

# Uso de servicios en la nube

## Adenda a la Metodología de Ciberdefensa para Organizaciones

Mejores Prácticas en Ciberseguridad



# A.03

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 “Uso de servicios en la nube: Adenda a la 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/cloud\\_services](https://www.gov.il/en/Departments/policies/cloud_services). Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

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

# Índice

## Prólogo

/Pág. 2

## Antecedentes

/Pág. 8

## 01. Terminología de los servicios en la nube

/Pág. 10

## 02. Diseño de un plan de seguridad para los servicios en la nube

/Pág. 18

## 03. Controles de seguridad para los servicios en la nube

/Pág. 29

# 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. Prolifera-ron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se de-

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

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

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

## Israel, líder en ciberseguridad a nivel mundial

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

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

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

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

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

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

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

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

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

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

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



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

## El BID y la INCD: uniendo esfuerzos

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

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

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

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

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



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



# Antecedentes

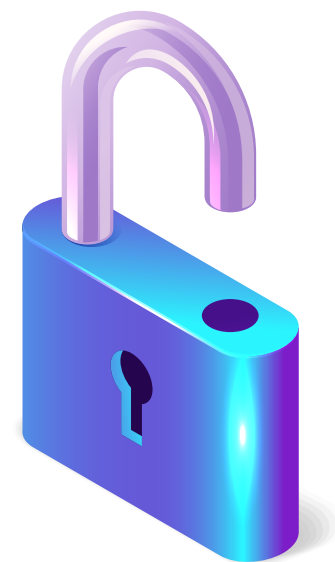
En el ámbito de las tecnologías de la información (TI) hay una tendencia creciente entre las organizaciones y los usuarios finales a recurrir a los servicios en la nube. Esto se percibe en el uso de tecnologías aplicadas que ofrecen esos servicios, tanto mediante nuevas aplicaciones de los fabricantes de aplicaciones en la nube como a través de estrategias comerciales que convierten o cambian la actividad informática existente para operar desde aplicaciones o infraestructuras situadas en la nube.

Una encuesta publicada en febrero de 2017 por Gartner, una empresa líder mundial en encuestas de mercado sobre tecnologías de la información, calcula un aumento del 18% en el uso de los servicios en la nube en 2017 (con un gasto mundial de unos US\$246.800 millones). Gartner anticipa además que para 2020 la mitad de todas las operaciones tercerizadas de servicios de TI se producirán en los servicios en la nube.

Muchas organizaciones están experimentando un cambio fundamental en el uso que hacen de los servicios de TI. Hasta la fecha, la mayoría de las aplicaciones han sido mantenidas, adoptadas y, a veces, desarrolladas por el departamento informático de las organizaciones. Sin embargo, en la actualidad es evidente que las áreas de negocios de las organizaciones están promoviendo canales separados para construir o utilizar servicios de TI a fin de respaldar la actividad comercial mediante un modelo de servicio en la nube.

Actualmente los servicios ofrecidos en la nube son muchos y variados, y cambian a una velocidad vertiginosa. También son muchos y variados los puntos importantes y las implicaciones que deben tener en cuenta los Directores de Seguridad de la Información (CISO, por sus siglas en inglés) al determinar y aplicar medidas de seguridad apropiadas.

Esta publicación está destinada a los CISO y es una adenda a la Metodología de Ciberdefensa para Organizaciones difundida por la Dirección Nacional de Ciberseguridad en 2017.<sup>2</sup> Su objetivo es presentar los métodos de trabajo recomendados a la hora de construir un plan de seguridad, haciendo referencia específicamente a los servicios en la nube que las organizaciones reciben y usan.



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

# /01.

## Terminología de los servicios en la nube



La computación en la nube se refiere a la situación en la que se utilizan recursos remotos de hardware o software a través de una red pública o privada.

**Cuadro 1.** Listado de términos vinculados con la computación en la nube

Término	Explicación
PSN	Proveedor de los servicios en la nube
CSN	Cliente de los servicios en la nube
SSN	Socio de los servicios en la nube
Portabilidad en la nube	La posibilidad de mover una aplicación de información de un proveedor de los servicios en la nube a otro
Computación elástica	El uso de recursos y la posibilidad de ampliarlos o reducirlos según sea necesario
Middleware en la nube	Software que media entre varios proveedores de los servicios en la nube
OpenStack	Software de código abierto que permite la automatización en la creación de un entorno en la nube e incluye una función de almacenamiento y otra de comunicaciones y programas de gestión
PPU	Pago por uso
RTO (siglas en inglés)	Objetivo de tiempo de recuperación de la disponibilidad a la que se compromete el proveedor de los servicios en la nube
SLA (siglas en inglés)	Acuerdo de nivel de servicio: acuerdo acerca del nivel de servicio al que se compromete el proveedor de servicios
Dependencia en exclusiva de un único proveedor de servicios (vendor lock-in)	Tipo de contrato con el proveedor de la nube y la posibilidad de rescindirlo

## Modelos de servicio en la nube

Hay varios modelos de servicio en la nube, entre los que destacan los siguientes:

### 01

**Housing:** si una empresa prefiere ahorrar en la construcción de su propia sala de servidores que cumpla con los estándares más estrictos –como una estructura subterránea reforzada, que requiere una gran inversión en infraestructuras eléctricas, de refrigeración y contra incendios, y otros elementos– puede preferir almacenar su equipo informático en una instalación apropiada de un proveedor conocido, mediante un modelo denominado *housing*. A los clientes se les proporciona el área donde almacenar sus equipos informáticos, electricidad y aire acondicionado, así como protección contra incendios y seguridad física las 24 horas y los siete días de la semana, pero deben adquirir, instalar y mantener el *hardware* por su cuenta.

### 02

**Infraestructura como servicios (IaaS, por sus siglas en inglés):** se trata del modelo de servicio básico y más común para empresas y organizaciones. El objetivo principal es evitar tener que construir salas de computadoras o comprar y mantener equipos de *hardware*, con

instalaciones de almacenamiento, servidores, componentes de comunicaciones y de seguridad de la información, y en su lugar recibir servicios de pago según el uso, basados en un modelo de objetos virtuales que se puede controlar usando una interfaz de servicio.

### 03

**Plataforma como servicio (PaaS, por sus siglas en inglés):** en este modelo, además del *hardware* y la infraestructura, el proveedor de la nube también ofrece al cliente una plataforma de paquetes de *software* básicos para permitir un entorno de desarrollo de aplicaciones, probar los productos del cliente y habilitar servicios informáticos desde la plataforma.

### 04

**Software como servicio (SaaS, por sus siglas en inglés):** en este modelo, el proveedor de la nube suministra *software* e infraestructura, y también las aplicaciones finales del cliente. La aplicación se compra a una empresa especializada en un campo de aplicaciones específico.

### 05

**Datos como servicio (DaaS, por sus siglas en inglés):** en este modelo, la organización consume información de una base de datos

en la nube y la integra en su propio sistema de información. Por ejemplo, una compañía eléctrica que planifica su producción futura puede integrar información sobre el pronóstico del tiempo para los próximos días. La empresa se conecta a la base de datos, que puede almacenarse en la nube, y tomar la información relevante como un servicio de una entidad que la vende. En este caso, la organización debe verificar la información para asegurarse de su fiabilidad.

## Seguridad como servicio

**SECaaS (por sus siglas en inglés):** se trata de un modelo de negocio para usar servicios de seguridad a través de la nube a fin de ahorrar costos de recursos humanos, *hardware*, *software* y licencias. Entre los servicios proporcionados generalmente se incluyen la identificación, el bloqueo de *software* malicioso (*malware*), la prevención de vulneración de las redes, monitoreo y respuestas a incidentes.



## Tipos de implementación

Suele hablarse de cuatro tipos de implementación de la nube:

### 01

**Nube pública:** contexto en el que los servicios en la nube son proporcionados por medio de una infraestructura (*hardware*, *software* y aplicaciones) que se comparte y está abierta a todos, en ocasiones incluso de forma gratuita. Si bien existe una separación y diferenciación lógica y a veces física entre clientes y cuentas, los recursos son compartidos.

### 02

**Nube privada:** situación en la que los servicios en la nube son proporcionados por medio de una infraestructura (*hardware*, *software* y aplicaciones) a la que solo pueden acceder ciertos clientes. En ocasiones la infraestructura se encuentra en las instalaciones propias del cliente y, a veces, en las instalaciones del proveedor de la nube. La comunicación y el acceso a la infraestructura se brindan exclusivamente a un solo cliente, que probablemente tendrá una participación considerable en su administración.



# 03

**Nube comunitaria:** contexto en el que un determinado sector o varias organizaciones con un interés compartido se unen para recibir los servicios en la nube específicos para ellos.

# 04

**Nube híbrida:** situación en la que un cliente usa una nube privada para ciertas aplicaciones y una nube pública para otras a fin de conectar la información o aplicaciones con otras aplicaciones u otra información.

## Arquitecturas posibles

En la computación en la nube, hay dos arquitecturas posibles al optar por la nube:

# 01

**Inquilino único:** dependiendo del tipo de servicio e implementación en la nube, el uso es exclusivo para un cliente y este no lo divide ni comparte con otros usuarios dentro o fuera de la organización. Esto puede abarcar desde el uso de *hardware* hasta el de una aplicación desarrollada exclusivamente para el cliente (generalmente en la implementación de una nube privada).

# 02

**Múltiples inquilinos:** en este caso y según el tipo de servicio e implementación de la nube, el cliente comparte recursos con otros usuarios, a veces dentro de la organización e incluso fuera de ella.

Para llevar a cabo de manera óptima la actividad de una organización con un proveedor de la nube, es necesario que la organización cuente con profesionales específicos. A continuación, en el cuadro 2, se presentan algunos cargos y su descripción. Cada organización contará con ellos en función de sus recursos y su consumo de los servicios en la nube.



## Cuadro 2. Responsables de los servicios en la nube dentro de la organización

Denominación del cargo	Descripción
Responsable de la nube	<p>Administra la actividad de la nube de la organización; está a cargo del mapa de información y los servicios y ubicaciones en la nube; realiza los contratos con los proveedores de la nube (junto con el administrador de adquisiciones de la organización) y presenta a los proveedores de la nube las necesidades en relación con las siguientes dimensiones:</p> <ul style="list-style-type: none"> <li>• Información: método de almacenamiento.</li> <li>• Servicio y disponibilidad requerida, según las necesidades de la empresa.</li> <li>• Caracterización del tráfico de información hacia y desde la nube.</li> </ul>
Administrador de aplicaciones en la nube	Es el responsable de recopilar los requisitos organizativos de las unidades de la organización en materia de aplicaciones en la nube y comunicárselos al responsable de la nube y al CISO.
Especialista en integración de proveedores de la nube	Está a cargo de la seguridad de la información de los canales de transmisión de información, el cifrado de la información y la planificación de la seguridad de la transferencia de información entre la nube y la organización o entre una nube y otra.
Especialista en seguridad de la información en la nube	<p>Se encarga de la seguridad de la infraestructura en el modelo IaaS y de asimilar los componentes de seguridad de la información:</p> <ul style="list-style-type: none"> <li>• A cargo de la seguridad de la información almacenada: responsable del cifrado de datos de desidentificación.</li> <li>• A cargo de la seguridad en relación con el acceso a la información, los sistemas operativos y las bases de datos.</li> <li>• A cargo de otorgar permisos en función de la necesidad de acceder a la información y realizar acciones sobre la información en la nube.</li> </ul> <p>Asegura la codificación en SaaS/PaaS.</p>
Especialista en control de la información en la nube	<p>IaaS: control de topología de red y definición de medios de seguridad de la información.</p> <p>PaaS: control del desarrollo de un código o una aplicación seguros.</p>
Especialista en planificación de la continuidad del negocio	Redacción de procedimientos de continuidad del negocio para aplicaciones e información almacenada en la nube.

# /02.

## Diseño de un plan de seguridad para los servicios en la nube

La necesidad de los servicios en la nube generalmente viene impulsada por las áreas de negocio. A veces, en el proceso de análisis acerca del uso de los servicios en la nube y de su implementación no se recurre al CISO ni al responsable de la nube.

En esta sección se examinan las consideraciones que el CISO y el responsable de la nube, si la organización cuenta con tales cargos, deben tener en cuenta al elaborar un plan de seguridad cuando la organización tiene la intención de comprar los servicios en la nube.

Aquí se presentará el modelo en el que el proveedor de la nube y la organización (el cliente) comparten las responsabilidades, en función de los distintos modelos de servicio, implementación y arquitectura para usar la nube.



### Primera fase: mapeo de activos y recopilación de la información

En esta fase, el CISO debe estudiar y analizar los datos relevantes para los servicios en la nube en la organización.

También debe entender las necesidades de la organización que motivan la intención de contratar los servicios en la nube (excluyen-

do los casos en los que se desea comprar los servicios en la nube por la necesidad de aumentar la seguridad y la protección de la organización).

Es apropiado examinar el tema de la seguridad de los datos desde el punto de vista de una organización que opera en Israel. El CISO debe examinar la esencia de los datos que la organización busca desarrollar, usar o almacenar a través de los servicios en la nube y tener en cuenta los siguientes elementos:

## 01

**Las leyes o reglamentos vinculantes para la organización** (por ejemplo, el reglamento sobre protección de la privacidad de la Autoridad Israelí de Derecho, Información y Tecnología [ILITA, por sus siglas en inglés]), que pueden prohibir o limitar el uso de información en el contexto de los servicios en la nube (por ejemplo, por clasificaciones de seguridad, sensibilidad de la organización o cuestiones de protección de la privacidad), en particular el almacenamiento de datos fuera de las fronteras de Israel.

## 02

**La naturaleza crítica de la disponibilidad de información** para la capacidad de funcionamiento de la organización, así como

la de sus clientes y proveedores y, especialmente en el caso de un sistema cuya actividad es crítica para la economía israelí, en caso de daños a una infraestructura de comunicación que conecta Israel con otros países.

## 03

Determinar si la **exposición de los datos a personal no autorizado** afecta la capacidad de la organización para funcionar, y también la de sus clientes y proveedores.

## 04

Definir si el **daño a la credibilidad de los datos** afectará la capacidad de la organización para funcionar y también la de sus clientes y proveedores.

## 05

Determinar si el **nivel de protección de los datos en los servicios en la nube** ha mejorado en comparación con los servicios que había previamente.

Si es posible, es mejor segmentar y definir los elementos sensibles de la información (por ejemplo, números de tarjetas de crédito, números de identificación).

El CISO debe determinar si el uso de los servicios en la nube incluye algún aspecto operativo que, si se daña, podría afectar de manera inmediata o continua a las operaciones de la actividad principal de la organización (por ejemplo, **una organización cuya actividad principal sea la venta a través de un sitio web almacenado en un servicio en la nube, donde el daño a la disponibilidad comprometería la actividad principal de la organización**).

El CISO debe saber qué tipo de servicio en la nube planea comprar la organización (SaaS, PaaS, IaaS).

Además, debe conocer la información básica del proveedor de la nube con respecto a:

# 01

Si es conocido y es líder en su campo.

# 02

Si cumple con normas de seguridad del servicio tales como las de Cloud Security Alliance (CSA), la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus siglas en inglés), la Organización Internacional de Normalización (ISO, por sus siglas en inglés),

la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés), el Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP, por sus siglas en inglés), el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), etc.

Es necesario redactar un **modelo de responsabilidad compartida** según el tipo de servicio en la nube y su implementación. Tales modelos pueden diferir de un proveedor a otro.

Es importante que la definición de las responsabilidades para la operación, instalación, mantenimiento y protección de cada capa estén claras y se reflejen en un **documento contractual** cuando se redacte el acuerdo.

Las capas deben recogerse en un contrato entre un proveedor de la nube y un cliente, donde **se ha de establecer claramente cuál de las partes es responsable de los aspectos operativos y de protección** (cuadro 3). Según el modelo, las responsabilidades se distribuyen de la siguiente manera:

# 01

**IaaS:** por lo general, el cliente tiene el control y es responsable de muchas capas, desde el nivel de la interfaz de red virtual hasta los datos.

# 02

**PaaS:** por lo general, el cliente tiene el control y es responsable de las capas de las aplicaciones.

# 03

**SaaS:** por lo general, el cliente no tiene control ni responsabilidad, excepto en el tipo de datos y el contenido y las definiciones de la interfaz de usuario; por lo demás, la responsabilidad recae enteramente en el proveedor.

**Cuadro 3.** Capas presentes en un contrato entre el proveedor y el cliente

Capa	Explicación
Información	El tipo y el contenido de los datos que se utilizarán y a los que se puede acceder en el servicio en la nube.
Interfaz de usuario	La forma en que el cliente o quien lo necesite accederá a los datos.
Aplicaciones	Las aplicaciones a través de las cuales los usuarios acceden y pueden usar los datos.
Base de datos	Base de datos para almacenar los datos y las aplicaciones.
Software	Los códigos utilizados para desarrollar y ejecutar aplicaciones.
Sistemas operativos	La plataforma que gestiona los recursos de <i>hardware</i> y <i>software</i> .
Máquinas virtuales	Un entorno de emulación que usará el cliente.
Interfaz de red virtual	Los medios y las definiciones de la comunicación entre máquinas virtuales en el entorno de emulación.
Hipervisor	El <i>software</i> y la interfaz para administrar un entorno de emulación y máquinas virtuales.
Hardware	Los recursos físicos, como la potencia de procesamiento y la memoria, que se asignan para el uso de un cliente.
Almacenamiento	Los recursos físicos asignados a un cliente para guardar y almacenar datos.
Comunicación	La mediación y método que permiten el acceso entre el entorno del cliente y el entorno del proveedor de la nube.
Ubicación física	El lugar donde se encuentran los recursos físicos del proveedor de la nube utilizados por el cliente.

**Cuadro 4.** Distribución de responsabilidades en el modelo IaaS, PaaS y SaaS

Responsabilidad del proveedor	Responsabilidad de la organización
<b>Modelo IaaS</b>	
<ul style="list-style-type: none"> <li>• Proporciona potencia informática en función de lo que el cliente requiere y ha contratado.</li> <li>• Disponibilidad de recursos informáticos durante el período del contrato.</li> </ul>	<ul style="list-style-type: none"> <li>• Establecimiento de la infraestructura, que incluye el sistema de almacenamiento, el sistema de servidor y la definición de las comunicaciones dentro de las organizaciones.</li> <li>• Definiciones del usuario.</li> <li>• Aplicación y disponibilidad a los usuarios.</li> <li>• Desarrollo de aplicaciones, operación y licencias de <i>software</i>.</li> <li>• Protección de los datos almacenados (encriptación, desidentificación).</li> <li>• Continuidad del negocio.</li> </ul>
<b>Modelo PaaS</b>	
<ul style="list-style-type: none"> <li>• Proporciona potencia informática en función de las necesidades del cliente y lo contratado.</li> <li>• Disponibilidad de recursos informáticos durante el período del contrato.</li> <li>• Proporciona una plataforma para el desarrollo y mantenimiento de aplicaciones, tanto en sus diferentes versiones como en cuanto a los parches (es decir, actualizaciones).</li> </ul>	<ul style="list-style-type: none"> <li>• Establecimiento de definiciones de las comunicaciones dentro de las organizaciones.</li> <li>• Definiciones del usuario.</li> <li>• Aplicación y disponibilidad a los usuarios.</li> <li>• Desarrollo de aplicaciones, operación y licencias de <i>software</i>.</li> <li>• Protección de la información almacenada (encriptación, desidentificación, etc.).</li> <li>• Continuidad del negocio.</li> </ul>
<b>Modelo SaaS</b>	
<ul style="list-style-type: none"> <li>• Establecimiento de la infraestructura, que incluye: sistema de almacenamiento, sistema de servidor y definiciones de las comunicaciones dentro de las organizaciones.</li> <li>• Aplicación y disponibilidad a los usuarios.</li> <li>• Desarrollo de aplicaciones, operación y licencias de <i>software</i>.</li> <li>• Protección de los datos almacenados.</li> <li>• Cifrado de datos, si es necesario.</li> <li>• Continuidad del negocio.</li> </ul>	<ul style="list-style-type: none"> <li>• Precisión de la información.</li> <li>• Definiciones del usuario.</li> <li>• Desidentificación de los datos.</li> </ul>

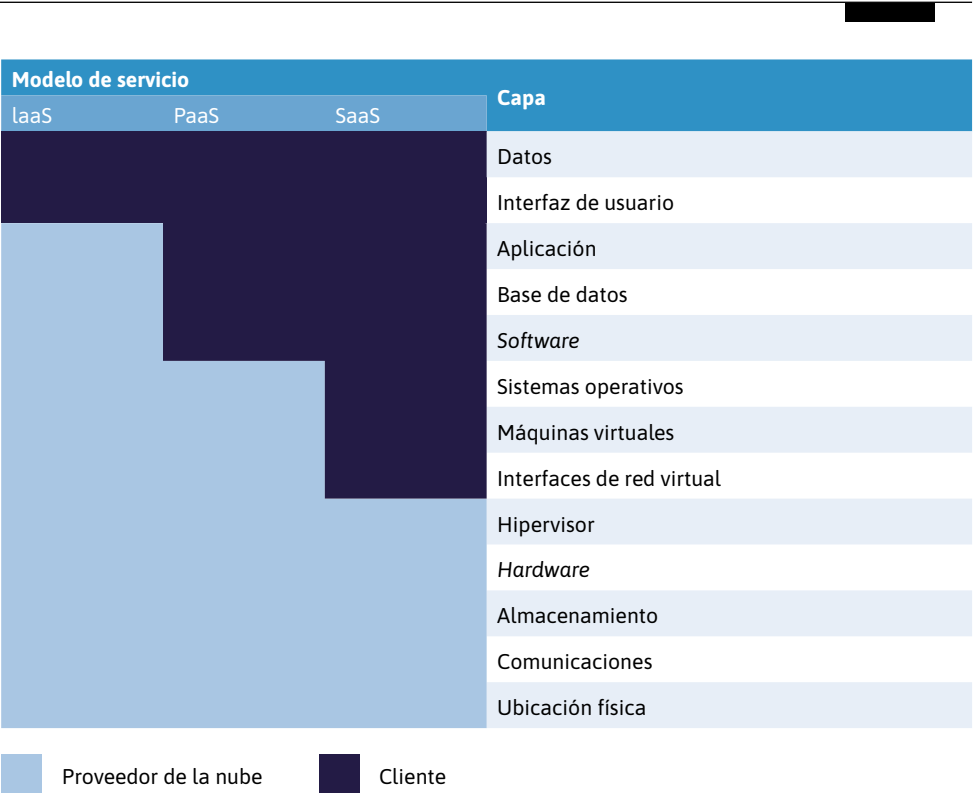


El cuadro 5 presenta un ejemplo del modelo de responsabilidad compartida entre el proveedor de la nube y el cliente según la división en capas (siguiendo el estándar PCI).

Como se indicó anteriormente, es fundamental establecer **un modelo de respon-**

**sabilidad compartida** entre la organización (cliente) y el proveedor de la nube. Sin embargo, esto no exime al CISO de estar familiarizado con los detalles técnicos y los relacionados con el proceso y características de cada una de las capas descritas previamente.

**Cuadro 5.** Ejemplo de modelo de responsabilidad compartida



Incluso en relación con las capas que por contrato son responsabilidad del proveedor de la nube, cuando en el curso del desarrollo

del plan de seguridad de la organización, el CISO debe referirse a las actividades y servicios en la nube que utiliza la organización,

tendrá que conocer y referirse a cada una de las capas y plantear las siguientes preguntas:

**01**  
¿Qué controles son necesarios y apropiados para cada capa?

**02**  
¿Qué controles están disponibles?

**03**  
¿Se puede contar con esos controles pidiéndole al proveedor que los suministre o deberá encargarse de ello la organización, según el modelo de responsabilidad compartida?

**04**  
Si el proveedor no los suministra, ¿hay controles compensatorios que puedan tenerse?

**05**  
Si no hay controles compensatorios, ¿es proporcionado el riesgo de no mantener estos controles?

**06**  
¿Cuál es la ubicación geográfica de la capa, es decir, su ubicación física? En relación con el acceso de la organización, la autoridad legal, las posibles sanciones por razones políticas por tratarse de una organización (cliente) israelí.

**07**  
¿Cuáles de los servicios en la nube son internos y propios del proveedor y cuáles compra a un subproveedor? ¿Quién es el subproveedor?

En este caso también es mejor segmentar por capas. Esto ayudará al CISO a saber qué productos está comprando la organización como parte de su paquete de servicios en la nube en términos de *hardware*, comunicaciones, *software* y aplicaciones. De este modo, puede analizar los riesgos y debilidades conocidos de cada uno de los productos en la fase de planificación y también más adelante, durante la vigencia del contrato de servicio, y, en consecuencia, elegir los controles y las respuestas adecuadas.

El CISO debe estar familiarizado con los eventos pasados, como ataques que puedan estar asociados con el proveedor de los servicios en la nube o sus subproveedores con respecto a los servicios suministrados a la organización.



## Segunda fase: evaluación de riesgos

En este punto, el CISO debe identificar los riesgos que el servicio en la nube representa para la organización en función de la información recopilada y analizada.

Además, debe considerar todos los escenarios relevantes de daños a la organización resultantes del uso de los servicios en la nube.

También debe conocer y referirse a la implementación y arquitectura para usar la nube prevista o existente de acuerdo con el modelo de servicio que se va a comprar.

Como parte de la elaboración del escenario, lo mejor es seleccionar primero la amenaza, es decir, el daño final relevante correspondiente al modelo de servicio y la implementación de la nube.

### Por ejemplo, el análisis del CISO mostró que:

“Los datos almacenados en la base de datos como parte de los servicios en la nube incluyen una lista de las direcciones de envío de los clientes. Cualquier cambio en esos campos y daño a la fiabilidad de los datos pueden causar una gran cantidad de daños operativos y económicos a la organización”. Por lo tanto, el CISO debe analizar los escenarios en los que podrían darse cambios en esos campos.

En la siguiente etapa, el CISO tendrá que **evaluar la probabilidad** de que realmente se dé cada escenario teniendo en cuenta los métodos de control existentes, a fin de examinar la necesidad de controles adicionales con respecto a los siguientes parámetros:

# 01

El nivel de competencias y recursos necesarios para permitir el escenario.

# 02

El nivel de vulnerabilidad de los componentes relevantes que permitirían el escenario.

# 03

El nivel de acceso lógico al activo, dado el modelo de servicio, las implementaciones y la arquitectura para usar la nube.

# 04

El nivel de acceso físico al activo, dado el modelo de servicio, la implementación y la arquitectura para usar la nube.

Tras seleccionar los escenarios para todos los daños finales relevantes, el CISO debe considerar, en orden descendente de preferencia –desde el escenario más probable hasta el menos probable–, los controles que se deben aplicar y si pueden aplicarse o no. Si no es posible, ¿qué alternativas operativas existen, tanto desde una perspectiva organizacional como con relación al modelo de servicio, implementación y arquitectura para usar la nube, que puedan proporcionar una respuesta que cumpla con un nivel razonable de gestión de riesgos?

Volviendo al ejemplo anterior (“cualquier cambio en esos campos y daño a la fiabilidad de los datos pueden causar a la organización una gran cantidad de daños operativos y económicos”), en el cuadro 6 se muestra cómo se vería un modelo de este método de análisis de riesgos.

Cuadro 6. Ejemplo de análisis de riesgos

La amenaza	Daño a la fiabilidad de los datos: cambios en los datos en listas de direcciones de clientes almacenadas en el servidor de la base de datos		
Modelo de servicio en la nube	IaaS		
Implementación de la nube	Público		
Arquitectura para usar la nube	Múltiples inquilinos		

Escenario	Análisis de la probabilidad	Evaluación de la probabilidad	Controles a considerar
Un inquilino diferente obtiene acceso a la lista	<ul style="list-style-type: none"><li>Nivel de especialización y recursos: <b>bajo</b></li><li>Nivel de vulnerabilidad del servidor de base de datos: <b>medio</b></li><li>Nivel de accesibilidad lógica de otros inquilinos: <b>medio</b></li><li>Nivel de accesibilidad física: <b>bajo</b></li></ul>	Medio	<ul style="list-style-type: none"><li>Cifrado: separación mediante cifrado seguro con una administración separada de las claves y a cargo de la organización y no del proveedor de la nube.</li><li>Nube privada virtual (VPC, por sus siglas en inglés): segmentación virtual de entornos creando una nube privada dentro de la nube pública.</li><li>Separación de los usuarios: mediante el uso de componentes físicos separados.</li></ul>

# /03.

## Controles de seguridad para los servicios en la nube

### Agentes de seguridad para el acceso a la nube

Las características y capacidades de los sistemas de CASB son los siguientes:

#### 01

**Exposición:** proporcionan al cliente la capacidad de ver y controlar servicios autorizados y no autorizados y le permiten controlar su ciberseguridad o sistema informático en lugar de bloquear completamente ciertos servicios en la nube, además de administrar y limitar el acceso a la actividad y los datos dentro de los servicios según los permisos de cada usuario o equipo.

Los agentes de seguridad para el acceso a la nube (CASB, por sus siglas en inglés) son sistemas de seguridad y control, algunos de los cuales son vendidos por el proveedor de la nube y otros por terceras empresas. Están ubicados entre el cliente y el proveedor de la nube para permitir la integración o separación de acuerdo con las definiciones de seguridad de la organización (cliente) durante el acceso y uso de las aplicaciones y servicios de la nube por parte del cliente. Proporcionan una respuesta a los riesgos que conllevan los servicios en la nube, hacen cumplir las políticas de seguridad y cumplen los requisitos reglamentarios, aun cuando los servicios en la nube sean externos al sitio del cliente y estén fuera de su control directo.

También permiten exponer una actividad informática invisible en materia de aplicaciones, uso, usuarios, datos o archivos en el entorno de la nube y aplicaciones de terceros conectadas a la nube, incluidos dispositivos móviles y clientes sincronizados.

## 02

**Conformidad:** brindan la opción de verificar si se cumplen los requisitos reglamentarios aplicables a la organización en cuanto a guardar y asegurar la protección y la privacidad de la información del cliente; verifican las aplicaciones y su uso en relación con los requisitos reglamentarios aplicables a la organización; y, al identificar incumplimientos, proporcionan la capacidad de realizar cambios o acciones de prevención para cumplir con dichos requisitos.

## 03

**Protección de datos:** son una aplicación de seguridad en la nube que consta de un mecanismo para identificar y prevenir fugas de datos, como prever la posibilidad de usar huellas digitales para documentos en función de los contextos (usuario, ubicación, actividad, etc.). Permiten administrar permisos, compartir información y generar informes y advertencias a medida, así como cifrar las transferencias de datos.

## 04

**Protección contra amenazas:** permiten escanear, detectar, manejar y bloquear actividades maliciosas o no autorizadas en los servicios en la nube autorizados y no autorizados mediante el uso del análisis de *malware*, ya sea de manera estática o dinámica, identificar anomalías de usuarios y priorizar el manejo de incidentes en función de su gravedad.

### Servicios en la nube de varios proveedores en simultáneo

A veces, las organizaciones eligen o se ven obligadas a usar servicios en la nube de varios proveedores, ya sea por consideraciones de costos, debido a cambios en las aplicaciones requeridas, o también por una política de seguridad en materia de separación y distribución de riesgos.

La sincronización de proveedores supone un desafío. Algunos proporcionan servicios de operaciones de TI y otros ofrecen servicios relacionados con la protección de datos.

Faltan sistemas de control que cumplan con los estándares para servir como interfaces de programación de aplicaciones (API, por sus siglas en inglés) entre los servicios en la nube suministrados por varios proveedores. Por ello, se puede utilizar un *software* de código abierto o recurrir a la gestión de los servicios en la nube de un proveedor externo para administrar el control concentrado a fin de contar con la capacidad de monitorear aplicaciones y servidores, controlar el acceso y hacer cumplir la política.

No todos los proveedores de la nube ofrecen los mismos servicios, y algunos se centran en herramientas de mensajería, flujo de trabajo o administración, lo cual a veces puede hacer que se obtengan bajas prestaciones. Una solución puede ser recurrir a un *software* de terceros, generalmente de código abierto, que permita un servicio alternativo adecuado para los entornos de todos los proveedores de la nube.

Aun cuando se trata de usar servicios estándar similares, puede haber diferencias en la administración del mismo servicio entre los proveedores de la nube. También en tales casos, hay proveedores externos que suministran API específicamente adaptadas para ser usadas con diferentes proveedores de los servicios en la nube.



# Controles de seguridad para organizaciones que usan servicios en la nube

El énfasis en el control hace referencia a los aspectos particulares de los servicios en la nube. Supone una ampliación del capítulo sobre los controles que un CISO debe implementar en el plan de seguridad completo de una organización, tal como se describe en la **Metodología de Ciberde-**

**fensa para Organizaciones** publicada por la Dirección Nacional de Ciberseguridad. En el cuadro 7, la columna de identificación (ID) se refiere al número del control indicado en la Metodología de Ciberdefensa para Organizaciones en el contexto más inmediato, si existe.



Cuadro 7. Tabla de controles

IDENTIFICAR			
Familia	ID	Control	Ejemplo de aplicación de control
Responsabilidad de la Junta Directiva y de la Dirección	3.1.	Velar por la existencia de procesos efectivos	<p>1. Una política organizacional de protección de datos y ciberseguridad respecto de los servicios en la nube de la organización establecidos por la Dirección y el proveedor de la nube: amenazas, escenarios y controles para prevenirlos, procedimientos de recuperación ante desastres y de continuidad del negocio y procesos de identificación y respuesta a incidentes.</p> <p>2. Certificaciones de que el proveedor de la nube cumple con los estándares relevantes para asegurar sus servicios, tales como:</p> <ul style="list-style-type: none"><li>a. Los pilares fundamentales son la <b>norma ISO 27001</b> de la Organización Internacional de Normalización, que define los principios para establecer, administrar y mantener sistemas de seguridad de datos adecuados para las organizaciones, y la <b>SOC 2</b>, una norma formulada por el Instituto de Contadores Públicos de los Estados Unidos (AICPA, por sus siglas en inglés), que prueba los controles de seguridad a fin de mantener la disponibilidad, fiabilidad y confidencialidad de los datos en las organizaciones.</li><li>b. <b>CSA STAR</b>: considerada una certificación líder en este campo. Consta de tres niveles, el segundo de los cuales se centra en mantener la ISO 27001 y la matriz de mejores prácticas de monitoreo continuo de controles (CCM, por sus siglas en inglés).</li><li>c. <b>ISO 27017 y 27018</b>: son normas emitidas por la Organización Internacional de Normalización que definen los controles de seguridad y privacidad en los servicios en la nube.</li><li>d. <b>Estándar de seguridad de datos de la industria de tarjetas de pago (PCI-DSS, por sus siglas en inglés)</b>: estándar de las compañías de tarjetas de crédito para proteger datos y transacciones de crédito, expuesta en el documento titulado <i>Cloud Computing Guidelines</i>.</li></ul>
	3.2.	relacionados con el cumplimiento de las políticas y normas de gestión de riesgos	



IDENTIFICAR			
Familia	ID	Control	Ejemplo de aplicación de control
Responsabilidad de la Junta Directiva y de la Dirección	3.1.	Velar por la existencia de procesos efectivos	e. <b>NIST-SP 800-144:</b> controles de seguridad para los servicios en la nube emitidos por el NIST de los Estados Unidos que las organizaciones federales de ese país deben implementar en virtud de la Ley Federal de Modernización de la Seguridad de la Información (FISMA, por sus siglas en inglés) para obtener una licencia de operador.
	3.2.	relacionados con el cumplimiento de las políticas y normas de gestión de riesgos	f. <b>FedRAMP:</b> se trata de un programa federal estadounidense de evaluación de riesgos, permisos y control de los servicios en la nube (relevante para la actividad de la empresa en los Estados Unidos, especialmente ante los organismos gubernamentales).  g. <b>ILITA:</b> Reglamento de Protección de Privacidad 7809, que define la seguridad de las bases de datos.  h. <b>Reglamento General de Protección de Datos de la Unión Europea (RGPD UE):</b> normas de protección de la privacidad emitidas por la Unión Europea.  i. <b>HIPAA:</b> ley aplicable en los Estados Unidos que tiene como objetivo principal proteger la privacidad y asegurar la confidencialidad de los datos médicos.
Compatibilidad		Aplicar la política de privacidad	3. Acuerdo jurídico que realiza el asesor jurídico del cliente en el que se define claramente la responsabilidad del proveedor de la nube en materia de protección de los datos que permiten la identificación personal, y en el que se debe hacer referencia a la compensación por daños o pérdidas.  4. Hacer que el proveedor de la nube firme los acuerdos de protección de privacidad de los reguladores relevantes.  5. Separar bases de datos: los datos almacenados en el servicio en la nube que contengan listas anónimas y datos que revelen una identificación personal vinculada con listas anónimas deben almacenarse en las instalaciones del cliente o del proveedor de la nube de una manera más segura.

## IDENTIFICAR

Familia	ID	Control	Ejemplo de aplicación de control
Control y auditorías	3.4.	Realizar auditorías de los procesos operativos y de la organización	<p>6. Recibir informes de auditoría del proveedor de la nube, tales como auditorías realizadas por una institución auditora independiente de los procesos operativos y de la organización en relación con los servicios ofrecidos, con el objeto de entender los controles de seguridad que el proveedor de la nube aplica en el marco de sus servicios, con énfasis en los siguientes temas:</p> <ul style="list-style-type: none"> <li>a. Controles de seguridad que garantizan la separación de las aplicaciones y los datos del cliente de los datos de otros clientes en un entorno de múltiples inquilinos.</li> <li>b. Controles de seguridad para prevenir el acceso no autorizado por parte de los trabajadores del proveedor de la nube a los datos y aplicaciones del cliente (por ejemplo, SOC 2).</li> </ul> <p>7. Asegurarse de que también haya auditorías para proporcionar seguridad en las medidas de autoservicio, además de los servicios que ofrece el proveedor de la nube, por ejemplo, un medio de registrarse para el servicio o los procedimientos de pago. Dichas medidas de autoservicio para clientes suelen ser más vulnerables que el servicio en sí, por lo que es necesario asegurarse de que las auditorías también las incluyan.</p>

## PROTECCIÓN

Cadena de suministro y externalización	16.2.	Usar herramientas legales y contractuales para definir las responsabilidades del proveedor y del cliente de la nube	<p>8. Un contrato de servicio vinculante que especifica la división de responsabilidades del proveedor y del cliente de la organización. Se pueden especificar las responsabilidades a nivel de las capas. La responsabilidad debe referirse a la protección y seguridad de la capa, a las operaciones y al manejo de percances.</p> <p>9. El contrato de servicio debe incluir la ubicación de los datos (físicos, especificando los países), las leyes aplicables y un compromiso de que los datos no serán trasladados a una jurisdicción diferente sin el conocimiento del cliente.</p>
--	-------	---	---

PROTECCIÓN			
Familia	ID	Control	Ejemplo de aplicación de control
Cadena de suministro y externalización	<b>16.2.</b>	Usar herramientas legales y contractuales para definir las responsabilidades del proveedor y del cliente de la nube	10. El contrato también debe incluir una referencia a cada subproveedor que brinde servicios al proveedor principal en el contexto de los servicios proporcionados en la nube.
			11. El contrato de servicio debe indicar la obligación del proveedor de la nube de informar al cliente acerca de cualquier penetración en la red, descubrimiento de <i>malware</i> , percances, fallas y cualquier tipo de incidente que ponga en riesgo o afecte los datos del cliente y su capacidad funcional en relación con los servicios en la nube suministrados.
			12. Con respecto a la presentación de la información, el contrato debe especificar horarios, procedimientos de la provisión de información, la parte responsable del incidente como parte del establecimiento de índices de indemnización y compensación al cliente, si fuera necesario.
			13. Un ejemplo de contrato de servicio es el de la CSA: Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union. (Acuerdo de nivel de privacidad para la venta de servicios en la nube en la Unión Europea). Disponible en: <a href="https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf">https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf</a>
Control de acceso del personal	<b>4.6.</b> <b>4.7.</b> <b>4.29.</b> <b>4.34.</b> <b>19.10.</b>	Realizar la gestión del personal, sus funciones e identidades	14. Para los clientes cuyas organizaciones tienen un sistema de gestión de identidad y permisos, se recomienda ampliar su uso en el contexto del acceso a los servicios en la nube, tanto desde el punto de vista de la eficiencia como del control cuando se produce un cambio de puesto o el despido de un empleado.
			15. El cliente debe tener permisos para administrar las identidades y permisos de los usuarios.
			16. El cliente debe describir cómo se produce la sincronización cuando se crea un nuevo usuario, prestando especial atención a los puestos temporales, los cambios en los usuarios actuales y el cierre de las cuentas de usuarios que dejan de trabajar en la organización. Los percances en la sincronización pueden dar lugar a riesgos de exposición de datos.

## PROTECCIÓN

Familia	ID	Control	Ejemplo de aplicación de control
Control de acceso del personal	4.6. 4.7. 4.29. 4.34. 19.10.	Realizar la gestión del personal, sus funciones e identidades	<p>17. El cliente debe tener la capacidad de ejecutar un ingreso y cierre de sesión de un usuario en un solo proceso (federación de directorio activo) para garantizar que se desconecte de todos los servicios en la nube, adquiriendo identidad como servicio (IDaaS, por sus siglas en inglés).</p> <p>18. Auditorías y registros de acceso y uso por parte de los usuarios de los servicios en la nube, incluida la identificación del usuario al iniciar sesión (nombre de usuario, estaciones donde se realizó el inicio de sesión, fallas de inicio de sesión, acceso o falla de acceso a áreas compartimentadas), recuperación o eliminación de datos, como impresión, etc.</p> <p>19. Soporte con mecanismos de identificación sólidos y complejos, como identificación de dos pasos y de varias etapas, identificación biométrica, etc.</p> <p>20. La capacidad del cliente para describir y hacer cumplir, en el contexto del acceso a los servicios en la nube, la gestión de funciones y grupos en la organización con base en la política de seguridad bajo la cual opera.</p> <p>21. Limitación del acceso en función de las posiciones, direcciones de red, el control de acceso al medio (MAC, por sus siglas en inglés) y la ubicación geográfica.</p>
Proteger la información	5.2. 5.3. 5.4. 5.5.	Segmentar y clasificar los datos a fin de implementar la seguridad adecuada	<p>22. Crear una lista de activos de datos: identificar los activos, clasificarlos según su importancia para el cliente o la regulación aplicable, definir a los propietarios y su responsabilidad por problemas relacionados con los datos, la ubicación de los datos y el acceso a los mismos.</p> <p>23. Para todos los tipos de datos:</p> <p>a. Datos estructurados (planificación de recursos empresariales [ERP, por sus siglas en inglés], gestión de relaciones con los clientes [CRM, por sus siglas en inglés]) almacenados en las bases de datos en un entorno de múltiples inquilinos: seguridad por separación y aislamiento o mezcla en la base de datos, uso de cifrado para asegurar la base de datos.</p>

PROTECCIÓN			
Familia	ID	Control	Ejemplo de aplicación de control
Proteger la información	5.2. 5.3. 5.4. 5.5.	Segmentar y clasificar los datos a fin de implementar la seguridad adecuada	<p>b. Datos no estructurados (imágenes, documentos escaneados y archivos multimedia) pueden ser confidenciales y deben editarse o estar protegidos (firmas, domicilios y otros datos personales).</p> <p>24. En cuanto a la privacidad de los datos, tener en cuenta los requisitos legales y reglamentarios sobre el acceso, almacenamiento y uso de datos que permiten la identificación personal. Establecer límites en el acceso a los datos y en su uso, marcar los datos como tales, almacenarlos de manera segura haciendo referencia, por ejemplo, a la ubicación geográfica y proporcionar acceso exclusivamente a los usuarios autorizados.</p> <p>25. Establecer la confidencialidad, fiabilidad y disponibilidad de los datos: usar aplicaciones que puedan clasificar datos, encriptar datos confidenciales durante el almacenamiento y la transmisión. En relación con el almacenamiento separado de claves de encriptación, usar técnicas de verificación de datos como la transformación de claves o <i>hashing</i>, con copias de respaldo y aplicaciones de recuperación rápida.</p> <p>26. Aplicar mecanismos de identificación y permiso de acceso a datos y recopilación de historial y registros de acceso para su uso con fines de auditorías e investigaciones.</p> <p>27. Monitorear acciones de transferencia de datos entre el cliente y el proveedor de la nube para reducir/prevenir las transferencias de datos no autorizadas por medio de:</p> <ul style="list-style-type: none"> <li>a. El monitoreo de la actividad de la base de datos (MABD).</li> <li>b. El monitoreo de la actividad de los archivos (MAA).</li> <li>c. El filtrado de URL.</li> <li>d. La prevención de la pérdida de datos (PPD).</li> </ul> <p>28. Usar algoritmos de detección de intrusos, los cuales dividen los datos en varias partes y almacenan cada una en un servidor de almacenamiento diferente.</p> <p>29. En el modelo IaaS, cifrar volúmenes como protección contra la duplicación y el acceso no autorizado.</p>



PROTECCIÓN			
Familia	ID	Control	Ejemplo de aplicación de control
Seguridad de la red	7.1.	Filtrar, identificar y separar para proteger el tráfico de red	<p>30. Filtrar el tráfico de red utilizando aplicaciones tales como cortafuegos (<i>firewall</i>), si el proveedor ofrece dicho servicio (generalmente administrado por el cliente).</p> <p>a. Requerir que el proveedor de la nube proporcione una lista de puertos abiertos.</p> <p>b. Con respecto al filtrado del tráfico de red, utilizar también IPv6, no solo el protocolo IPv4.</p>
Prevención del código malicioso	7.6.		
	9.3.		
	9.9.		
	9.24.	Filtrar, identificar y separar para proteger el tráfico de red	<p>31. Proteger contra ataques de denegación de servicio distribuido (DDOS, por sus siglas en inglés): la capacidad del proveedor de la nube y de su proveedor de Internet para manejar el tráfico de red de alto volumen –por ejemplo, identificar un ataque a gran escala contra el proveedor, identificar un ataque a pequeña escala centrado en el servidor del cliente–, generación de advertencias automáticas de un ataque, uso de cortafuegos de aplicaciones web (WAF, por sus siglas en inglés), capacidad de llevar a cabo un análisis posterior al ataque.</p> <p>32. Uso de <i>software</i> de escaneo actualizado para protegerse contra el <i>malware</i>, proporcionado por el proveedor de la nube o por terceros con una API adecuada para los servicios del proveedor:</p> <p>a. A nivel del sistema operativo de las estaciones finales y servidores: antivirus actualizado y administrado continuamente. En los modelos SaaS y PaaS, esta responsabilidad es del proveedor; en el IaaS, es del cliente.</p> <p>b. Filtrar el tráfico de comunicaciones: uso de sistemas de detección y prevención de intrusos (IDS/IPS, por sus siglas en inglés), WAF; es responsabilidad del proveedor en todos los modelos.</p> <p>c. Filtrar el tráfico, recibir archivos en correos electrónicos y navegar: SandBox, MailRelay. En SaaS y PaaS es responsabilidad del proveedor; en IaaS, del cliente.</p> <p>d. Navegación: filtrar mediante filtrado de URL y proxy; es responsabilidad del proveedor en todos los modelos.</p>
Separación de entornos	10.2.		
	10.8.		
	10.9.		

PROTECCIÓN			
Familia	ID	Control	Ejemplo de aplicación de control
Seguridad de la red	<b>7.1.</b>	Filtrar, identificar y separar para proteger el tráfico de red	<p>33. Registros y actualizaciones:</p> <p>a. El proveedor de la nube otorga la capacidad para ver la integridad de la red a través de un sistema o interfaz, en tiempo real.</p> <p>b. Establecer los escenarios para manejar incidentes (como ataques) y procedimiento para informar al cliente: definición de los tipos de incidentes que el proveedor de la nube debe informar al cliente, por ejemplo, la identificación de código malicioso en el servidor del cliente o de comunicaciones maliciosas del servidor del cliente al servidor del atacante (servidor de mando y control), cómo se maneja el incidente, ayuda para evaluar el daño y acciones para repararlo y asegurar el sistema a fin de evitar su repetición.</p> <p>c. Tener en cuenta las limitaciones legales para recopilar y almacenar registros en relación con la protección de la privacidad.</p> <p>d. El cliente debe indicar al proveedor de la nube qué registros debe hacerle llegar y por qué medio con el fin de realizar una investigación independiente de los incidentes.</p> <p>34. Herramientas y medios para separar a unos clientes de otros y a los clientes de Internet:</p> <p>a. Segmentación de la red mediante la separación de la red de área local virtual (VLAN, por sus siglas en inglés).</p> <p>b. Tráfico cifrado: conexión a un servicio de sitio a sitio o de cliente a sitio mediante una red privada virtual (VPN, por sus siglas en inglés), uso de cifrado como seguridad de protocolo de Internet (IPsec, por sus siglas en inglés), seguridad de la capa de transporte/capa de conexiones seguras (TLS/SSL, por sus siglas en inglés).</p> <p>c. Cortafuegos para filtrar el tráfico entre las VLAN.</p> <p>d. Filtrado del tráfico de red por parte del proveedor, por ejemplo, utilizando hipervisor o ebttables (software de Linux para filtrar el tráfico de red).</p>
Prevención del código malicioso	<b>7.6.</b> <b>9.3.</b> <b>9.9.</b> <b>9.24.</b>		
Separación de entornos	<b>10.2.</b> <b>10.8.</b> <b>10.9.</b>		

PROTECCIÓN			
Familia	ID	Control	Ejemplo de aplicación de control
Seguridad de la red	<b>7.1.</b>	Filtrar, identificar y separar para proteger el tráfico de red	35. Endurecimiento de máquinas y servidores virtuales, como servicios de bloqueo y cancelación, utilizando sistemas de administración de parches para actualizar los parches de seguridad. En los modelos SaaS y PaaS es responsabilidad del proveedor; en el modelo IaaS, del cliente.
Prevención del código malicioso	<b>7.6.</b>		
	<b>9.3.</b>		
	<b>9.9.</b>		
Separación de entornos	<b>9.24.</b>	10.2. 10.8. 10.9.	36. Protección de la red interna del proveedor de la nube: el cliente debe asegurarse de que el proveedor de la nube aplique auditorías de seguridad de su propia red interna, muestre los hallazgos de los informes de auditoría realizados por terceros o tenga pruebas de que cumple con los estándares regulatorios relevantes.
	<b>10.2.</b>		
	<b>10.8.</b>		
	<b>10.9.</b>		
Protección física y ambiental	<b>18.8.</b>	Realizar auditorías de seguridad de medios físicos y sitios	37. Análisis de los riesgos existentes de la ubicación geográfica y física donde el proveedor de la nube almacena los datos, en relación con desastres naturales, nivel de delincuencia y nivel de malestar social o político.
	<b>18.15.</b>		
	<b>18.17.</b>		
	<b>18.19.</b>		
	<b>18.20.</b>		
			38. Aplicación de auditorías de filtrado y prevención de acceso físico por parte de personal no autorizado a los sitios del proveedor de la nube que almacenan medios e infraestructuras que sirven al cliente en el contexto de los servicios en la nube: un sitio definido, guardias, control de entrada electrónica, monitoreo por cámaras, alarmas electrónicas, etc.
			39. Aplicación de medios de control de prevención y reducción de daños posterior a eventos externos o ambientales: condiciones climáticas extremas, inundaciones, incendios, terremotos, cortes de electricidad, etc. Por ejemplo, prueba de cumplimiento de la norma israelí 1243 de Seguridad contra incendios de computadoras y equipos periféricos o ISO 27001, que define la extinción de incendios con gas en salas de servidores y paneles eléctricos, sensores de temperatura, soluciones de drenaje, sistema de alimentación ininterrumpida o generador, etc.
			40. Aplicación de controles contra robo, pérdida, daño malicioso y vandalismo contra medios e infraestructuras relevantes para los proveedores de la nube: controles electrónicos de entrada, guardias, monitoreo por cámaras, alarmas electrónicas, cerraduras, etc.

PROTECCIÓN			
Familia	ID	Control	Ejemplo de aplicación de control
Protección física y ambiental	<b>18.8.</b> <b>18.15.</b> <b>18.17.</b> <b>18.19.</b> <b>18.20.</b>	Realizar auditorías de seguridad de medios físicos y sitios	41. Controles preventivos contra pérdida o filtración de datos en caso de descarte o reutilización de equipos de almacenamiento de datos: gestión de inventario, uso de compañías que desechan y trituran equipos electrónicos y medios magnéticos, limpieza profunda de memorias no volátiles.
DETECTAR			
Registro y monitoreo	<b>21.4.</b> <b>21.5.</b> <b>21.12.</b>	Recibir advertencias e informes del proveedor de la nube	<p>42. Acceso del cliente a las advertencias por parte de los sistemas de control de seguridad del proveedor de la nube, por ejemplo: un sistema de gestión de la información y eventos de seguridad para identificar una sospecha de un incidente malicioso.</p> <p>43. Recibir informes del proveedor de la nube de cada incidente que presente un riesgo de daño a los activos del cliente, incluidos los registros que permitan el análisis forense del incidente:</p> <ul style="list-style-type: none"> <li>a. Identificación del sistema cuyo sensor informó al sistema de gestión de información y eventos de seguridad, regla de este sistema que generó la emisión de la advertencia.</li> <li>b. Pruebas y análisis para verificar o encontrar la fuente de la alerta.</li> <li>c. Cambios para evitar recurrencias, etc.</li> </ul> <p>44. Recibir informes analíticos del proveedor de la nube en relación con la verificación, los permisos y la gestión de los datos con respecto a las aplicaciones y los datos utilizados por el cliente frente a los controles de seguridad que aplica el proveedor de la nube.</p>
RESPONDER			
Gestión de eventos e informes	<b>24.3.</b>	Articular un plan de respuesta a incidentes con el proveedor	<p>45. Asegurarse de que el proveedor de servicios tenga un servicio de respuesta a incidentes que cubra los siguientes aspectos:</p> <ul style="list-style-type: none"> <li>a. Identificación de incidentes: cómo se identifican los incidentes, si hay monitoreo las 24 horas, si el análisis de la identificación lo realiza un analista o se hace por medios tecnológicos automatizados.</li> </ul>

RESPONDER			
Familia	ID	Control	Ejemplo de aplicación de control
Gestión de eventos e informes	24.3.	Articular un plan de respuesta a incidentes con el proveedor	<p>b. Personal especializado para manejar incidentes: el proveedor declara el nivel de conocimiento profesional de su personal y la actitud del personal con respecto al número de incidentes y clientes del proveedor.</p> <p>46. Determinar por escrito la manera, los horarios y los tipos de incidentes sobre los que se emitirán informes: por ejemplo, recibir un informe de un incidente que ha afectado la confidencialidad, la integridad o la disponibilidad (o a más de una de ellas simultáneamente), o que ha producido filtraciones, interrupciones o acceso a datos y servicios relevantes para el cliente; cómo el proveedor maneja una sospecha de un incidente que no fue refutada en 24 horas, etc.</p> <p>47. Determinar por escrito la manera, la fase y el tipo de incidente que se informará al equipo de respuesta del cliente para manejar un incidente: se tendrá en cuenta la capacidad del cliente para proporcionar un equipo de respuesta y la disposición del proveedor para permitirlo. Esto es relevante en particular para el modelo IaaS.</p>

RECUPERAR			
Continuidad del negocio	25.1. 25.10. 25.14. 25.17. 25.19.	Implementar planes de respaldo y recuperación por parte del proveedor de la nube en caso de accidente o daño	<p>48. Asegurarse de que el proveedor de la nube tenga un plan de continuidad del negocio por escrito y de la recuperación de la empresa ante un desastre (plan de recuperación ante desastres [PRD]) y si la organización ha sido alcanzada o no.</p> <p>49. Asegurarse de que el proveedor tenga un sitio de recuperación ante desastres donde se realicen copias de respaldo calientes (en tiempo real) o frías (programadas regularmente) en función de la definición de la necesidad y la naturaleza crítica de los datos para el cliente.</p> <p>50. Verificar la ubicación física de la recuperación ante desastres y examinar si existen en el sitio limitaciones regulatorias, peligro gubernamental o riesgos asociados con la situación política y de seguridad del país que puedan afectar la disponibilidad y el estado operativo del sitio.</p>



RECUPERAR			
Familia	ID	Control	Ejemplo de aplicación de control
Continuidad del negocio	25.1. 25.10. 25.14. 25.17. 25.19.	Implementar planes de respaldo y recuperación por parte del proveedor de la nube en caso de accidente o daño	51. Elaborar un SLA para retomar el servicio y volver a estar en línea para reconstruir las copias de respaldo, con base en el análisis del cliente de la naturaleza crítica de la disponibilidad del servicio o de los datos (en minutos, horas, días); definir prioridades con el proveedor en función de las tarifas y su capacidad técnica.
	11.2	Definir el proceso de finalización del servicio	<p>52. En el contrato, definir el periodo de notificación que ambas partes deben respetar antes de finalizar la relación, generalmente de 30 días.</p> <p>53. El cliente debe tener un plan previo sobre qué necesita para transferir los datos o el servicio (en caso de que sea necesario un servicio continuo) a otro proveedor de la nube, dentro del tiempo de notificación, y sobre cómo hará esa transferencia.</p> <p>54. Es necesario definir, con anticipación y junto con el proveedor, una forma segura de transferir los datos almacenados en los servidores del proveedor de la nube al cliente al final del contrato, con base en las necesidades y petición del cliente, por ejemplo: transferencia física de medios de almacenamiento o uso de comunicaciones cifradas, en función de la cantidad y el tipo de datos.</p> <p>55. Estipular en el contrato que el proveedor de la nube está obligado a guardar, durante un periodo de uno a tres meses, los datos del cliente para garantizar que la copia transmitida al cliente sea utilizable y no esté corrompida.</p> <p>56. Estipular que el borrado de los datos ocurrirá solo después de recibir el permiso por escrito del cliente y que el proveedor no podrá proceder al borrado unilateralmente.</p> <p>57. En general, es necesario definir por adelantado con el proveedor de la nube la forma en que se borrarán los datos, las copias de respaldo, los registros y los informes de auditoría cuando el contrato finalice, de manera tal que se garantice que los datos del cliente no puedan restaurarse y que no haya riesgo de que se filtren a una persona no autorizada, que pueda volver a registrarlos en el disco de almacenamiento.</p> <p>58. Recibir una declaración oficial por escrito del proveedor de que los datos han sido borrados utilizando un mecanismo previamente decidido junto con el cliente.</p>



La presente publicación supone una **ampliación** de la **Metodología de Ciberdefensa para Organizaciones** difundida por la Dirección Nacional de Ciberseguridad, y ofrece contenido profesional detallado y complementario sobre el tema de la ciberseguridad.

En estas páginas se presentan algunos antecedentes sobre el tema y su contexto en relación con la ciberseguridad. Además, se proporcionan métodos de trabajo apropiados para su utilización, con el fin de fortalecer y aumentar la ciberseguridad.

Esta publicación se dirige a los CISO y constituye una herramienta y guía auxiliar para construir un plan de seguridad organizacional. No se destina a los fabricantes de productos de seguridad ni pretende exponer las mejores prácticas para fortalecer la seguridad mediante definiciones técnicas. Para ello, se recomienda utilizar los documentos de los fabricantes o el documento sobre mejores prácticas de la Dirección Nacional de Ciberseguridad.

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*

