraer un informe del establecimiento del sistema para verificar que tales eventos existen en el sistema de monitoreo.	4
Registro y monitoreo	21.18	Implementar un mecanismo de sesión de usuario en los sistemas de información.	Definir el mecanismo de registro y las reglas de uso de dicho mecanismo, incluidos los casos en que sea necesario guardar registros, las reglas de privacidad y la autorización de acceso al sistema de registro.	Se puede implementar utilizando el sistema de sesión de un usuario a través de la estación de trabajo, la instalación en servidores de aplicaciones o terminales.	4
Registro y monitoreo	21.19	Implementar mecanismos de identificación y alerta de intentos de ataque en tiempo real.	Estos mecanismos de alerta detectarán y alertarán en caso de un intento de ataque.	Se pueden implementar mediante la definición de reglas SIEM, alertando de ataques e incidentes de seguridad de datos. Y mediante el establecimiento de un centro de operaciones de seguridad.	4
Registro y monitoreo	21.20	Monitorear la comunicación entrante y saliente para identificar actividades irregulares o no autorizadas.		Se puede implementar analizando el tráfico del cortafuegos de la organización y el sistema de detección de intrusiones, y correlacionando frente a las fuentes externas para identificar la comunicación a servidores sospechosos.	3
Registro y monitoreo	21.21	Implementar dispositivos de monitoreo específicos de actividades de usuarios de niveles de alto riesgo (como usuarios con autorizaciones de alta seguridad).	La organización caracterizará las funciones organizacionales sensibles, y se asegurará de que estén cubiertas por reglas de monitoreo específicas en relación con actividades sensibles.	Es posible comparar con un grupo de usuarios confidenciales dentro del Active Directory o cargar una lista de dichos usuarios en la matriz de SIEM. Es posible alertar después de definir cualquier nuevo usuario Admin dentro del controlador de dominio.	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
22. Evaluación de los controles de seguridad			Las evaluaciones de los controles de seguridad están destinadas a analizar la implementación real de los controles, de acuerdo con esta Metodología de Ciberdefensa, y la efectividad de la defensa. Es deseable que la evaluación sea realizada por una entidad independiente o externa.		
Evaluación del control de la seguridad	22.1	Elaborar e implementar una política de gestión de vulnerabilidades de la seguridad de los datos, revisarla y actualizarla periódicamente.	La organización definirá una política de gestión de vulnerabilidades, que incluirá la identificación y evaluación de vulnerabilidades, su corrección, las responsabilidades y el seguimiento continuo.	La efectividad puede determinarse mediante pruebas de penetración y vulnerabilidad, equipos rojos, etc. Los controles deben evaluar periódicamente que los sistemas de ciberdefensa estén adecuadamente definidos y actualizados en relación con los cambios en la organización y las posibles amenazas cibernéticas.	2
	22.2	Definir un procedimiento de gestión de vulnerabilidades de la seguridad de los datos, que incluya la evaluación y corrección de vulnerabilidades.	La organización preparará una cartera de procedimientos y planes para implementar y operar una matriz de gestión de vulnerabilidad de seguridad de datos, haciendo hincapié en los sistemas de identificación, herramientas y empleo de peritos, subproveedores y empleo de empleados para encargarse de los hallazgos. Además, la matriz de gestión de vulnerabilidades de la seguridad de los datos incluirá una o más de las siguientes pruebas: evaluación del control de la seguridad, prueba de usuario malicioso, evaluación de amenazas internas y otras que determine la organización.	El programa de evaluación del control de la seguridad incluirá varios procedimientos y procesos, destinados a detectar vulnerabilidades, un seguimiento de los procesos y mecanismos de corrección, interfaces de proceso paralelos (gestión de actualizaciones de seguridad de datos, gestión de configuración del sistema de seguridad de datos, desarrollo seguro, etcétera). La organización se integrará en el programa de gestión de la vulnerabilidad de la seguridad de los datos, la prueba de penetración que simula usuarios internos y externos, los sistemas de evaluación de la configuración, etcétera.	2
	22.3	Evaluar periódicamente la penetrabilidad del sistema.	La organización evaluará periódicamente la penetrabilidad de las infraestructuras y aplicaciones (internas y externas, si son administradas por la organización).	Las organizaciones financieras, por ejemplo, realizan evaluaciones anuales de penetrabilidad, incluso plurianuales, de todos sus sistemas, pudiendo así realizar un seguimiento continuo.	3
	22.4	Contratar a una empresa independiente para evaluar la penetrabilidad.	La organización empleará expertos externos en seguridad de datos para realizar estas evaluaciones.	Ocasionalmente estas evaluaciones pueden realizarlas un equipo interno, no sujeto al sector de TI sino a un sector que no se encargue de corregir las fallas.	4

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Evaluación del control de la seguridad	22.5	Emplear un equipo independiente para realizar evaluaciones de penetración y ejercicios del equipo rojo, a fin de simular intentos de ataque contra sus activos.	La organización empleará un equipo externo de seguridad de datos para simular intentos de ataque con el fin de probar sus controles y capacidades de respuesta.	Este control puede probar las capacidades de respuesta de los equipos de monitoreo y las capacidades de los equipos de infraestructura y seguridad de datos para bloquear tales intentos en tiempo real.	4
Evaluación del control de la seguridad	22.6	Realizar evaluaciones continuas de la vulnerabilidad, de acuerdo con el proceso de gestión de vulnerabilidades de la organización, mediante una herramienta específica para todos los sistemas de datos (internos y externos).		Se puede implementar instalando una herramienta de evaluación del control de la seguridad y evaluando cada pocas semanas o meses (se pueden determinar tiempos específicos para entornos diversos).	2
					
Evaluación del control de la seguridad	22.7	Verificar que la herramienta de evaluación del control de la seguridad esté siempre actualizada y que contenga todas las vulnerabilidades descubiertas y notificadas.	Verificar que la herramienta de evaluación sea actualizable, tenga licencia (por lo tanto, se actualice regularmente) y esté actualizada.	Se puede evaluar en relación con las fechas de actualización de la lista de vulnerabilidades. Verificar la comunicación con el sitio de actualización del proveedor o la existencia de un sitio espejo dentro de la organización.	2
Evaluación del control de la seguridad	22.8	Validar las vulnerabilidades detectadas por el sistema automático, mediante un proceso interno, incluida una evaluación de las vulnerabilidades identificadas en otros sistemas.	La organización definirá un proceso de validación, tratando, al menos, las vulnerabilidades críticas detectadas, verificando, de manera manual o automática, la existencia de estas vulnerabilidades en otros sistemas.	Por ejemplo, si se descubre una vulnerabilidad crítica en Windows, o en la base de datos del sistema, es posible evaluar servidores no actualizados, ejecutando la misma versión con una herramienta.	4
Evaluación del control de la seguridad	22.9	Realizar escaneos con autorización especial, con la herramienta de evaluación de vulnerabilidades.	La organización designará una persona con autorización especial para el sistema que se esté escaneando, lo que permitirá realizar una evaluación exhaustiva de todos los procesos y actualizaciones instaladas, así como de las vulnerabilidades en sus definiciones más estrictas.	La mayoría de las herramientas de evaluación del control de la seguridad permiten un escaneo con autorización especial.	4

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Evaluación del control de la seguridad	22.10	Verificar la existencia de una herramienta automática que compare escaneos de vulnerabilidad pasados y presentes para permitir el control y el análisis de tendencias.	La organización realizará un seguimiento automático de las vulnerabilidades detectadas para identificar sistemas de alto riesgo o sistemas con una implementación de controles insatisfactoria.	Se puede implementar con las herramientas de escaneo o mediante una interfaz con sistemas de terceros (como SIEM).	4
Evaluación del control de la seguridad	22.11	Constatar la armonía de los resultados de las diferentes herramientas de evaluación de control de seguridad implementadas en la organización, a fin de obtener una imagen completa de la situación actual de diversas vulnerabilidades.	Verificar que todas las herramientas de evaluación y control de vulnerabilidades estén vinculadas a un sistema central para obtener una situación actual unificada de todas las vulnerabilidades y controles.	Se puede hacer mediante el establecimiento de una interfaz entre el escaneo de vulnerabilidades y las herramientas de administración de parches a una interfaz central, como SIEM, o una herramienta de análisis de datos o inteligencia empresarial, para producir un amplio informe de vulnerabilidad.	4
Evaluación del control de la seguridad	22.12	Integrar un mecanismo automático de corrección central de fallas.	La organización establecerá un sistema central para gestionar las vulnerabilidades y su corrección.	Puede implementarse mediante el establecimiento de interfaces entre la matriz de gestión de vulnerabilidades y el sistema de lectura organizacional, o mediante el uso de un sistema designado (gobernanza, riesgos y conformidad [GRC]).	3
Evaluación del control de la seguridad	22.13	Controlar el proceso de corrección de vulnerabilidades. Aplicar objetivos medibles para corregir vulnerabilidades, de acuerdo con su gravedad.	La organización definirá los objetivos del acuerdo de nivel de servicio para hacer frente a las vulnerabilidades, en función de su gravedad. Además, se deben definir alertas en relación con la desviación de las tablas temporales de corrección de vulnerabilidades, en relación con las medidas y objetivos definidos (acuerdo de nivel de servicio).	Por ejemplo, las vulnerabilidades críticas se corregirán de inmediato, las vulnerabilidades altas en un mes, las medias en tres meses, etc. Además, implementar alertas de acuerdo de nivel de servicio para las llamadas abiertas en la matriz de gestión de vulnerabilidades e informe sobre las desviaciones de estos objetivos.	3
23. Ciberdefensa proactiva					
Los controles cibernéticos proactivos le otorgan a la organización flexibilidad para defenderse contra ataques diversos. La organización recopilará datos actualizados sobre amenazas cibernéticas y medidas para afrontarlas, e información sobre su presencia digital, traduciendo la información sobre las medidas en controles ad hoc aplicables.				Además, la organización implementará una matriz de engaño de posibles atacantes (<i>honeypots</i> o sistemas trampas y otras tecnologías de engaño) para confundir al atacante, reducir su motivación, atraparlo tan pronto como penetre en la organización, etc. La organización implementará patrones de comportamiento basados en controles de análisis en entornos sensibles.	
Ciberdefensa proactiva	23.1	Definir y actualizar periódicamente un programa proactivo de ciberdefensa.	Un programa proactivo de ciberdefensa detectará nuevas amenazas, ajustará los controles a las amenazas detectadas, recopilará información de inteligencia y otros datos, y estudiará nuevos controles.		3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Ciberdefensa proactiva	23.2	Recopilar información actualizada sobre ciberamenazas y métodos para afrontarlas.	La organización aprenderá de las fuentes de información pública sobre nuevas amenazas cibernéticas, relevantes para sus actividades y tecnologías.	Se puede obtener acceso a información, herramientas gratuitas, tutoriales y otras herramientas de fuentes abiertas, como Metasploit, sitios de compañías de seguridad, etc., y contactar con empresas de inteligencia.	3
Ciberdefensa proactiva	23.3	Recopilar datos sobre su presencia digital (actividades operacionales, clientes, usuarios internos).	Dicha recopilación está destinada a identificar casos de exposición de datos sensibles en Internet, incluida la "red oscura".	Utilizar los servicios de empresas especializadas.	3
Ciberdefensa proactiva	23.4	Utilizar información sobre amenazas cibernéticas para diseñar y mejorar los controles aplicables.	La organización aplicará los cambios necesarios a las definiciones de sus sistemas de seguridad de datos, así como a su infraestructura y controles de aplicaciones, para hacer frente a las nuevas amenazas.	Los cambios pueden aplicarse a redes, cortafuegos, sistemas aplicativos y definiciones de interfaz, etc. Actualizar las reglas de los sistemas siguiendo la actualización de sus definiciones.	3
Ciberdefensa proactiva	23.5	Implementar una serie de engaños ante posibles atacantes.	La organización integrará tecnologías para atraer, engañar y retrasar a los posibles atacantes, para mejorar sus capacidades de identificación y respuesta.	Sistemas como los <i>honeypots</i> o redes trampa, los servidores virtuales designados y monitoreados y el sellado de archivos. Se puede implementar de varias maneras, como la definición de usuarios ficticios, objetos dentro del controlador de dominio, destinados a atraer a los atacantes, ocultando archivos con nombres atractivos, como "Salarios", "Contraseñas", "Secretos", etcétera.	3
Ciberdefensa proactiva	23.6	Integrar controles basados en el análisis de patrones de comportamiento (del sistema y los usuarios) en entornos sensibles.	La organización integrará sistemas, identificando anomalías en los niveles de servicio del servidor y la red y entornos de datos confidenciales.	Dichos sistemas pueden funcionar a nivel de servidor (Advanced Threat Analytics) y a nivel de red (MacAfee, NTBA, STRM Sourcefire 3d, etcétera).	3

RESPONDER


24. Gestión de eventos e informes

La organización debería ser capaz de gestionar un evento cibernético continuo de una manera que reduzca el daño, neutralice la amenaza y vuelva a la normalidad. Esto junto con informar sobre el evento, extraer lecciones y ajustar la matriz de defensa en consecuencia. Dichos controles persiguen este objetivo.

En su marco, la organización definirá medidas para hacer frente a un evento cibernético, informando a los empleados acerca de canales sobre un incidente de seguridad sospechoso, la entidad profesional (dentro o fuera de la organización) que proporciona conocimiento profesional, apoyo y asistencia en el monitoreo, la identificación, investigación y reacción ante los eventos cibernéticos. La organización definirá los informes que se elaborarán en caso de eventos cibernéticos y sus desenlaces (por ejemplo, para el equipo nacional de respuesta ante emergencias informáticas y el regulador), etc. Inspeccionar las capacidades de respuesta periódicamente, utilizando las pruebas que defina la organización.

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Gestión de eventos e informes	24.1	Elaborar e implementar una política reactiva ante eventos. Revisar y actualizar la política periódicamente.	La organización redactará e implementará una política reactiva ante incidentes de seguridad de datos, como parte de su política de seguridad de datos, y la revisará y actualizará.	Al elaborar la política de tratamiento de eventos, se han de designar empleados y equipos de respuesta, definir niveles de gravedad y medios de comunicación con las autoridades (la policía, ILITA, la Dirección Nacional de Ciberseguridad, el regulador, etcétera). Definir los administradores de eventos (varios funcionarios pueden tener el control durante varios eventos, como ataques de <i>ransomware</i> , amenazas de publicar los datos de los usuarios, etcétera). Es importante redactar esta política en colaboración con terceros relevantes, como reguladores, proveedores, con especial atención a los sistemas en la nube, subcontratando empleados, etc. Se recomienda definir situaciones durante las cuales se debe abrir una sala de control, cuándo y cómo implicar a la administración, la frecuencia de los informes, apelar al equipo nacional de respuesta ante emergencias informáticas o a la Dirección Nacional de Ciberseguridad, la recuperación, etcétera.	2
	24.2	Desarrollar un plan para enfrentar los incidentes de seguridad informática y cibernética.	La organización desarrollará un plan para identificar, hacer frente y responder a eventos cibernéticos y de datos, que incluirá: un resumen de la comprensión de las capacidades de respuesta a incidentes de seguridad; una descripción de las capacidades para hacer frente a los eventos, respuesta a las demandas de la organización, considerando sus tareas y tamaño, y eventos que exigen su notificación; un suministro de medios de medición de las capacidades de la organización para hacer frente a los eventos; y los recursos y soporte administrativo necesarios para mantener y mejorar las capacidades de respuesta.		2
	24.3	Desarrollar capacidades para hacer frente a los eventos de ciberseguridad y de datos, incluidos preparativos, detección y análisis, intercepción y recuperación.	Estos controles tienen como objetivo asegurar que la organización mantenga el conocimiento y las herramientas necesarias para informar, contener y gestionar un evento de manera eficaz y para hacer frente a sus consecuencias.	Puede implementarse mediante el plan para hacer frente a incidentes de seguridad, haciendo hincapié en la contratación de profesionales que sirvan de base para la detección de eventos y la respuesta correspondientes, capacitando al equipo para hacer frente a varios eventos (propagación de virus, <i>ransomware</i> , manejo de un ataque de denegación de servicio distribuido [DDoS, por sus siglas en inglés], filtración de información, etcétera). Se puede implementar mediante herramientas de informes o equipos de respuesta ante emergencias informáticas.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Gestión de eventos e informes	24.4	Integrar mecanismos automáticos para soportar el manejo de eventos.	Administrar múltiples eventos y alertas es complicado. Por consiguiente, se requiere automatizar tanto como sea posible el seguimiento del estado de alerta, las actividades requeridas, las decisiones, etcétera.	Se puede implementar vinculando los sistemas de comando y control al monitoreo de eventos y los sistemas de detección. Es posible definir procedimientos de respuesta dentro de los sistemas de mando y control. Puede hacerse mediante sistemas de apoyo a la toma de decisiones, sistemas de gestión de flujo de trabajo o sistemas de tickets. Se recomienda que tales herramientas ayuden a la organización a localizar eventos a largo plazo, eventos graves no tratados adecuadamente y situaciones que requieran una intervención inmediata.	3
Gestión de eventos e informes	24.5	Registrar los incidentes de seguridad de datos y cómo enfrentarlos, incluida la recopilación de datos, actividades y conclusiones.	La organización mantendrá un mecanismo centralizado de presentación de informes, para tener un informe unificado y completo de la situación del evento y la evaluación de los riesgos.	Puede ser implementado centralmente por un centro de operaciones de seguridad, que recolecte y registre datos.	2
Gestión de eventos e informes	24.6	Definir canales de informes de seguridad de los datos para los empleados.	La organización aplicará procedimientos obligatorios de presentación de informes con un formato determinado en casos de eventos cibernéticos.	Puede implementarse instruyendo a los empleados sobre incidentes de seguridad de datos y sus procedimientos para informar al respecto. Se recomienda recurrir al equipo nacional de respuesta ante emergencias informáticas para obtener asistencia en torno a la respuesta y la recuperación.	1
Gestión de eventos e informes	24.7	Definir un empleado cuyo trabajo sea proporcionar conocimiento profesional, apoyo y acompañamiento en el monitoreo, detección, informe y respuesta a incidentes de seguridad de datos.	La organización designará una entidad profesional para que sirva como fuente de conocimiento profesional, en la identificación y el informe de incidentes de seguridad de datos.	Puede ser una entidad interna o externa, que tenga experiencia en identificar, informar y responder a eventos. Guiará a los equipos que actúan cuando se produce un evento y compartirá su experiencia en caso de eventos cibernéticos.	3
Gestión de eventos e informes	24.8	Integrar un mecanismo que brinde accesibilidad a la información sobre reacciones a eventos de ciberseguridad y de datos.	La organización proporcionará acceso a un archivo que contenga procedimientos de detección y respuesta en caso de eventos de ciberseguridad y de datos.	Puede implementarse mediante cualquier sistema de gestión de datos o documentación, o bien mediante una copia impresa.	2
Gestión de eventos e informes	24.9	Instruir a los empleados relevantes en materia de reacción ante incidentes de seguridad.	La organización capacitará a todas las entidades involucradas en el manejo de incidentes de seguridad de datos para identificar y responder a tales eventos. Estos seminarios se actualizarán periódicamente.	Los seminarios deben tratar los procedimientos de respuesta, mejores prácticas y herramientas destinadas a hacer que esa información esté accesible durante tales eventos.	2
Gestión de eventos e informes	24.10	Integrar simulaciones de eventos dentro de la capacitación para mejorar la efectividad de respuesta de los equipos en crisis.	La organización simulará escenarios de incidentes de seguridad de datos para probar su disponibilidad y prepararse en consecuencia.	En algunos ejercicios se simularán eventos de manera guiada, y el guía del ejercicio medirá las reacciones de los equipos. Otros ejercicios simularán eventos en entornos de producción, con medios reales, como los ejercicios sobre el <i>phishing</i> .	3

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Gestión de eventos e informes	24.11	Implementar mecanismos automáticos para proporcionar entornos de capacitación realistas.	La organización simulará incidentes de seguridad de datos reales en entornos que simulen el entorno organizativo.	Los casos se pueden simular en entornos de prueba o en laboratorios externos designados (un laboratorio cibernético profesional).	4
Gestión de eventos e informes	24.12	Examinar las capacidades de respuesta periódicamente, a fin de verificar su efectividad. Para eso, utilizar la prueba definida por la organización, que incluirá una simulación de un evento real. Registrar los resultados de cada prueba periódica.	Para probar las capacidades de respuesta a incidentes de seguridad de datos, la organización simulará ataques reales, entre otras cosas con herramientas de ataque automático. La organización registrará y derivará lecciones de estos ejercicios, y elaborará un reporte informativo.	Puede medirse mediante un <i>script</i> de evento, contando los eventos detectados y la calidad de la respuesta (minimización de los daños, comunicación entre entidades, concentración e intervención, recuperación). La detección de eventos puede integrarse con intentos reales de penetración llevados a cabo en la organización. Se utilizarán herramientas de ataque reales en la prueba.	3
					
RECUPERAR					
25. Continuidad del negocio El objetivo de la organización es mantener la continuidad del negocio y minimizar los daños causados por los eventos cibernéticos. Esa es la razón de ser de los controles de continuidad del negocio. La organización debería verificar la rápida recuperación de sus infraestructuras cibernéticas.				Preparar infraestructuras alternativas (incluidas disponibilidad y redundancia), probar y practicar periódicamente el plan de continuidad del negocio. Realizar copias de seguridad eficaces, disponibles y confiables es fundamental para la continuidad del negocio y deben realizarse regularmente.	
Continuidad del negocio	25.1	Definir, implementar, revisar y actualizar una política de continuidad del negocio en relación con la ciberdefensa.	La organización preparará un plan de continuidad del negocio, derivado de sus objetivos, mediante la implementación de controles y procesos para lograr estos objetivos. El plan tomará en consideración varios escenarios de desastres y procesos críticos. La organización definirá aquellos activos al servicio de tareas y funciones críticas (físicas y digitales) de la organización. También establecerá el período máximo de cierre de servicios esenciales antes de volver a la normalidad (en situaciones de emergencia). Como parte del plan de continuidad, la organización determinará el período de tiempo dentro del cual las tareas esenciales volverán a la normalidad desde la operación del plan.	La organización redactará, implementará y actualizará periódicamente un plan de continuidad del negocio. Dicho plan definirá la conducta de la organización en períodos normales y de emergencia para garantizar la continuidad del negocio (incluidos índices comunes, como el tiempo objetivo de recuperación) en casos de eventos cibernéticos. Es posible encontrar ayuda en normas como la ISO 22301.	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Continuidad del negocio	25.2	Preparar la planificación de la capacidad requerida para emergencias (de informática, comunicación, servicios de apoyo).	La organización se asegurará de que los sistemas y la infraestructura destinados a la continuidad del negocio en emergencias, respalden la capacidad deseada para los alcances y períodos de tiempo requeridos.	Se puede implementar siguiendo un mapeo de servicios críticos, definiendo los objetivos de recuperación y supervivencia de cada servicio. Normalmente, la organización mide la capacidad requerida en el sitio alternativo, en términos de infraestructuras de comunicación, infraestructuras de sistemas, aplicaciones y licencias.	2
Continuidad del negocio	25.3	Instruir a los empleados sobre la continuidad del negocio.	La organización instruirá a los empleados en los procedimientos de continuidad del negocio.	Establecer las funciones de los empleados en la recuperación, los sitios temporales de reunión, de logística y operaciones, y los objetivos de recuperación de los distintos niveles del equipo y la organización.	2
Continuidad del negocio	25.4	Ejercitar el plan de continuidad del negocio de manera periódica.	La organización preparará y realizará ejercicios de preparación para evaluar la efectividad del plan de continuidad del negocio.	Eso podrá hacerse mediante la puesta en práctica de varios escenarios. Se recomienda que el ejercicio incluya los aspectos de TI del plan de continuidad del negocio, como las comunicaciones telefónicas e informáticas, también aspectos complementarios, como los proveedores y los servicios (locales y en la nube), guiados por el plan de la continuidad del negocio. Además es importante aumentar la concienciación sobre las emergencias, teniendo en cuenta la necesidad y la urgencia de cambiar las nuevas versiones al entorno de producción, siendo estrictos al acompañar a visitantes, tratando de recuperar archivos, ejercitando la gestión de eventos cibernéticos, la toma de decisiones a nivel de gestión, los informes y extrayendo enseñanzas.	2
Continuidad del negocio	25.5	Ejercitar el plan de continuidad del negocio mediante simulaciones periódicas.	La organización utilizará simulaciones e involucrará a los empleados que se espera que participen en la implementación del plan de recuperación.	Para llevar a cabo simulaciones tan cercanas a la realidad, preparar escenarios de desastres, operar el plan (de manera reducida) en el entorno de recuperación ante desastres y probar la validez del plan.	3
Continuidad del negocio	25.6	Probar el plan de continuidad periódicamente y subsanar las lagunas descubiertas.	La organización revisará y corregirá periódicamente su plan de continuidad del negocio.	Por ejemplo, mediante un programa de pruebas, que realice un cambio parcial a un entorno de emergencia o a varios sistemas, para probar los procesos de cambio.	2
Continuidad del negocio	25.7	Probar el plan de continuidad en el sitio alternativo, con el fin de familiarizar al equipo de continuidad con el sitio y sus recursos y evaluar las capacidades del sitio para apoyar las actividades que requieren continuidad.	La organización preparará procesos y procedimientos para familiarizarse y practicar con el sitio de respaldo como parte del ejercicio de la continuidad del negocio.	Se puede hacer viajando al sitio de respaldo, familiarizándose con el sistema almacenado allí y ejerciendo el cambio real al sitio alternativo.	2
Continuidad del negocio	25.8	Utilizar herramientas automatizadas para probar a fondo el plan de continuidad.	La organización utilizará herramientas automatizadas que permiten controlar y probar la efectividad del plan.	Dichas herramientas pueden ser un control de la matriz de respaldo, incluyendo alertas de falla, control de alta disponibilidad entre los sitios principal y secundario, monitoreo de comunicaciones entre sitios, etcétera.	8

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Continuidad del negocio	25.9	Realizar una recuperación completa del sistema como parte de las pruebas del plan de continuidad.	La organización realizará periódicamente una recuperación completa de la copia de seguridad de los sistemas definidos como parte del plan de recuperación ante desastres.	Por ejemplo, una recuperación completa en el entorno de copia de seguridad. Tras la recuperación, realizar pruebas de aceptación para verificar la funcionalidad completa que incluyan comparaciones de datos, pruebas de configuración y trabajo con los sistemas recuperados.	3
Continuidad del negocio	25.10	Establecer un sitio alternativo de respaldo y computación que permita una recuperación completa al mismo nivel de seguridad que el sitio principal.	La organización establecerá y mantendrá un sitio secundario, que contendrá copias de los sistemas, así como datos y sistemas de seguridad de almacenamiento, todo lo cual respaldará la recuperación y la continuidad del negocio de los procesos críticos.	Se puede implementar duplicando servidores y entornos de supervivencia en el sitio alternativo, técnicas de virtualización, etcétera.	2
Continuidad del negocio	25.11	Verificar la separación física y lógica para evitar que ambos sitios sean atacados simultáneamente.		La organización velará para que exista una distancia geográfica adecuada entre ambos sitios, así como entre las redes de computadoras y la infraestructura de soporte.	2
Continuidad del negocio	25.12	Definir el sitio de respaldo de una manera que favorezca la aplicación del plan de recuperación.	La organización definirá sistemas y líneas de comunicación de manera que permita una recuperación rápida y efectiva.	Esto puede implementarse mediante sistemas de alta disponibilidad en varias configuraciones, lo que permite la duplicación de datos y la disponibilidad de manera rápida tras la recuperación en el sitio alternativo.	2
Continuidad del negocio	25.13	Identificar posibles problemas de accesibilidad al sitio alternativo en casos de desastres regionales y tomar las medidas preventivas adecuadas.	La organización verificará la accesibilidad del sitio en casos de desastre.	Por ejemplo, verificar la existencia de varios enfoques, la supervivencia a los terremotos y la accesibilidad remota.	2
Continuidad del negocio	21.14	Preparar acuerdos de infraestructura de sitios de respaldo, que contengan cláusulas de prioridad de servicio, de acuerdo con los objetivos de recuperación de la organización.	La organización verificará que sus acuerdos de servicio contengan cláusulas que comprometan al proveedor a un servicio y tiempos de respuesta compatibles con sus objetivos.	Se puede verificar que los acuerdos de nivel de servicio con los tiempos de respuesta y recuperación de los programadores del sistema del proveedor del sitio de respaldo sean compatibles con el tiempo objetivo de recuperación del servicio de la organización. Es posible indicar la prioridad fundamental para la recuperación de servicios críticos.	2
Continuidad del negocio	21.15	Verificar la preparación del sitio alternativo para funcionar como sitio principal y servir de apoyo en las tareas y funciones esenciales de la organización.	La organización verificará que todos los servicios (incluido el soporte y la infraestructura) en el sitio de respaldo estén disponibles y sean funcionales en cualquier momento.	Eso puede verificarse preparando listas de etiquetado detalladas para sistemas de soporte e infraestructura, y mediante pruebas periódicas de normalidad (así como durante el ejercicio).	2

Familia	ID	Monitoreo	Explicación complementaria	Ejemplo de realización del monitoreo	Nivel de control
Continuidad del negocio	25.16	Preparar copias de seguridad de las redes de comunicación y verificar la existencia de servicios de comunicación alternativos para reducir la dependencia de un único punto de falla.	La organización verificará la existencia de una red de comunicación alternativa entre sus sitios principal y de respaldo, así como un enlace de comunicación dual al sitio principal.	Se puede verificar comprando y operando líneas de comunicación de respaldo, minimizando así la dependencia de un único punto de falla.	2
Continuidad del negocio	25.17	Requerir que los proveedores de servicios de emergencia alternativos preparen y prueben periódicamente un plan de continuidad del negocio.	La organización verificará que los objetivos de recuperación de los proveedores sean compatibles con los suyos.	Los proveedores pueden proporcionar sus propios planes de emergencia, incluidos los objetivos de recuperación de los servicios prestados a la organización.	2
Continuidad del negocio	25.18	Preparar y proteger las copias de seguridad de los niveles de usuario, sistema y documentación.	La organización realizará una copia de seguridad de todos sus datos esenciales y garantizará su disponibilidad, integridad y confidencialidad.	Copias de seguridad en discos, cintas y en la nube.	1
Continuidad del negocio	25.19	Verificar la fiabilidad y disponibilidad del respaldo. 	La organización se asegurará de contar con copias de seguridad confiables y disponibles.	Se puede hacer con pruebas de recuperación periódicas.	2
Continuidad del negocio	25.20	Conservar una copia de seguridad de los datos críticos lejos del sitio principal.	La organización se asegurará de conservar una copia de seguridad en un sitio remoto, protegida de desastres ambientales (incendios, etcétera).	Se puede hacer directamente realizando una copia de seguridad en un sitio remoto, o mediante la entrega regular de los soportes que contengan la copia de seguridad a ese sitio.	2
Continuidad del negocio	25.21	Implementar un mecanismo de recuperación de transacciones para sistemas basados en transacciones.	La organización instalará un mecanismo para recuperar transacciones fallidas debido a una falla del sistema o un cambio a un sistema de respaldo.	Se puede implementar en diversas configuraciones: una configuración de escritura doble (dos transacciones paralelas en los sistemas principal y de respaldo), verificando las transacciones tras enviarlas y etiquetando las transacciones fallidas. En los sistemas de gestión de colas, se puede hacer una copia de seguridad de la cola.	2
Continuidad del negocio	25.22	Verificar una capacidad de recuperación para una situación operativa conocida.	Verificar la existencia de mecanismos que permitan la recuperación de datos o la configuración para una situación conocida.	Se puede realizar mediante una copia de seguridad de la configuración en un punto de tiempo (antes de implementar cambios), y determinando puntos de recuperación de datos y mecanismos de reversión.	3
Continuidad del negocio	25.23	Verificar el servicio y la redundancia de la infraestructura crítica.	La organización verificará la redundancia de servicios e infraestructuras críticas, a fin de minimizar la dependencia de un único punto de falla.	Se puede implementar mediante la redundancia de infraestructuras críticas, como equipos de comunicación, servicios de red principales, sistemas de seguridad y almacenamiento, etcétera.	3

Anexos

Anexo 1. Ejemplo de ejecución de evaluación de riesgos para un activo informático

Cuadro A1.1. Ejemplo de ejecución de evaluación de riesgos para un activo informático

En el siguiente ejemplo el cálculo es: **Riesgo = 3I + P = 3x3 + 2**

	Pregunta	Ejemplo de respuesta	Puntuación ponderada
Cuestionario del nivel de impacto (intensidad [I]). Este cuestionario aparece en la página 34 (cuadro 4).	¿Cuál es el nivel de daño causado a la organización después de la fuga del activo? C	2	Valor máximo = 3
	¿Cuál es el nivel de daño causado a la organización después de la interrupción de la información existente en el sistema? I	1	
	¿Cuál es el nivel de daño causado a la organización después de un apagado del sistema a largo plazo? D	3	
Cuestionario del nivel de exposición (probabilidad [P]). Este cuestionario aparece en la página 38 (cuadro 5)	¿Cuántos usuarios tiene el sistema?	2	Valor medio = 2
	¿Quiénes son los usuarios del sistema?	4	
	¿Cuántas interfaces tiene el sistema?	1	
	¿Cuál es la naturaleza de las interfaces del sistema?	1	
	¿Qué tipo de información existe en el sistema?	3	
	¿Hay un acceso remoto al sistema?	1	
	¿Cuál es el nivel de permisos de compartimentación en el sistema?	2	
	¿Cuál es el nivel de actualización del sistema?	3	
	¿Cuál es la política de actualizaciones y parches de seguridad?	4	
	¿Cuál es el nivel de seguridad física del sistema?	2	
Sistema de puntuación de riesgo ponderado			3 x 3 + 2 = 11

Después de contestar el cuestionario anterior para todos los activos de la organización, se obtiene lo siguiente (cuadro A1.2.).

Cuadro A1.2. Ejemplo de cálculo de riesgo de un activo

Probabilidad (P)				Intensidad (I)
1	2	3	4	
7	10 Sistema C	13	16 Sistema A	4
6	9	12	15	3
5 Sistema E	8	11 Sistema B Sistema D	14	2
4	7	10	13	1

Anexo 2.

Kit de herramientas para la aplicación de la Metodología de Ciberdefensa

Con el fin de ayudar en la implementación de la Metodología de Ciberdefensa y hacerla accesible a diferentes audiencias objetivo, la INCD desarrollará un conjunto de herramientas. Además, diversas entidades económicas también pueden desarrollar kits de herramientas, como es habitual en casos similares en todo el mundo.

El conjunto de herramientas que la INCD planea desarrollar consiste en:

01

Un proceso de automatización de la Metodología de Ciberdefensa a través de una plataforma tecnológica conveniente y eficiente.

02

Formas genéricas y procedimientos listos para su uso por parte de la organización, como por ejemplo, un documento de política corporativa acerca de los aspectos de ciberdefensa, procedimiento de control de la Metodología de Ciberdefensa, plantillas de formularios, en-

tre otros. La organización debe adaptar estos ejemplos y plantillas a según sus necesidades.

03

Una calculadora de evaluación de riesgos, para la automatización de algunas fórmulas sencillas de la Metodología de Ciberdefensa.

04

Ejemplos de mapeo de activos cibernéticos.

05

Información de enriquecimiento para los controles.

06

Mejores prácticas para controles seleccionados.

07

Kits de entrenamiento para diferentes poblaciones objetivo.

Es posible encontrar un kit de herramientas que soporta la Metodología de Ciberdefensa de acuerdo con la siguiente jerarquía:

- Una percepción nacional, sobre la base de la cual se escribe la Metodología de Ciberdefensa para Organizaciones.
- Una Metodología de Ciberdefensa, que presenta las diversas cuestiones de protección en el nivel básico (por ejemplo, seguimiento, conciencia, separación de redes, gestión de la cadena de suministro, etcétera).
- Mejores prácticas: sobre la base de esta metodología, se escribirán junto con los usuarios directrices específicas para la tecnología o servicio, etc., como por ejem-

plo, mejor práctica de endurecimiento de los servidores de base de datos de un tipo particular o cómo trabajar correctamente con el sistema operativo WIN 10, etcétera.

- Extensiones profesionales: junto a la Metodología de Ciberdefensa habrá documentos de extensión con información adicional que no depende de una tecnología específica (mejor práctica), sino que, por el contrario, es más amplia y detallada que los requisitos básicos de la Metodología de Ciberdefensa (“extensión profesional”).

La información anterior estará accesible en diversas formas (guías, cursos en línea, localizador para las pequeñas empresas, cursos de capacitación, etc.).

Gráfico A2.1. Implementación de la Metodología de Ciberdefensa

	Mejores prácticas A	Mejores prácticas B	Mejores prácticas C	Mejores prácticas D	Mejores prácticas E
Extensiones profesionales	Metodología de Ciberdefensa para Organizaciones / ciberseguridad				
Por ejemplo: desarrollo seguro, trabajo en un entorno de nube, externalización y cadena de suministro, continuidad del negocio, etc.	Percepción				

Anexo 3. Controles para la defensa de una organización de categoría A: lo más destacado para proveedores de servicios TI



Cuadro A3.1. Liderazgo y supervisión de los controles de protección

Familia	Encabezamiento	Supervisión	Explicación complementaria
Responsabilidad de la Dirección	Gobierno corporativo	Examine periódicamente el enfoque de la organización sobre seguridad de la información y gestión de ciberdefensa y su aplicación.	En el marco de este seguimiento, examine los controles de seguridad implementados en la organización, y también la política de seguridad de la información y la protección de los procesos de negocio críticos de la organización.
Prevención de código malicioso	Detección y prevención de código malicioso en los puntos finales y servidores de la organización	Implemente herramientas para detectar y prevenir el código malicioso en los puntos finales y servidores de la organización. Estas herramientas se ejecutan en modo de protección activa y también se llevan a cabo exploraciones periódicas.	Debido a que algunos artefactos pueden penetrar en los mecanismos de seguridad, asegúrese de que los controles para el manejo de código malicioso también se aplicarán al nivel de las estaciones de trabajo.
Prevención de código malicioso	Actualizaciones automáticas	Ejecute actualizaciones automáticas de todos los sistemas de identificación y prevención de código malicioso dentro de la organización.	La organización activará las actualizaciones automáticas de un servidor central, gestionado por la organización o por un proveedor de servicios reconocido. Estas actualizaciones mantendrán las herramientas de protección constantemente actualizadas.
Cifrado	Criterios de cifrado	Defina los usos que requieren cifrado y el tipo de cifrado necesario, de conformidad con las leyes, directrices, procedimientos, reglamentaciones y compromisos de negocios.	La organización definirá qué información y sistemas deben ser encriptados y registrará la configuración de la encriptación de información. Los requisitos pueden derivar de los requisitos aplicables a la organización o de los de retención de información.
Protección de estaciones de trabajo y servidores	Política de endurecimiento	Defina, documente e implemente una política de endurecimiento para estaciones de trabajo y servidores, que cumpla con los requisitos de seguridad de la información de la organización.	La organización definirá los requisitos de endurecimiento de los sistemas dentro de la organización, con énfasis en los requisitos básicos, la frecuencia de cambios y el nivel de clasificación. Luego documentará los requisitos de un marco general que servirá como base para la escritura de los procedimientos de endurecimiento.

Familia	Encabezamiento	Supervisión	Explicación complementaria
Protección de estaciones de trabajo y servidores	Implementación del endurecimiento	Es necesario definir la configuración del sistema para proporcionar la funcionalidad mínima requerida (mientras bloquea las funciones, puertos y protocolos innecesarios).	La organización definirá procedimientos para cada sistema y tipo de servidor, con base en prácticas aceptables de endurecimiento para incluir, como mínimo: <ol style="list-style-type: none"> 1. Reducción de la superficie de ataque del sistema mediante el bloqueo de los puertos innecesarios. 2. Desactivación de los servicios innecesarios. 3. Remoción de cuentas de usuario invitado. 4. Preferencia de usar protocolo de comunicación segura entre servidores. 5. Obtención de alertas de una manera ordenada. 6. Bloqueo de las funciones sensibles del sistema. 7. Envío de registros de eventos del sistema a un servidor de monitorización. 8. Bloqueo de la instalación de software por parte de usuarios no autorizados.
	Computación en la nube pública	Responsabilidad compartida	Es necesario entender la división de funciones entre el proveedor de servicios y la organización, e implementar el monitoreo de protección en consecuencia.
		Compartir información sensible	Asegúrese de que no haya datos que se transfieran a los servicios en la nube, que no deben ser transferidos siguiendo las regulaciones y las responsabilidades de la organización.
Protección de la información	Protección de la información almacenada en recursos compartidos	Evite la transferencia de datos no autorizada o involuntaria a través de recursos compartidos del sistema.	Al utilizar los servicios en la nube pública se debe dividir la responsabilidad de la protección cibernética entre cuestiones bajo la responsabilidad del proveedor y cuestiones bajo la responsabilidad del cliente. Esta división de la responsabilidad depende de la naturaleza del servicio y modelo de implementación. La organización tiene que entender cuáles son los temas que están bajo su responsabilidad y poner en práctica las consecuencias de esta responsabilidad.
Seguridad de la red	Gestión de conexiones (sesiones) a nivel de red	Hay datos que la organización no puede transferir para su almacenamiento o procesamiento en los servicios de la nube pública debido a consideraciones regulatorias o compromisos con terceras partes. Antes de transferir datos a la nube, asegúrese de que esos datos no se transfieren ni se mantienen en los servicios en la nube.	La organización debe impedir la transferencia de información de forma no autorizada, por ejemplo, mediante el uso de carpetas compartidas, correo electrónico, medios extraíbles, etc.
	Fiabilidad de las sesiones	La organización operará dispositivos tecnológicos con el fin de proteger los servicios contra ataques DoS.	Defiéndase de los ataques DoS de diversos tipos, como cargar los recursos informáticos para que colapsen, cargar el ancho de banda de comunicación, cargar la página web para que se bloquee, entre otros.
		Asegúrese de que el servicio DNS es proporcionado por un servidor de confianza (interno o externo a la empresa).	La organización permitirá obtener direcciones de servicios de traducción solo desde un servidor interno seguro, con el fin de evitar el enrutamiento de comunicación errónea (intencionalmente o no) a objetivos hostiles.

Familia	Encabezamiento	Supervisión	Explicación complementaria
Seguridad de la red	Límites de la red	Es necesario limitar el número de canales de comunicación fuera del sistema.	La organización reducirá y unirá los canales de comunicación para asegurar un mejor control sobre las conexiones con el sistema.
		Bloquee por defecto todo el tráfico de red y de forma manual permita cualquier tráfico deseable por medio de reglas de excepción.	La organización definirá las reglas de filtrado de tráfico de la red con el fin de bloquear por defecto todo el tráfico no se defina explícitamente como permitido.
		Use direcciones de red separadas (diferentes subredes) para conectarse a diferentes zonas de seguridad.	La organización determinará que cada subred tenga un rango de direcciones separado, que será publicado en el cortafuegos y enrutador.
Control de acceso	Administración de los usuarios	Configure cuentas de usuario que soporten las funciones de negocio de la organización.	Por lo menos, separe la cuenta “administrador” de la cuenta de “usuario”. También es necesario configurar los usuarios que manejan las funciones de seguridad del sistema (como la creación de usuarios, gestión de acceso y privilegios del sistema, gestión de los sistemas de seguridad de la información, etcétera).
	Administración de permisos	Defina y haga cumplir los privilegios de acceso lógico al sistema y la información de acuerdo con la política de control de acceso.	El control de acceso se puede hacer a nivel personal (con base en la identidad), o a nivel del rol (basado en roles), y su objetivo es controlar el acceso de las entidades (usuarios o procesos informáticos) a objetos (archivos, discos, dispositivos, etcétera).
Recursos humanos y sensibilización de los empleados	Gestión de permisos durante el reclutamiento, movilidad o salida	Revise y actualice los permisos de acceso de un empleado mientras se desplaza de un trabajo a otro.	Defina la actualización de los procesos de movilidad de los empleados y de los permisos de conformidad con la nueva función (eliminación de permisos innecesarios y establecimiento de permisos necesarios para el nuevo trabajo).
Seguridad en las compras y desarrollo	Requisitos de seguridad en la contratación y en el desarrollo de sistemas	Seguridad de la cadena de suministro: solicite a los proveedores que cumplan con los requisitos de seguridad corporativa, reglamentos, normas y directrices.	La organización se asegurará de que los proveedores de servicios cumplan con los requisitos de cumplimiento de la organización, así como con los requisitos reglamentarios aplicables en los países en los que opera la organización.

Familia	Encabezamiento	Supervisión	Explicación complementaria
Protección física y ambiental	Iluminación de emergencia	Implemente y mantenga la iluminación de emergencia automática, que se activará en el caso de una rotura o interrupción en la fuente de alimentación e incluirá las salidas de emergencia y rutas de evacuación en la instalación.	
	Protección contra incendios	Implemente y mantenga los recursos o sistemas de detección y extinción de incendios para los sistemas de información que tienen una fuente de energía independiente.	
Registro y monitoreo	Mecanismo de monitoreo	<p>Active un mecanismo de documentación que produzca registros de control sobre los incidentes en la organización. Es necesario registrar, al menos, los eventos de los sistemas que contienen información confidencial de clientes, sistemas críticos para el rendimiento empresarial y sistemas centrales (servidores, componentes de comunicaciones, aplicaciones, bases de datos, etcétera).</p> <p>Los mecanismos de monitoreo y documentación incluirán, como mínimo, información sobre la naturaleza del acto cometido, fecha y hora, origen y destino de la operación, identificación de usuario, identificación de proceso, fracaso/éxito, nombre de archivo mixto.</p>	La organización se asegurará de que los sistemas de infraestructura y sistemas aplicativos activen un mecanismo de lista de eventos, y que los registros se mantienen durante un periodo establecido por la organización. Los registros de control contendrán información, como el tipo de evento, cuándo se produjo, su fuente, nombre de usuario. En cualquier caso, monitoree los sistemas de procesamiento de información sensible, que son parte de la infraestructura crítica de la organización o que gestionan los procesos centrales de la organización.
Gestión de eventos e informes	Manejo de incidentes cibernéticos y seguridad de la información	Defina canales de información desde los empleados hacia los encargados con el fin de notificar sobre incidentes de seguridad sospechosos.	La organización aplicará procedimientos para los eventos que requieran la presentación de informes, y para la manera de informar acerca de un evento definido como un ciberincidente.
Continuidad del negocio	Disponibilidad de recursos	Realice copias de seguridad a nivel de sistema y de usuario y de documentación, y garantice la protección de las copias de seguridad.	La organización realizará una copia de seguridad de toda la información crítica en los sistemas de información que soportan los procesos de negocio y garantizará la disponibilidad, integridad y confidencialidad de las copias de seguridad.

Anexo 4. Cumplimiento de las normas

La Metodología de Ciberdefensa tiene su base de conocimientos en las normas internacionales aceptadas, como NIST 800-53 e ISO 27001. Con el fin de hacer más fácil para las organizaciones adoptar aquellos que aparecen en esta publicación, la INCD ha vinculado los controles existentes con controles equivalentes en las normas mencionadas. En particular, una organización que cumple con la Metodología de Ciberdefensa y requiere la acreditación de la norma ISO 27001 puede utilizar el anexo de cumplimiento de las normas.

Más tarde, en paralelo con el desarrollo de la Metodología de Ciberdefensa, la INCD asignará los controles en relación con las principales normas nacionales e internacionales. Entre las normas más importantes que se pueden asignar, se encuentran las siguientes:

- Circular de Conducta Bancaria Aprobada 357 + 361.
- Circular de Gestión de Riesgo cibernético del Departamento de Mercado de Capitales.
- Directrices de ILITA.
- ISO 27032

Cumplimiento de ISO 27001

Dado que esta Metodología de Ciberdefensa se construye dependiendo en gran parte de las normas internacionales y, en particular, de la norma ISO 27001, la observancia que requiere una organización que implementa esta Metodología en función del pleno cumplimiento de los requisitos para una revisión de la certificación no es mayor.

Con el fin de facilitar a las organizaciones que están certificadas o están considerando la posibilidad de iniciar un proceso de certificación ISO 27001, puede usarse el cuadro de conversión que vincula los controles de la Metodología de Ciberdefensa con la declaración de aplicabilidad de la norma, el cual se encuentra en la página web de la INCD.

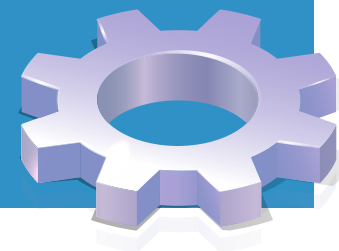
Anexo 5. Controles de protección fundamental para lograr una alta puntuación en poco tiempo

La Metodología de Ciberdefensa define un proceso de gestión de riesgos y, posteriormente, un requisito para el ejercicio de los controles en el marco de un plan de trabajo. Por otro lado, en algunas organizaciones existe la necesidad de centrar las primeras actividades en el rendimiento. Estas actividades incluyen, de hecho, los controles con el más alto costo-beneficio.

El Instituto SANS es considerado uno de los líderes mundiales en definiciones de los controles de seguridad críticos (CSC), que son los más eficaces. La aplicación de los controles, que cubren 20 temas, proporciona a la organización una respuesta frente al 88% de los ataques conocidos.²

Una organización que desee tener un panorama general sobre su preparación para la defensa puede hacerlo recorriendo los controles de protección críticos, que están marcados con un símbolo de llave en el cuadro 8, y que forman parte de las diversas familias de control.

Los controles en este documento se basan en la misma lógica, pero no necesariamente representan los controles clave del Instituto SANS.



2. Más información disponible en: <https://www.sans.org/critical-security-controls/history>.

Cuadro A5.1. Guía de Controles

Familia	Detección
Gestión y evaluación de riesgos	2.1
Control de acceso	4.2, 4.4, 4.17
Protección de la información	5.1
Protección de estaciones de trabajo y servidores	6.5
Prevención de código malicioso	7.1, 7.2, 7.3, 7.9
Cifrado	8.6
Seguridad de la red	9.1, 9.9, 9.12, 9.24, 9.25
Separación de entornos	10.2, 10.4
Computación en la nube pública	11.4, 11.6
Seguridad de los soportes físicos	15.7
Cadena de suministro y externalización	16.2
Seguridad en las compras y el desarrollo	17.14
Protección física y ambiental	18.6
Capacitación e instrucción	20.2
Registro y monitoreo	21.1
Evaluación de controles de seguridad	22.6
Gestión de eventos y generación de informes	24.12
Continuidad del negocio	25.1, 25.19

Anexo 6. Banco de controles

El banco de controles es un elemento significativo de la Metodología de Ciberdefensa. El banco, establecido sobre la base de normas comunes a nivel mundial, contiene muchos elementos destinados a mejorar la comprensión de la organización durante la implementación de los controles. Por razones de comodidad y eficiencia, las capas necesarias de información fueron insertadas en el cuerpo de esta publicación con el fin de implementar la Metodología de Ciberdefensa. Al mismo tiempo, se han establecido y escrito capas enriquecidas con información adicional sobre todos los controles. Estas capas son las siguientes:

01

CID: confidencialidad, integridad y disponibilidad son los aspectos de seguridad de la información que están protegidos por el control.

02

Cadena de ciberataque (cyber kill chain): etapa en la cadena de ataque durante la cual el control desempeña un papel.

03

Categorías de activos para las cuales el control es relevante: IT, OT, servicios o bases de datos.

04

Niveles de riesgo en los cuales se requiere la implementación: Si el nivel de riesgo de un activo es mayor, serán necesarios controles que proporcionen un nivel de protección más alto, adaptado al riesgo relevante para el activo (niveles 1-4 derivados de la tercera etapa del proceso de gestión de riesgos descrita en esta publicación).

05

Tipo de control: un control puede ser de guía (como un procedimiento), preventivo (como los sistemas de filtrado de *malware*) o de detección (por ejemplo, sistemas de vigilancia y de alarma).

06

Control del cumplimiento de los estándares comunes: en la primera etapa de la publicación de la Metodología de Ciberdefensa los controles se asignan a las normas ISO 27001 y NIST 800-53.

Mayor información sobre los capítulos de controles se puede encontrar en el sitio web de la INCD.

Anexo 7.

Hacer frente a un ciberincidente significativo

La Metodología de Ciberdefensa asume que es imposible garantizar una protección completa frente a los ataques cibernéticos. Por lo tanto, los capítulos de controles están diseñados para preparar a la organización para hacer frente y recuperarse con daños menores de incidentes cibernéticos. Por otro lado, a la luz de la experiencia pasada, se sabe que la gestión de importantes eventos cibernéticos es un campo profesional que requiere conocimientos especializados, herramientas, infraestructura y capacitación profesional especializada, los cuales no existen en todas las organizaciones. El equipo de respuesta ante emergencias informáticas (CERT, por sus siglas en inglés) nacional fue establecido bajo la INCD con el fin de ayudar a las organizaciones en el tratamiento de este tipo de eventos. La misión del CERT es mejorar la capacidad de recuperación cibernética de la economía israelí, proporcionando asistencia inicial y tratamiento frente a las amenazas informáticas, y también coordinar y obtener información pertinente de los distintos órganos en Israel y en el exterior.

Funciones y actividades del CERT

01

Manejar incidentes: desde la presentación de informes, asistencia y coordinación del manejo de ciberincidentes, hasta la asistencia en la recuperación e investigación.

02

Manejar vulnerabilidades y artefactos: recepción de los artefactos, realización de investigaciones para comprenderlos, y difusión de métodos y formas de manejarlos.

03

Hacer frente y prevenir amenazas informáticas: a través de actividades proactivas para detectarlos, identificarlos e investigarlos.

04

Desarrollar y difundir conocimientos para la protección de las audiencias objetivo: incluidas las herramientas y tecnologías para el intercambio de información

05

Informar y sensibilizar al público en general, público especializado y profesionales que trabajan en seguridad cibernética.

06

Desarrollar y fomentar de las relaciones con los organismos equivalentes en el mundo: intercambio de información, metodologías de defensa, etc.

Solicitar ayuda para recuperarse es posible. Vea las formas de contacto en el sitio web del INCD:

https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page.





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*

