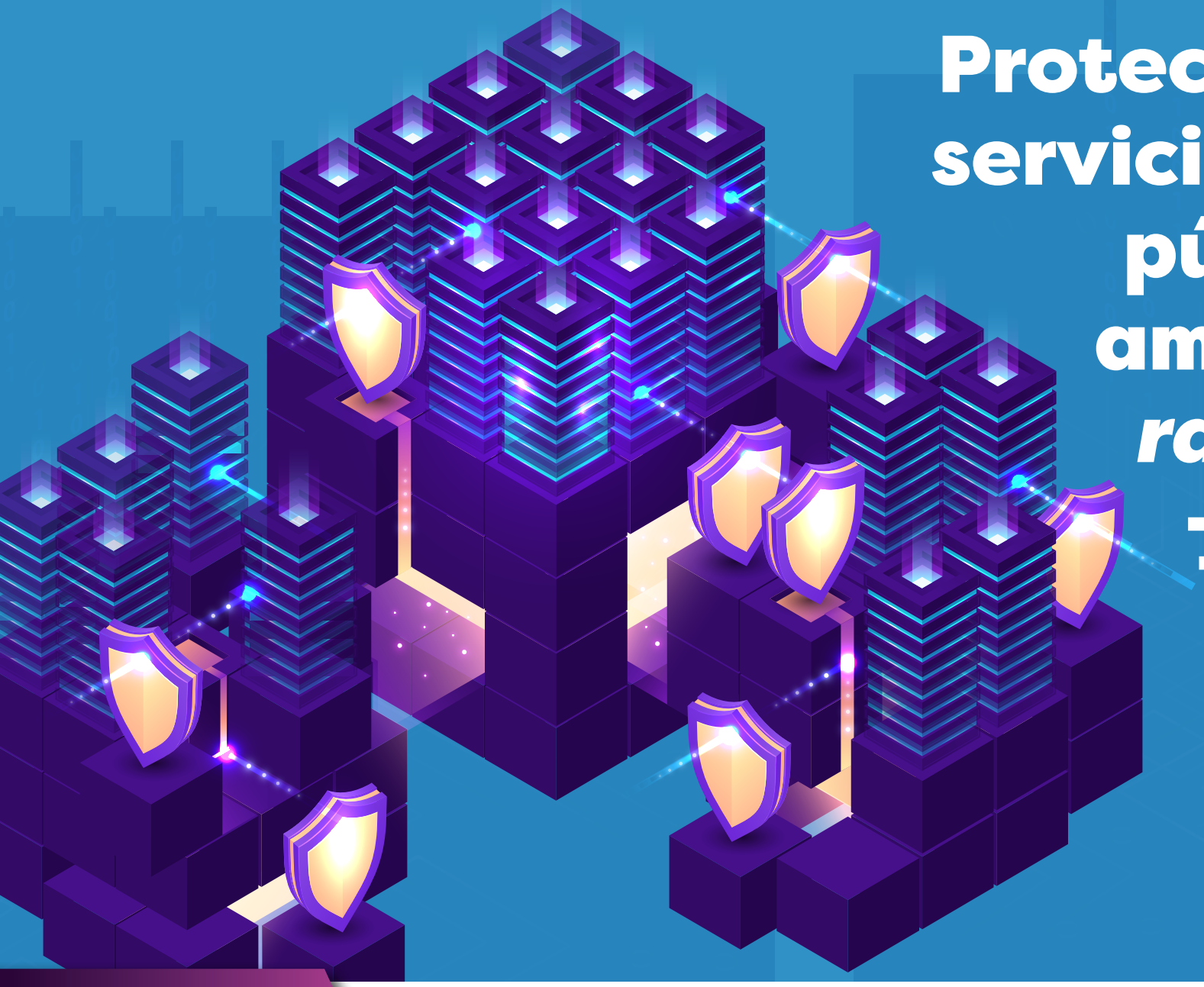


Protección de los servicios de nube pública ante amenazas de *ransomware*

Mejores Prácticas en Ciberseguridad

B.22

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Clasificaciones JEL: D82, H12, K24, L86, L96, M12, M15, O2, O20, O21, O33.

Palabras clave: Ciberseguridad, amenazas cibernéticas, rasomware, protección de datos, cifrado de información, secuestro de información, securización de sistemas, respuesta a incidentes, copias de seguridad, nube.

Publicado originalmente por la Dirección Nacional de Ciberseguridad de Israel en idioma hebreo bajo el título *Aseguramiento de los servicios en la nube pública frente a la amenaza de secuestro de datos (ransomware)*.

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).

El documento original se encuentra disponible en el siguiente enlace: **https://www.gov.il/he/pages/alert_1810**. 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

La transformación digital y el reto de la ciberseguridad

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

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

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/quienes-somos/topicos/modernizacion-del-estado/datos-y-gobierno-digital**

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 organizaciones 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.

Listado de siglas

Sigla	Definición
AD	*Active Directory*
AD FS	Servicios de federación de *Active Directory*
AIBOM	Lista de materiales de IA
AiTM	Adversario en el medio
API	Interfaz de programación de aplicaciones
AS-REP	Respuesta del servidor de autenticación
ASVS	Estándar de verificación de seguridad en aplicaciones
ATT&CK	Tácticas, técnicas y conocimientos comunes de los adversarios
AWS	*Amazon Web Services*
BCP	Plan de continuidad del negocio
BYOD	Traiga su propio dispositivo
C2	Comando y control
CAF	Marco de adopción de la nube
CASB	Agente de seguridad de acceso a la nube
CD	Entrega continua
CI	Integración continua
CIS	Center for Internet Security
CISA	Agencia de Ciberseguridad y Seguridad de las Infraestructuras
CMM	Modelo de madurez de capacidades
CSA	Cloud Security Alliance
CSC	Cliente de servicios en la nube
CSP	Proveedor de servicios en la nube
CSPM	Gestión de posturas de seguridad en la nube
CTI	Inteligencia sobre ciberamenazas
CWPP	Plataforma de protección de la carga de trabajo en la nube
D3FEND	Marco de detección, denegación y disrupción que potencia la defensa de la red
DDoS	(Ataque) distribuido de denegación de servicio
DevSecOps	Desarrollo, seguridad y operaciones
DISA	Agencia de Sistemas de Información de Defensa
DLP	Prevención de fugas de datos
DNS	Servidor de nombres de dominio
DR	Recuperación ante desastres
DRP	Plan de recuperación ante desastres
DSPM	Gestión de posturas de seguridad de datos
ENISA	Agencia de la Unión Europea para la Ciberseguridad
FedRAMP	Programa Federal de Gestión de Riesgos y Autorizaciones
FIDO	Identidad rápida en línea
FinOps	Operaciones financieras
GCP	*Google Cloud Platform*
GW	*Gateway*
H2M	De humano a máquina
HSM	Módulo de seguridad de *hardware*
IA	Inteligencia artificial
IaaS	Infraestructura como servicio
IaC	Infraestructura como código
IAM	Gestión de identidades y accesos
IEC	Comisión Electrotécnica Internacional
IMDS	Servicio de metadatos de instancia
IR	Respuesta a incidentes
ISO	Organización Internacional de Normalización
KMS	Servidor de gestión de claves
LDAP	Protocolo ligero de acceso a directorios
LOTS	Vivir de sitios de confianza

Sigla	Definición
M2M	Máquina a máquina
MASVS	Estándar de verificación de seguridad en aplicaciones móviles
MFA	Autenticación multifactor
NIST	Instituto Nacional de Normas y Tecnología
NTLM	NT LAN Manager
OCI	*Oracle Cloud Infrastructure*
OS	Sistema operativo
OWASP	Proyecto abierto de seguridad en aplicaciones web
PaaS	Plataforma como servicio
PET	Tecnologías de mejora de la privacidad
PII	Información de identificación personal
RDDoS	(Ataque) DDoS de rescate
RDP	Protocolo de escritorio remoto
RMM	Supervisión y gestión remotas
S3	Servicio de almacenamiento simple
SaaS	*Software* como servicio
SaaSBOM	Lista de materiales de *software* como servicio
SAML	Lenguaje de marcado para confirmaciones de seguridad
SASE	Servicio de acceso seguro Edge
SBOM	Lista de materiales de *software*
SCA	Análisis de composición de *software*
SIEM	Gestión de eventos e información de seguridad
SLA	Acuerdo de nivel de servicio
SOAR	Orquestación, automatización y respuesta de seguridad
SOC	Centro de operaciones de seguridad
SoD	Separación de funciones
SRM	Modelo de responsabilidad compartida
SSH	*Secure Shell*
SSO	Inicio de sesión único
SSPM	Gestión de posturas de seguridad de SaaS

Sigla	Definición
SSRF	Falsificación de solicitudes del lado del servidor
STAR	Seguridad, confianza, garantía y riesgo
STIG	Guías de implementación técnica de seguridad
TIC	Tecnologías de la información y las comunicaciones
TTP	Tácticas, técnicas y procedimientos
URL	Localizador uniforme de recursos
VPC	Nube privada virtual
VPN	Red privada virtual
WAAP	Protección de aplicaciones web y API
WAF	Cortafuegos de aplicaciones web

Resumen ejecutivo

Un análisis de los ciberincidentes reportados en los últimos cinco años indica que los ataques de secuestro de datos (*ransomware*) son responsables del 32% de los ciberincidentes y provocan el 38% de las pérdidas financieras. Mientras la frecuencia de incidentes de *ransomware* en 2015 fue del 1% de los ciberincidentes, en los últimos años se observa un aumento significativo en el ámbito de actividad, que en 2023 fue del 52%.

¡Un incidente de *ransomware* común cuesta alrededor de US$1,4 millones! Esto es más de 12 veces el daño financiero promedio en comparación con otros ciberataques. Los incidentes graves de *ransomware* pueden ser mucho más devastadores. En los casos más extremos, los daños pueden llegar hasta aproximadamente US$50 millones, en comparación con los US$22 millones en casos de ciberataques sin *ransomware* (Cyentia Institute, 2024).

En los últimos meses y en los últimos años en general, han aumentado los intentos de ataque de *ransomware* y el contenido de los mismos contra servicios de nube pública como parte de una tendencia global hacia la explotación de organizaciones que utilizan servicios en la nube para almacenar su infraestructura e información. **Los ataques más exitosos se producen debido a una configuración e implementación incorrecta o mejorable por parte del cliente de servicios en la nube (CSC, por sus siglas en inglés), que exponen vulnerabilidades y vectores de ataque explotables. Por lo general, sin necesidad de un alto nivel de experiencia o la inversión de numerosos recursos[2] por parte de los atacantes (CSA, 2024).**

Uno de los incidentes más emblemáticos de 2023 se llevó a cabo contra proveedores de servicios en la nube (CSP, por sus siglas en inglés) que utilizaban MOVEit; en esa oportunidad una vulnerabilidad en el producto permitió al atacante ejecutar un ataque de *ransomware*. Esto demuestra que la amenaza del *ransomware* también es pertinente para las organizaciones que consumen servicios de nube pública (CSA, 2023; Check Point, 2023).

Según el informe de la Dirección Nacional de Ciberseguridad de Israel (INCD, por sus siglas en inglés), el coste económico de los ciberataques en el Estado de Israel es de más de US$3.000 millones al año (INCD, 2024a). Si las organizaciones y los individuos en el mercado no toman medidas de protección adecuadas, se espera que estos costos sigan creciendo cada año durante los próximos años, a partir del desarrollo tecnológico en todas las áreas de la vida y el consecuente aumento en la cantidad de ataques y en su naturaleza.

La finalidad de esta publicación es proporcionar información recopilada, dirigida a las autoridades de ciberseguridad y protección de la información acerca de los siguientes temas:

01

Las ciberamenazas en general, y la amenaza de *ransomware* en particular, y su posible impacto en las organizaciones que utilizan servicios de nube pública.

02

La presentación de estudios de caso para fomentar la sensibilización sobre la amenaza de *ransomware*, de modo que los lectores puedan hacer uso de los estudios aquí incluidos y otra información relevante en los debates ante los comités directivos y los tomadores de decisiones, y también al planificar y ejecutar acciones de protección.

03

La presentación de formas de reducir el riesgo, con el objetivo de que las organizaciones puedan adoptar las recomendaciones y ajustar su plan de seguridad anual para hacer frente a los ataques de *ransomware*.

2. Los términos *activo* y *recurso* se utilizan indistintamente en esta publicación.

Introducción

Contexto general

La computación en la nube es un modelo operativo y un conjunto de tecnologías que se utilizan para gestionar grupos compartidos de recursos informáticos mediante la abstracción de la computación, las redes, el almacenamiento, etc. El modelo de nube presenta una realidad en la que los componentes y recursos pueden orquestarse, asignarse y asimilarse rápidamente, también aumentarse y disminuirse según las necesidades, e incluso es posible desmantelarlos, lo que posibilita la implementación de un modelo dinámico de consumo y asimilación.

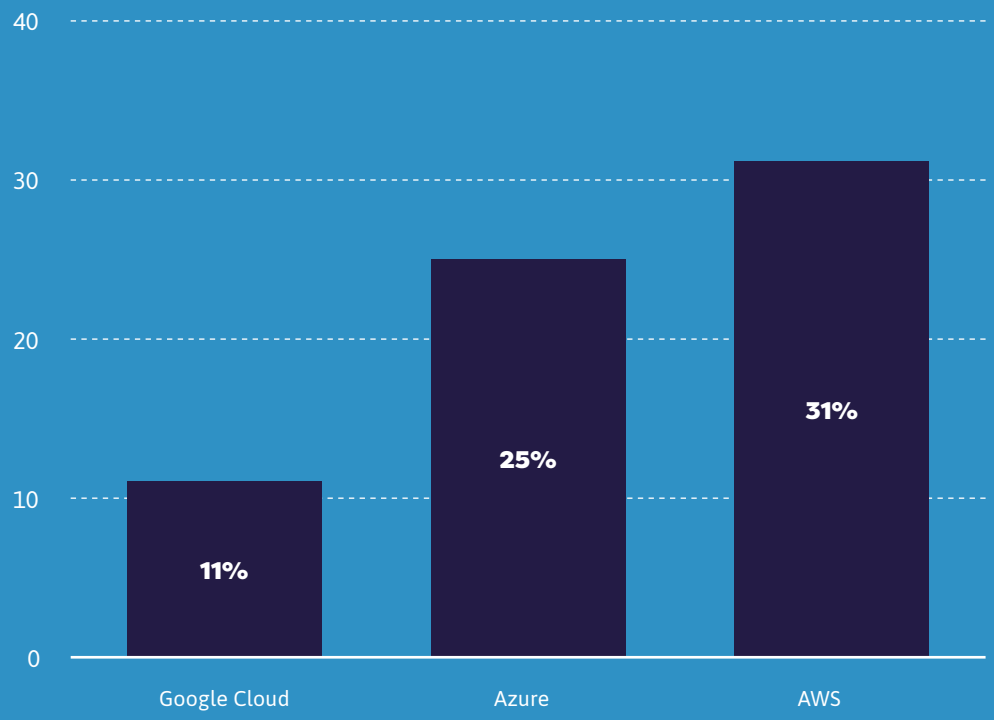
Los beneficios incluyen la colaboración entre las partes interesadas (*stakeholders*), agilidad, flexibilidad, disponibilidad y reducción de costes. Además, permite el acceso a nuevas capacidades tecnológicas que habitualmente no son asequibles para organizaciones con recursos limitados.

Tendencia mundial a pasar al uso de una nube pública

En los últimos años puede observarse una tendencia creciente en la que cada vez más organizaciones trasladan la gestión de sus recursos e información a servicios de nube pública. Esta transición se manifiesta en el almacenamiento externo de la información privada de la organización y/o en la gestión de los recursos informáticos externos. Según estimaciones, para finales de 2024 el volumen de almacenamiento de información en servicios en la nube rondará los 200 zetabytes (Morgan, 2024).

Existen docenas de empresas diferentes que brindan servicios en la nube a clientes de diferentes tamaños, desde pequeñas empresas hasta grandes organizaciones, y para diversos usos, desde sitios web hasta grandes proyectos que se almacenan y operan íntegramente con la ayuda de recursos de la nube. De todos los CSP, los tres más antiguos poseen dos tercios de la cuota de mercado: *Amazon Web Services* (AWS), que es parte de la empresa Amazon y el más antiguo del sector, posee el 31% del mercado; Azure, el servicio de Microsoft que existe desde 2010, tiene el 25% del mercado; *Google Cloud Platform* (GCP), el proveedor de la nube bajo la empresa paraguas Alphabet, posee el 11% del mercado (Gráfico 1).

Gráfico 1. Alcance del uso de proveedores de servicios de nube reconocidos en el primer trimestre de 2024



Fuente: Elaboración propia con base en Richter (2024).

La transición al uso de una nube pública atrae no solo a los clientes y organizaciones, sino también a quienes buscan aprovecharse de estas plataformas, al igual que ocurre con muchas tendencias tecnológicas. No sorprende que en los últimos años y en paralelo con el aumento del uso de servicios de nube pública, se identifiquen cada vez más campañas en las que partes maliciosas realizan ataques de secuestro de datos (*ransomware*) contra organizaciones que utilizan estas plataformas.

Un análisis de los incidentes reportados en los últimos cinco años señala que los ataques de *ransomware* son responsables del 32% de los ciberincidentes y provocan el 38% de las pérdidas financieras. Además, mientras la frecuencia de incidentes de *ransomware* en 2015 fue del 1% de los ciberincidentes, en los últimos años se observa un aumento significativo en el ámbito de actividad, que en 2023 fue del 52%. ¡Un incidente de *ransomware* común cuesta alrededor de US$1,4 millones! Esto es más de 12 veces el daño financiero promedio en comparación con otros ciberataques. Incluso, los incidentes graves con *ransomware* pueden ser mucho más devastadores, dado que en los casos más extremos los daños pueden llegar hasta aproximadamente US$50 millones, en comparación con los US$22 millones de ciberataques sin *ransomware* (Cyentia Institute, 2024). En los últimos meses y en los últimos años en general, han aumentado los intentos de ataque de *ransomware* y el contenido de los mismos contra servicios de nube pública (*public cloud services*), como parte de una tendencia global hacia la explotación de organizaciones que utilizan servicios en la nube para almacenar su infraestructura e información. Los ataques más exitosos se producen debido a una configuración e implementación incorrecta o mejorable por parte del CSC, que exponen vulnerabilidades y vectores de ataque explotables. Por lo general, sin necesidad de un alto nivel de experiencia y/o la inversión de numerosos recursos por parte de los atacantes (CSA, 2024).

Uno de los incidentes más emblemáticos de 2023 fue un ataque contra un CSP que utilizaba MOVEit; en esa oportunidad la vulnerabilidad en el producto permitió al atacante ejecutar un ataque de *ransomware*. Esto demuestra que la amenaza del *ransomware* también es pertinente para las organizaciones que consumen servicios de nube pública (CSA, 2023; Check Point, 2023).

Según el informe de la INCD, el coste económico de los ciberataques en el Estado de Israel es de más de US$3.000 millones al año (INCD, 2024a). Si las organizaciones y los individuos en el mercado no toman medidas de protección adecuadas, se espera que estos costos sigan creciendo cada año durante los próximos años, a partir del desarrollo tecnológico en todas las áreas de la vida y el consecuente aumento esperado en la cantidad de ataques y en su naturaleza.

En vista de estos hechos, es necesario que las organizaciones que utilizan servicios de nube pública tomen las medidas adecuadas para reducir el riesgo de un ciberincidente, incluyendo el *ransomware*, el cual a su vez puede causar daños directos e indirectos.

Modelos comunes de implementación en la nube

Es frecuente hacer referencia a cuatro modelos de implementación en la nube (NIST, 2011):

01

Nube pública. Los servicios en la nube se proporcionan a través de una infraestructura (*hardware, software* e implementaciones) que es común y abierta a todos, en ocasiones incluso gratuita. Si bien existe una división y separación lógica, y en ocasiones física, entre los clientes y las cuentas, se trata de un intercambio de recursos.

02

Nube privada. Los servicios en la nube se proporcionan a través de una infraestructura (*hardware, software* e implementaciones), accesible solo para el cliente en particular. En algunas ocasiones esta infraestructura está en la ubicación del cliente, mientras que en otras se encuentra en la del proveedor de la nube. La comunicación y el acceso a la infraestructura se proporcionan exclusivamente al cliente designado, y su implicación en su gestión puede ser elevada.

03

Nube comunitaria. Un determinado sector o varias organizaciones con un interés común se unen para recibir servicios de nube específicos para ellos.

04

Nube híbrida. Un cliente utiliza una nube privada para determinadas aplicaciones y también una nube pública con el fin de vincular la información o aplicación con otras aplicaciones o información.

De esta forma, en la computación en la nube existen dos opciones de puesta en práctica según la arquitectura:

01

Inquilino único (*single-tenant*). Según el tipo de servicio en la nube y de implementación, el uso del cliente es exclusivo, no presenta divisiones y no es compartido con otros usuarios dentro y fuera del CSC. Lo anterior puede manifestarse de diversas maneras, desde el uso de un recurso de *hardware* hasta una aplicación desarrollada específicamente para el cliente (generalmente en la implementación de una nube privada).

02

Inquilinos múltiples (*multi-tenants*). En este caso según el tipo de servicio en la nube y de implementación, el cliente comparte un recurso con usuarios adicionales, ya sea dentro del CSC o en otras organizaciones.

Modelos comunes de servicios de nube pública

Existen varios modelos comunes de servicios de nube pública, de los cuales los más destacados son los siguientes (NIST, 2011):

01

Infraestructura como servicio (IaaS, por sus siglas en inglés). El modelo básico y más habitual como servicio para empresas y organizaciones. Su objetivo principal es evitar la construcción de salas de computación y la compra y mantenimiento de componentes de *hardware*, que incluyen matrices de almacenamiento, servidores, componentes de comunicación y componentes de aseguramiento de la información. En cambio, la organización recibe servicios de nube por una tarifa acorde a su consumo usando un modelo de objetos virtuales que pueden controlarse a través de una interfaz de servicio.

02

Plataforma como servicio (PaaS, por sus siglas en inglés). En este modelo, además de los componentes de *hardware* e infraestructura, el proveedor de la nube proporciona al cliente una plataforma de paquetes de *software* básicos, que se utiliza para un entorno de desarrollo de aplicaciones, realizar pruebas de productos de clientes y brindar servicios informáticos desde la plataforma.

03

Software como servicio (SaaS, por sus siglas en inglés). En este modelo, el proveedor de la nube proporciona tanto el *hardware* y la infraestructura, como las aplicaciones finales del cliente, cuando la aplicación se compra a una empresa que se especializa en un ámbito específico.

Modelo de responsabilidad compartida

Por lo general, los CSP utilizan el modelo de responsabilidad compartida (SRM, por sus siglas en inglés) para especificar la función de cada parte del acuerdo de contratación y las tareas de seguridad que están bajo su responsabilidad.

Sin embargo, en la práctica los requisitos legales y reglamentarios no eliminan la responsabilidad legal (*accountability*) del CSC de proporcionar un nivel adecuado de protección de la información y los servicios. Por consiguiente, el CSC debe considerar este modelo como una herramienta de apoyo a la toma de decisiones, ya que debe asumir plenamente las implicancias de los riesgos y la exposición que supone la vinculación con el CSP (Gráfico 2).

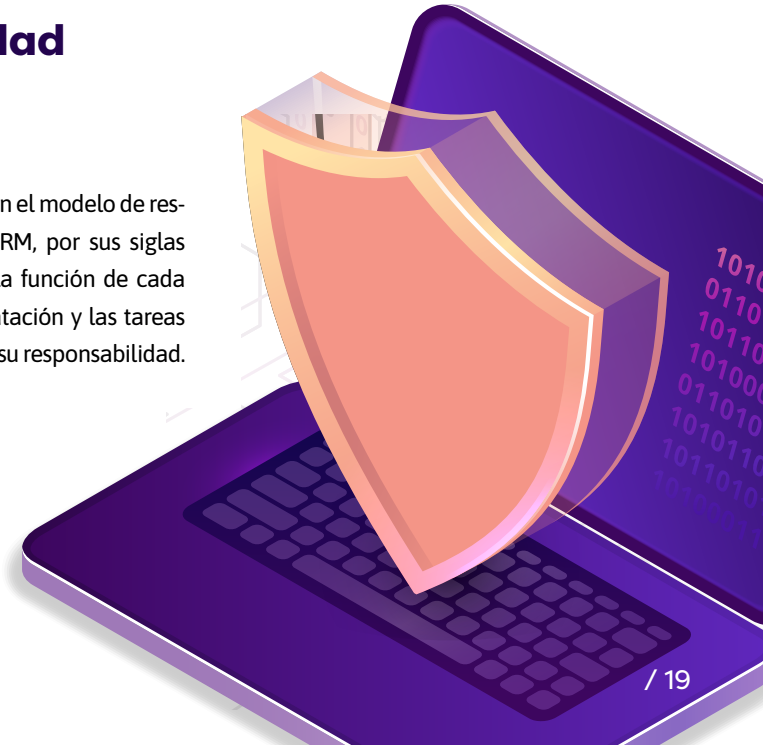
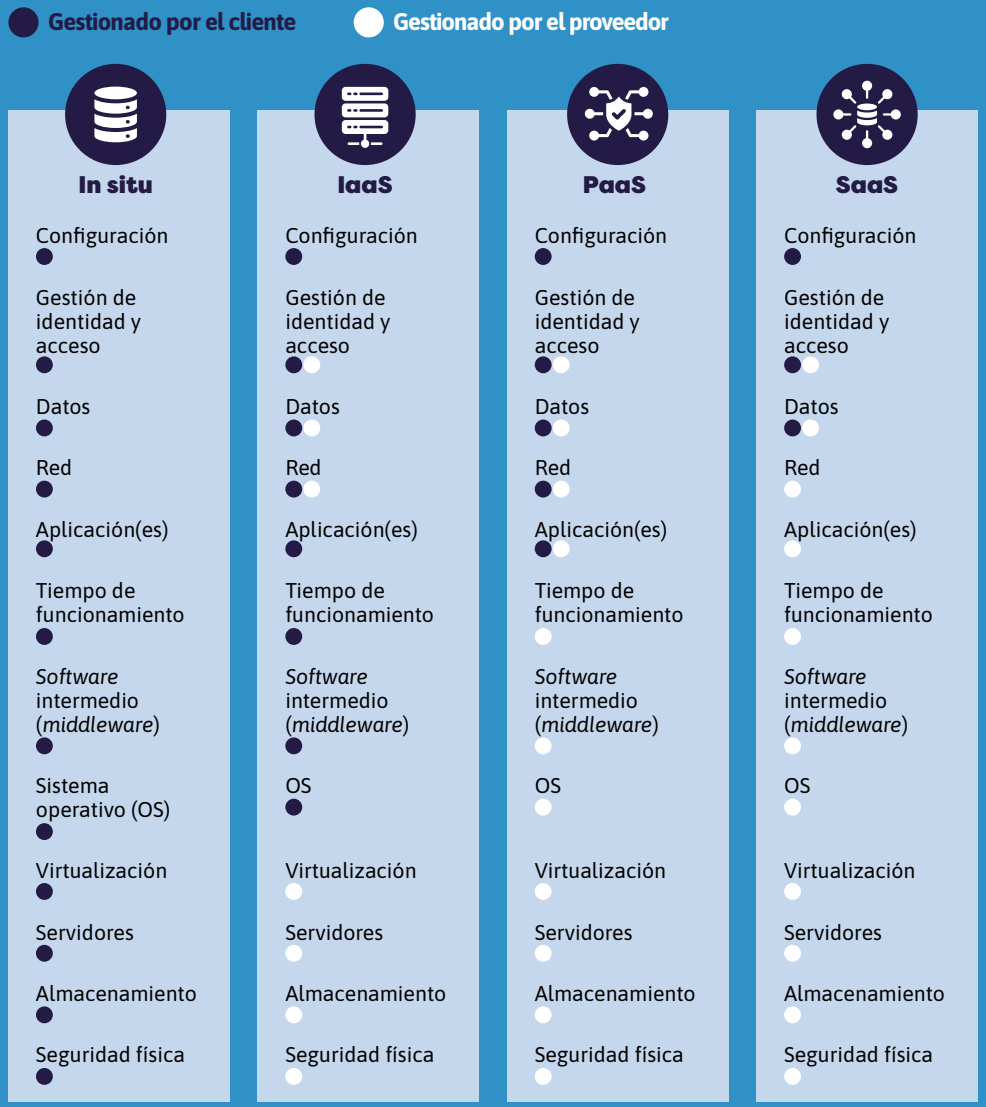


Gráfico 2. Modelo común de responsabilidad compartida



Fuente: Tomado del documento publicado por la CSA (2024), que se basa en el modelo de distribución de responsabilidades de la organización estadounidense Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA, por sus siglas en inglés).

En líneas generales, la responsabilidad compartida puede desglosarse según el modelo de servicio elegido, tal como se describe a continuación.

Iaas

Por lo general, el CSC tiene control y responsabilidad sobre muchas capas, desde el nivel de las interfaces de la red virtual hasta la información (Cuadro 1).

Cuadro 1. División de responsabilidad entre las partes en el modelo IaaS

Responsabilidad del CSP en el modelo IaaS	Responsabilidad del CSC en el modelo IaaS
• Suministro de la potencia informática según lo necesario y lo adquirido. • Puesta a disposición de los recursos informáticos durante la duración del compromiso contractual.	• Establecimiento del plan de infraestructura, que incluye: sistema de almacenamiento, sistema de servidor, configuraciones de comunicación dentro de la organización. • Definición de usuarios. • Implementación y su disponibilidad para los usuarios. • Desarrollo de la implementación, su operación y licenciamiento del *software*. • Protección de la información almacenada (cifrado, anonimización, etc.). • Continuidad del negocio.

PaaS

Por lo general, el CSC tiene control y responsabilidad sobre la aplicación y las capas de aplicación (Cuadro 2).

Cuadro 2. División de responsabilidad entre las partes en el modelo PaaS

Responsabilidad del CSP en el modelo PaaS	Responsabilidad del CSC en el modelo PaaS
• Suministro de la potencia informática según lo necesario y lo adquirido. • Puesta a disposición de los recursos informáticos durante la duración del compromiso contractual. • Entrega de una plataforma para el desarrollo de aplicaciones y mantenimiento de la misma tanto a nivel de gestión de versiones como de instalación de actualizaciones de seguridad (parches).	• Definiciones de comunicación intraorganizacional. • Definición de usuarios. • Implementación y su disponibilidad para los usuarios. • Desarrollo de la implementación, su operación y licenciamiento del *software*. • Protección de la información almacenada (cifrado, anonimización, etc.). • Continuidad del negocio.

SaaS

Por lo general, el CSC tiene control y responsabilidad muy limitados, excepto por el tipo y contenido de la información y la configuración y permisos del usuario, por lo que la responsabilidad recae principalmente en el CSP (Cuadro 3).

Cuadro 3. División de responsabilidad entre las partes en el modelo SaaS

Responsabilidad del CSP en el modelo SaaS	Responsabilidad del CSC en el modelo SaaS
• Establecimiento del plan de infraestructura, que incluye: sistema de almacenamiento, sistema de servidor, configuraciones de comunicación dentro de la organización. • Implementación y su disponibilidad para los usuarios. • Desarrollo de la implementación, su operación y licenciamiento del *software*. • Protección de la información almacenada. • Cifrado de la información, en su caso. • Continuidad del negocio.	• Corrección de la información. • Definición de usuarios y permisos. • Integridad de la información.

Anidado en nube (*nesting cloud*)

El anidamiento en la nube es una configuración de trabajo jerárquica en la que un CSP utiliza la infraestructura de un segundo CSP. Por ejemplo, un CSP proporciona a sus clientes un servicio de configuración SaaS, cuando depende de la infraestructura central de otro CSP que le proporciona una infraestructura de configuración IaaS. Esta configuración de trabajo permite a los CSP con recursos limitados u otras necesidades comerciales obtener acceso a capacidades avanzadas que no están disponibles para ellos de forma rutinaria.

Sin embargo, esta configuración de trabajo crea un alto nivel de dependencia entre los CSP, por lo que es habitual que numerosos CSC, especialmente aquellos que utilizan SaaS, no tengan conocimiento de su existencia. Este hecho puede afectar la capacidad del CSC para cumplir con los requisitos e indicadores de continuidad del negocio y con otros requisitos adicionales, como la necesidad de preservar la soberanía de los datos (*data sovereignty*).

Interfaces comunes para gestionar un entorno de nube pública

El acceso al entorno de la nube es posible a través de varias interfaces comunes. Como parte del concepto de seguridad, el CSC debe garantizar que estas interfaces reciban un nivel de seguridad adecuado. Esto se debe a que un error al aplicar una configuración o el empleo de un control de seguridad no adecuado al nivel de riesgo puede darle al atacante un acceso fácil y rápido a la información de la organización.

A continuación, se resumen las interfaces de gestión comunes:

01

Panel de gestión web. Puede incluir módulos de extensión como Cloud Shell y un host bastión (*bastion host*). Del mismo modo, se acepta que esta interfaz permita cargar archivos, como una lista de cuentas de usuario, con la ventaja de simplificar varios procesos de automatización.

02

Interfaz de línea de comandos (CLI, por sus siglas en inglés). Se activa desde el equipo o punto final del usuario; además, permite la automatización total o parcial.

03

Interfaz de programación de aplicaciones (API, por sus siglas en inglés). Permite la conectividad a nivel máquina a máquina (M2M, por sus siglas en inglés), así como de humano a máquina (H2M, por sus siglas en inglés), que proporciona capacidades de gestión avanzadas y amplias, entre ellas, el aumento de capacidades para realizar la integración con productos y servicios externos.

04

Kit de desarrollo de *software* (SDK, por sus siglas en inglés). Permite a los fabricantes de *software* y otras partes ampliar las capacidades de la solución en su nombre mediante la integración con el entorno de nube pública. De esta manera, la puesta en práctica habitual implica el uso de una API que el proveedor de la nube pública externaliza.

05

Servicio de metadatos de instancia (IMDS, por sus siglas en inglés) en nube. Permite el acceso a una instancia de un determinado activo y a sus metadatos. Aunque se trata de un servicio que se considera interno y no es accesible al cliente final de forma rutinaria, una puesta en práctica defectuosa puede posibilitar los ciberataques incluso fuera del entorno de nube del CSC. Un ejemplo es el uso de la falsificación de solicitudes del lado del servidor (SSRF, por sus siglas en inglés).

06

Red privada virtual (VPN, por sus siglas en inglés). Interfaz que permite una conexión remota de forma temporal o permanente entre sitios (S2S, por sus siglas en inglés).

Además de las interfaces para gestionar un entorno de nube pública, recursos como máquinas virtuales y contenedores pueden externalizar las interfaces de gestión comunes. A continuación, se muestran algunos ejemplos habituales:

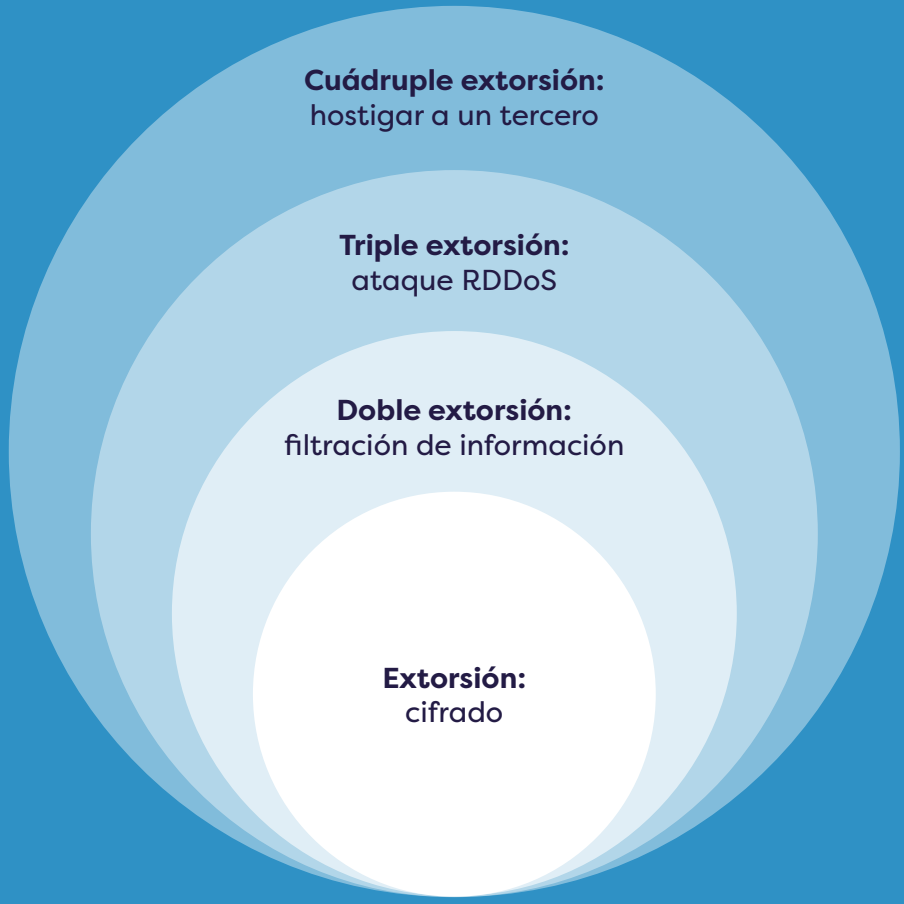
- **Protocolo de escritorio remoto (RDP, por sus siglas en inglés).** Interfaz de gestión frecuente en el entorno Windows.
- **WS-Management/WS-Remoting.** Interfaz que permite la ejecución remota de comandos y *scripts* de *Power Shell*.
- **Instrumentación de gestión de Windows (WMI, por sus siglas en inglés).** Interfaz de gestión de ajustes de configuración en el entorno Windows.
- ***Secure Shell* (SSH, por sus siglas en inglés).** Interfaz de gestión frecuente en el entorno Linux.
- **Protocolo simple de gestión de redes (SNMP, por sus siglas en inglés).** Interfaz de gestión frecuente para dispositivos de red, por ejemplo, cortafuegos (*firewall*).
- **Interfaces de acceso remoto, gestión y monitoreo (RMM, por sus siglas en inglés) de terceros.**
- **Protocolos de gestión dedicados para soluciones y sistemas de información y ciberseguridad.**

/01.
Patrones de acción comunes de los atacantes que utilizan *ransomware*

En su versión original el *ransomware* es un *software* malicioso (*malware*) cuyo propósito es impedir que un individuo o una organización acceda a su información mediante el uso de cifrado. De esta manera, se le exige a la víctima el pago de un rescate como condición para liberar la información.

Con el paso de los años, los atacantes han desarrollado varios patrones de acción que utilizan *ransomware* (Gráfico 3).

Gráfico 3. Patrones de acción comunes de los atacantes que utilizan *ransomware*



Nota: RDDoS: Ataque DDoS de rescate.

Asimismo, con el transcurso de los años es posible observar una evolución en los patrones de acción por parte de los atacantes, donde cada nuevo patrón de acción incluye al anterior, y ofrece una nueva capacidad. El Cuadro 4 muestra una ampliación sobre esto.

Cuadro 4. Patrones de acción comunes de los atacantes que utilizan *ransomware*

Patrón de la acción	Descripción
Extorsión: cifrado	El cifrado de la información para impedir el acceso a ella. Así, se exige a la organización (la "víctima") que cumpla con las demandas del "secuestrador" como condición para deshacer el cifrado. Este es el primer patrón de acción que utilizaron los ciberdelincuentes.
Doble extorsión: filtración de información	El filtrado de la información antes de su cifrado/eliminación, con el objetivo de ampliar el alcance de la exposición/vulneración del CSC, como por ejemplo, la amenaza de que la divulgación de información sensible dañe la reputación y/o resulte en la imposición de sanciones regulatorias.
Triple extorsión: ataque RDDoS*	Ataque RDDoS.
Cuádruple extorsión: hostigar a un tercero	Una amenaza que apela directa o indirectamente al cliente final u otras partes interesadas (como un regulador) a fin de ejercer presión sobre el CSC para que cumpla con los requisitos o como medida punitiva por negarse a cumplir con las condiciones del secuestro de datos.

Nota: *Este ataque en la nube pública se conoce como denegación de monedero (DoW, por sus siglas en inglés) y negación económica de la sostenibilidad (EDoS, por sus siglas en inglés).

A fin de intensificar el efecto del ataque, es habitual que se realice una combinación de los siguientes principios:

01

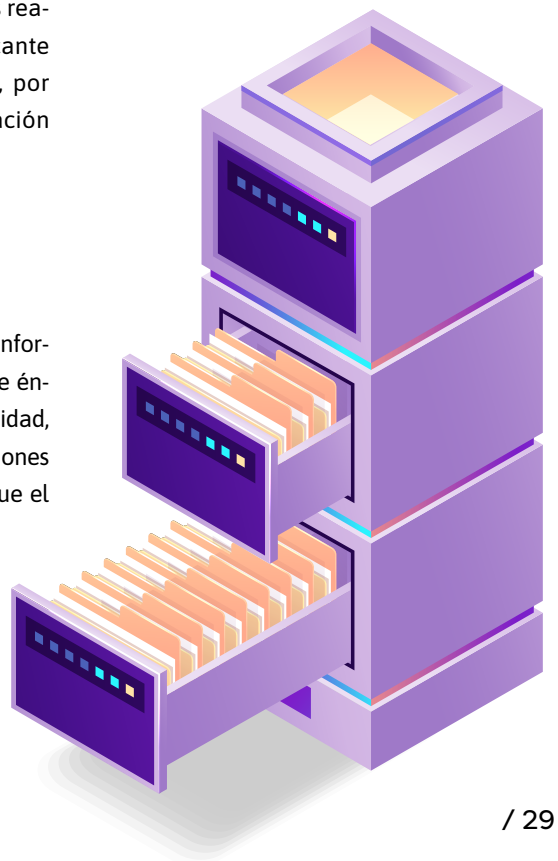
Alteración de la información. El atacante realiza cambios en la información existente con el objetivo de dañar la fiabilidad e integridad del CSC. Es habitual que el proceso de alteración se lleve a cabo durante un largo período de tiempo (semanas/meses/años), con el objetivo de dificultar que el CSC pueda localizar las modificaciones realizadas. Asimismo, esto permite al atacante "contaminar" las copias de seguridad, por lo que realizar un proceso de restauración por parte del CSC no será efectivo.

02

Limpiador (*wiper*). Impide el acceso a la información mediante su eliminación. Se pone énfasis en la eliminación de copias de seguridad, instantáneas (*snapshot*), gestión de versiones y réplicas, con el objetivo de dificultar que el CSC pueda recuperarse del incidente.

03

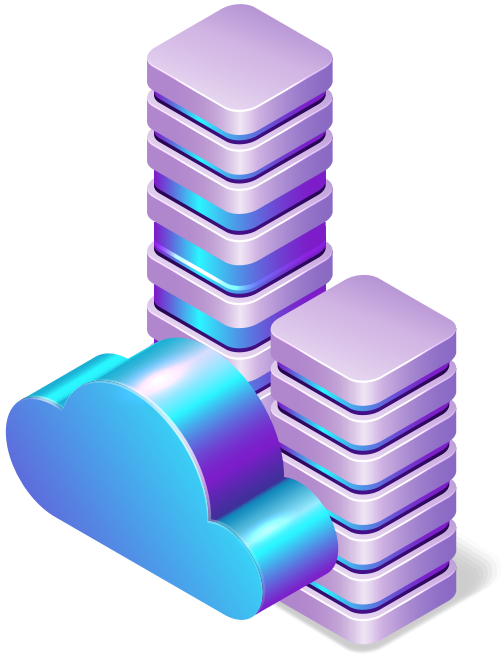
Adición de "ruido de fondo". Con el objetivo de crear una carga inusual sobre el equipo de seguridad de la información y ciberseguridad del CSC y/o difuminar los rastros, el atacante puede utilizar varios vectores de ataque simultáneamente o en serie.



/02.
Estudios de casos de ciberataques contra un entorno de nube pública

En este capítulo, se presentan una serie de estudios de casos de ataques contra un entorno de nube pública, con el objetivo de permitir a las autoridades de seguridad de la información y ciberseguridad comprender mejor este tipo de ataques.

La información aquí incluida puede ayudar a involucrar a tomadores de decisiones y a promover una cultura organizacional orientada a la seguridad de la información y la ciberseguridad.



Ataques ocurridos a nivel del CSP

01

Vulneración de los servidores del CSP debido a un ataque por confusión de dependencias

Por lo general, el *software* moderno también incluye bibliotecas y módulos (paquetes de *software*) que provienen de fuera de la organización. Habitualmente, estas bibliotecas se concentran en repositorios de *software* (*code repositories*) públicos, ya sea formales o semiformales. Estos módulos también se denominan dependencias de *software*, ya que el *software* depende de su correcta descarga e inclusión en el proceso de construcción para funcionar adecuadamente.

Existen repositorios para diferentes lenguajes de programación, como PyPI para Python, NPM para Node.js, RubyGems para Ruby, Maven para Java y NuGet para .NET. De hecho, varios usuarios, tanto organizaciones como particulares, pueden publicar el código que hayan desarrollado en estos repositorios.

Sin embargo, estas bases de datos generalmente no cuentan con rutinas de trabajo efectivas para la seguridad de la información y ciberseguridad, por lo que es habitual encontrar códigos maliciosos en ellas.

En el proceso de creación del *software*, ya sea manualmente por parte de un desarrollador o automáticamente en procesos de integración continua y entrega continua (CI/CD, por sus siglas en inglés), el administrador de paquetes de *software* (*software package manager*) descarga las versiones actuales desde las bibliotecas utilizadas por el desarrollador o desde un servidor, y el código se adjunta al código propietario escrito por el desarrollador o la organización (INCD, 2021).

En una de las plataformas de nube pública, el CSP permitió a los CSC establecer un localizador uniforme de recursos (URL, por sus siglas en inglés) para un repositorio de código externo, lo que expuso a los CSC a un ataque de confusión de dependencias. Como consecuencia, se generó una vulnerabilidad por la cual el atacante podría realizar una ejecución remota de código (RCE, por sus siglas en inglés) en un servicio gestionado de orquestación de flujos de trabajo llamado *Cloud Composer*. La vulnerabilidad específica del CSP se reveló en 2024 y la existencia de este tipo de vulnerabilidad se conoce desde 2021 (Matan, 2024).

02

Filtración de información mediante un ataque SSRF por mal diseño del IMDS a nivel del CSP

En julio de 2019 un tercero obtuvo acceso a las bases de datos de un banco centroamericano y logró filtrar los datos personales de unos 100 millones de ciudadanos estadounidenses y otros 6 millones de ciudadanos canadienses (Capital One, s.f.)

El ataque constó de varias etapas: en la primera, el atacante localizó una vulnerabilidad en el servidor web del CSC con capacidad de proxy inverso; en la segunda, aprovechó la vulnerabilidad anterior para poner en práctica un ataque SSRF; en la tercera, el ataque SSRF le permitió obtener acceso al IMDS v1.0; en la cuarta, debido a una falla de diseño, la versión IMDS v1.0 permitió al atacante consultar los metadatos del recurso (aunque el atacante provenía de Internet), por lo que obtuvo acceso a las credenciales del recurso. Finalmente, el atacante utilizó esa información obtenida para acceder al contenedor "*bucket*" del servicio de almacenamiento simple (S3) perteneciente al CSC y copió la información a otro *bucket* S3 de su propiedad (Nicholson, 2023; Vasudevan, 2022).

03

Ataque de *ransomware* debido a aislamiento inadecuado entre entornos de clientes del CSP

En el marco de este incidente, un atacante logró establecerse en el entorno de un cliente y desde allí saltar al entorno de un segundo cliente debido a un aislamiento inadecuado, por ejemplo, la falta de una partición de red adecuada entre diferentes clientes o el uso de la misma instancia de un sistema de gestión de identidades y accesos (IAM, por sus siglas en inglés) para diferentes clientes, lo que amplía el alcance del ataque de *ransomware*. Esto incluye la filtración de información sensible. Cabe señalar que se observaron varios incidentes de este tipo, principalmente en CSP pequeños y medianos.

04

Suplantación de identidad por implementación inadecuada del *token* SAML

Una plataforma SaaS permitió a los CSC acceder mediante un inicio de sesión único (SSO, por sus siglas en inglés) utilizando un *token* de lenguaje de marcado para confirmaciones de seguridad (SAML, por sus siglas en inglés). Debido a una implementación tecnológica deficiente, los CSC existentes podían modificar el contenido del *token* SAML y, por lo tanto, hacerse pasar por un usuario asociado con otro CSC (SSO Circle, 2016).

05

Acceso a los recursos del cliente debido a toma de control de la cuenta de administrador del CSP

Un atacante logró apoderarse de la cuenta de un administrador del sistema (*account take over*) de un CSP que brinda servicios de gestión de identidad, autenticación y control de acceso. A partir de eso, pudo recolectar información de autenticación del sistema (como *tokens* de acceso), lo que le permitió acceder a los recursos de los clientes (Manage Engine, 2024). En otras palabras, a través de un ataque a la cadena de suministro, el atacante pudo obtener acceso a los recursos del cliente.

Ataques ocurridos a nivel del CSC

01

Acceso a información confidencial a partir de un ataque Golden SAML

Golden SAML es un tipo de ataque que permite al atacante extender su dominio sobre las infraestructuras organizativas locales (*on-premises*), de forma de acceder a recursos existentes en el entorno de nube pública del CSC.

De manera similar a un ataque Golden Ticket contra la infraestructura corporativa local, este ataque permite al atacante hacerse pasar por un usuario legítimo del CSC, lo que le da acceso a los recursos disponibles en el CSP (Netwrix, s.f.; Reiner, 2017). El ataque puede realizarse utilizando varios métodos, como robar la clave privada del servicio de federación de *Active Directory* (AD FS, por sus siglas en inglés) instalado en la infraestructura organizativa local del CSC y firmar un *token* SAML suplantado, y en el siguiente paso, utilizar el *token* SAML suplantado para obtener acceso a los recursos almacenados en un entorno de nube pública.

Mediante este ataque, un número significativo de atacantes logró hacerse con información confidencial de varias organizaciones que estaba almacenada en un entorno de nube pública. Esto incluye información almacenada en plataformas SaaS reconocidas, a pesar de que originalmente el atacante no tenía datos de acceso a este entorno (Google Cloud, s.f.).

02

Brote de *ransomware* por transferencia de activos a una sala de servidores alternativa

En 2023 dos empresas migraron activos a una sala de servidores alternativa. Tras la transferencia de activos, que contenían un *ransomware* cuya existencia se desconocía, estalló un ataque de *ransomware* que se extendió por la red y provocó cifrado y pérdida de información a la misma empresa y a sus clientes, lo que incluyó la eliminación de copias de seguridad (Culafi, 2023; Whittaker, 2023).

03

Cierre de actividad empresarial de una compañía por ataque en varias etapas

En 2014 una empresa sufrió un ataque en múltiples etapas. En la primera, el atacante inició un ataque distribuido de denegación de servicio (DDoS, por sus siglas en inglés), por lo que es probable que su objetivo fuera desviar la atención de la empresa de las siguientes etapas del ataque. En la segunda etapa, logró obtener acceso al panel de gestión de AWS de la empresa y exigió el pago de un rescate como condición para detener el ataque DDoS. La empresa cambió los detalles de acceso al panel de gestión de AWS, pero el atacante creó cuentas alternativas con anticipación, lo que le permitió mantener la retención a lo largo del tiempo. Cuando el atacante comprendió que la empresa no pensaba pagar el rescate, comenzó a eliminar información del entorno de AWS, como el almacenamiento en bloque elástico (EBS, por sus siglas en inglés) y contenido almacenado en *buckets* S3. Debido a ello, se perdió información de la empresa y de sus clientes, incluyendo las copias de seguridad, lo que finalmente produjo el cierre de la actividad empresarial de la compañía (Goldman, 2014).

04

Almacenamiento de secretos en el servicio en la nube de gestión de código fuente de GitHub

Un informe de la compañía GitGuardian para 2024 muestra que en 2023 se expusieron más de 12,8 millones de secretos (como claves API, nombres de usuarios, contraseñas, claves de encriptación, *tokens* de acceso) que estaban almacenados en repositorios públicos de GitHub (un servicio de nube pública para la gestión de código fuente de GitHub). Como consecuencia, algunos de los secretos permitieron ataques continuos, como controlar el entorno de nube pública del CSC y filtrar información (GitGuardian, 2024). Además, es habitual que los atacantes que se han afianzado en el entorno de nube pública del CSC lo utilicen para campañas de ataque horizontal, como una campaña de suplantación de identidad (*phishing*) a fin de propagar un *ransomware* (Laceworks Labs, 2022).

Frecuentemente los causantes de este tipo de incidentes son la falta de un proceso de desarrollo seguro efectivo, incluyendo el incumplimiento de las recomendaciones aceptadas para el desarrollo de la nube, que comprenden la intención de utilizar medios específicos para proteger secretos, como un servidor de gestión de claves (KMS, por sus siglas en inglés) o un módulo de seguridad de *hardware* (HSM, por sus siglas en inglés), y también la falta de un proceso de búsqueda oportuno para localizar secretos en el código fuente y la existencia un control de acceso deficiente.

05

Filtración de información y chantaje al CSC debido a claves de acceso filtradas

Un atacante que logró hacerse con las claves de acceso (*access keys*) de un entorno de nube pública del CSC implementó un ataque de varias etapas. En la primera, utilizó las claves de acceso para acceder a la información disponible en el contenedor de tipo *bucket* S3; en la segunda, filtró la información del *bucket* S3; en la tercera, desactivó el mecanismo de control de versiones (*version control*); y, por último, eliminó el contenido del *bucket* S3 y dejó una carta en la que solicitaba el pago de un rescate (Invictus, 2024).

06

Exposición a ataques DDoS de rescate (RDDoS)

Es habitual que los atacantes en el ciberespacio aprovechen la vulnerabilidad del CSC para llevar a cabo ataques RDDoS. Frente a ellos, los CSC que no aceptan los términos del secuestro o no tienen un sistema de seguridad con un nivel adecuado de resiliencia, sufren pérdidas financieras y de otro tipo a lo largo del tiempo. Así, por ejemplo, un ataque RDDoS que dure varias horas o más tiempo puede suponer elevados costes de facturación para el CSC por parte del CSP. Y el daño va más allá de las consecuencias derivadas del perjuicio a la disponibilidad del servicio empresarial.

07

Penetración de la plataforma de correo electrónico SaaS debido a la aplicación de un control de acceso débil

Un número significativo de organizaciones que utilizaban una plataforma de correo electrónico SaaS no aplicaron un control de acceso adecuado, como imponer el uso de autenticación multifactor (MFA, por sus siglas en inglés). Como resultado, el atacante pudo obtener la contraseña de acceso, lo que le dio acceso a los servicios e información de la nube. En algunos casos, el atacante implementó reglas que incluían enviar una copia oculta del mensaje saliente/recibido en el buzón del usuario, a otro buzón de correo electrónico de su propiedad. De esta forma, el atacante mantuvo la retención incluso después de que el usuario cambiara la contraseña de acceso.

/03. Vectores habituales de penetración para entornos de nube pública

Cada CSC debe llevar a cabo un proceso oportuno de gestión de riesgos, dentro del cual se realiza el mapeo de los vectores de ataque relevantes a su perfil de riesgo.

Aprovechamiento de una configuración deficiente (*misconfiguration*)

La nube pública ofrece alta accesibilidad a servicios e información desde cualquier lugar, en cualquier dispositivo y en cualquier momento. Es habitual observar brechas en el conocimiento sobre este tema de parte de los profesionales que se desempeñan en este campo, lo que se debe en parte a la carga y diversidad de tareas, la amplia y variada oferta de servicios disponibles en la nube pública, la variedad de CSP existentes en el mercado y la adopción de conceptos avanzados como desarrollo y operaciones (DevOps, por sus nombres en inglés), que transfieren parte del control a quienes no tienen la seguridad de la información y la ciberseguridad como eje central. Al mismo tiempo, numerosas organizaciones no tienen un proceso efectivo de gestión de cambios y no utilizan controles aceptados para reducir la probabilidad de que se materialicen diversos riesgos.

La consecuencia habitual de un error al aplicar una definición de configuración en la nube es la exposición de los servicios y la información a todos los usuarios de Internet, entre ellos, a los atacantes en el ciberespacio. Al revisar varias publicaciones, puede observarse que este es un vector de ataque muy habitual.

Mal diseño de arquitectura multiinquilino

El uso de una nube pública se basa en compartir recursos entre diferentes clientes, lo que se conoce como arquitectura multiinquilino. Sin embargo, es común que los proveedores de la nube, especialmente los más pequeños, no apliquen un aislamiento adecuado entre los clientes, lo que aumenta la probabilidad de sufrir un ciberincidente por medio de movimiento lateral. Así, por ejemplo, un determinado cliente podría llegar a tener acceso a la información de otro cliente diferente, un cliente desconocido podría desplazarse al entorno de un cliente determinado o, incluso, un atacante podría aprovechar una vulnerabilidad en un componente de acceso compartido, que permita el uso de información de identificación de un CSC desconocido, para acceder a la información de otro CSC diferente.

Uso de un código abierto (*open source*) que contenga una puerta trasera (*backdoor*) u otra vulnerabilidad

El uso de código abierto está muy extendido en la actualidad; sin embargo, muchos CSC no son lo suficientemente conscientes de que el código puede contener un implante malicioso, como una puerta trasera (*backdoor*), o bien *malware* cuyo propósito sea utilizar los recursos informáticos existentes para el minado de moneda digital (*cryptomining*), entre otras cosas.

Como resultado de esto, el equipo de desarrollo y/o el equipo de tecnología de la información (TI) pueden utilizar código abierto (como herramientas, bibliotecas de códigos, copia de muestras de códigos disponibles en bases de datos comunes) que contiene vulnerabilidades y, por lo tanto, pueden brindar a los atacantes acceso completo al entorno.

Falta de protección adecuada de los secretos

El uso de secretos está generalizado a nivel de infraestructura y aplicaciones, incluyendo el código fuente que también sirve para procesos de automatización en el entorno de la nube. Los secretos que el CSC puede utilizar incluyen claves API, usuarios/contraseñas y certificados digitales, entre otros.

Por lo general, las organizaciones no aplican un nivel adecuado de protección a los secretos, por lo que estos son almacenados en texto claro en el código fuente o en las distintas áreas de almacenamiento del entorno de la nube. Incluso, en numerosas ocasiones, tampoco aplican un control de acceso adecuado ni utilizan los mecanismos recomendados por el proveedor de la nube, como KMS o HSM.

Además, existe una tendencia hacia el uso de sistemas de gestión de código (SCM, por sus siglas en inglés) en un entorno de nube pública, que en ocasiones implica compartir información con el público y/o entidades de terceros, por ejemplo en la subcontratación, e incluso compartir código fuente que el CSC ha desarrollado en el marco de proyectos de código abierto.

Todo esto aumenta la probabilidad de que los secretos se revelen a personas no autorizadas, lo que a su vez posibilita un amplio acceso a los recursos existentes en el entorno de la nube pública.

Interfaces API expuestas sin el aseguramiento adecuado

La exposición directa de interfaces API que contienen vulnerabilidades y/o que no cuentan con la implementación de mecanismos de seguridad aceptados, tales como API Gateway (API GW) o protección de aplicaciones web y API (WAAP, por sus siglas en inglés), facilita que un atacante obtenga acceso a información sensible.

Vulnerabilidad compartida (*shared vulnerability*) en servicios de nube públicos

De acuerdo con el modelo de distribución de responsabilidad compartida, el CSP es responsable de cuestiones transversales, como la seguridad de la infraestructura. En caso de exposición a una vulnerabilidad compartida, es habitual que los CSC dependan del CSP para aplicar el parche requerido, dado que, en numerosas ocasiones, los CSC desconocen por completo la existencia de vulnerabilidades en los servicios del proveedor. La reparación depende de una serie de parámetros, como la capacidad del proveedor para realizarla y el acuerdo de servicio definido entre las partes (SLA, por sus siglas en inglés). En algunos casos, después de aplicar el parche, es posible que el cliente deba realizar acciones adicionales, como reiniciar las máquinas virtuales.

Adicionalmente, las vulnerabilidades publicadas por los proveedores de servicios en la nube junto con las actualizaciones críticas (día 1) pueden permitir la ejecución de acciones maliciosas, incluyendo ataques de *ransomware*. Un ejemplo de esto es la vulnerabilidad en un servicio de CSP publicada en septiembre de 2022, que posibilitó la escalada de privilegios (*privilege escalation*) por una parte externa (Frichette, 2022).

En ocasiones se publican nuevas vulnerabilidades (*zero-days*) que permiten un uso malicioso de los servicios de la nube pública, como iniciar desde el entorno de la nube un ataque contra el CSC o un tercero. Un ejemplo reciente es el aprovechamiento de una vulnerabilidad crítica en el servicio OneDrive, que permitía a los atacantes cifrar información y eliminar las copias de seguridad, de manera de evitar las medidas de seguridad comunes (Yair, s.f.).

Aprovechamiento de mecanismos de sincronización de datos, replicación y transferencia de información a un contenedor

Los servicios en la nube incluyen mecanismos de sincronización de archivos entre un punto final y la nube, replicación a nivel de región, una opción para aplicar replicación entre diferentes regiones, y transferencia de información a un contenedor. Algunos de estos mecanismos suelen estar activados por defecto, a veces sin el conocimiento de los clientes. Además, es común que los usuarios ejecuten estos servicios a nivel de punto final de manera de eludir los procesos regulares de TI (*shadow IT*), con el objetivo de acortar los tiempos de respuesta y superar las barreras organizacionales que perjudican el nivel de productividad.

En un contexto como este, un atacante puede inyectar un archivo malicioso utilizando un mecanismo de sincronización de archivos que busca archivos nuevos o nuevas versiones de archivos para cargarlos en la nube. Por lo general, el archivo malicioso llegará, a través de un correo electrónico de *phishing* o de *phishing* dirigido (*spear phishing*), como un archivo adjunto a un mensaje que intenta parecerse a un archivo inocente. Después de descargar el archivo, el servicio lo subirá automáticamente a la plataforma en la nube, desde donde el archivo se propagará a carpetas compartidas, a partir de las cuales serán posibles acciones maliciosas adicionales.

En los casos en los que el *ransomware* cifra los archivos en un determinado punto final, el atacante podría recurrir a la sincronización y/o replicación de archivos y/o transferencia de información a un contenedor para actualizar o sobrescribir las copias de seguridad almacenadas en una nube pública, con el objetivo de dañar al CSC hasta el punto de impedir su capacidad de recuperación, si fuese necesario.

Credenciales de acceso pirateadas

Hay varias formas de obtener credenciales de acceso a una plataforma en la nube utilizando credenciales obtenidas de forma maliciosa. A continuación, se muestran algunas de las más comunes:

01

Con la ayuda de un *infostealer*, el cual se activa en las computadoras finales (incluyendo los navegadores) de los usuarios del CSC y roba contraseñas y captura las pulsaciones de teclado (*keystrokes*), de manera de recopilar directamente información de autenticación al acceder a los servicios en la nube.

02

Credenciales de acceso filtradas ofrecidas en subastas en la web oscura (*darknet*), mediante campañas de *phishing* con diferentes niveles de complejidad, compra de credenciales de acceso filtradas en un incidente anterior (*credential stuffing*) o mediante otro método.

03

Ataques de fuerza bruta (*brute-force*) y similares, que permiten probar exhaustivamente contraseñas predeterminadas, débiles o todas las opciones de contraseña.

04

Búsqueda proactiva de repositorios de códigos y foros profesionales públicos para detectar secretos.

Ingeniería social

Existen varios cursos de acción posibles para poner en práctica ingeniería social hacia los usuarios de plataformas en la nube. A continuación, se muestran algunas formas comunes de acción:

01

Campañas de *phishing* o *phishing* dirigido. Su objetivo es obtener el nombre de usuario y contraseña a través de páginas de destino que presentan un mecanismo de inicio de sesión falso a los servicios en la nube.

02

Campañas de adversario en el medio (AiTM, por sus siglas en inglés).[3] Explotan mecanismos a través de los cuales pueden obtener información que los ayuda a acceder a plataformas en la nube. En estos casos, la campaña presenta una página de inicio de sesión a un servicio en la nube que, en los casos en los que también existe un componente de MFA son capaces de conseguirlo con pasos similares a las campañas de *phishing* normales, pero con capacidades más complejas. En junio de 2023, Microsoft identificó una campaña de este tipo destinada a obtener acceso a sus servicios (Toulas, 2024; Microsoft Threat Intelligence, 2023).

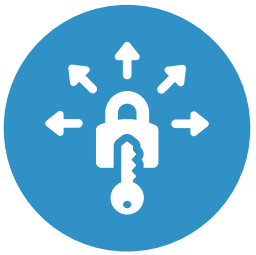
03

Una campaña de *phishing* en una conversación telefónica (*vishing*). En esa ocasión terceras partes se hacen pasar por una entidad legítima, generalmente empleados de TI, por lo cual obtienen detalles o convencen a los usuarios de conectarse a una página de *phishing*.

3. Este ataque también se conoce como Evilginx, debido a la herramienta de código abierto que suelen utilizar los atacantes en el ciberespacio.

04

Campaña de *smishing*. En ella el atacante se hace pasar por una entidad legítima, generalmente mediante el envío de mensajes de texto (SMS) en nombre del CSP o CSC sobre la necesidad de cambiar una contraseña, confirmar los detalles de identificación o actualizar un método de pago. De esta manera, el atacante recopila información y/o convence al usuario para que se conecte a una página de *phishing*.



Explotación de una vulnerabilidad existente en la infraestructura de federación

Las infraestructuras de federación (como AD FS) permiten a las organizaciones implementar SSO, de manera de evitar administrar varias identidades diferentes para un solo usuario y, al mismo tiempo, mejorar la experiencia del usuario.

A continuación, se muestran algunos métodos de acción comunes de los atacantes contra la infraestructura de federación:

01

Un atacante obtiene acceso a la infraestructura de federación, lo que le permite emitir credenciales de acceso falsas (como un *token* SAML), con lo que puede acceder a recursos en la nube pública.

02

El aprovechamiento de una vulnerabilidad en el entorno SaaS permite a un atacante reemplazar la URL legítima que dirige al usuario al proveedor de identidades (IdP, por sus siglas en inglés) legítimo, por una URL maliciosa que dirige al usuario a un sitio que recopila credenciales de acceso. Este ataque también se conoce como SAMLjacking.

Transferencia de información por parte del CSP a subproveedores sin el conocimiento y consentimiento del CSC

Los CSP con plataformas SaaS suelen hacer uso de un número relativamente grande de subproveedores, como un CSP secundario que proporciona reconocimiento óptico de caracteres (OCR, por sus siglas en inglés) o servicios de saneamiento de datos. En numerosas ocasiones, el CSC no es consciente de que su información sensible está siendo transferida al CSP, que a su vez no tiene ningún compromiso real con el CSC. Además, es habitual que el CSC no tenga capacidad real para garantizar el nivel de seguridad del CSP secundario y que cumpla con los requisitos legales y reglamentarios. Como consecuencia de esto, un incidente en el CSP secundario puede resultar en la divulgación de información sensible del CSC a partes no autorizadas y, en numerosas ocasiones, un atacante puede saltar del entorno del CSP secundario al entorno del CSP principal.

Establecimiento de una nueva cuenta de usuario antes del acceso de un usuario legítimo

En este ataque, el atacante primero crea una nueva cuenta de usuario en la plataforma SaaS con el mismo nombre que una cuenta de usuario legítima existente en el CSC. Luego, el atacante configura canales de recuperación secundarios (como una dirección de correo electrónico o un número de teléfono) en la cuenta que creó.

En el siguiente paso, el usuario legítimo intenta registrarse en el servicio y recibe un mensaje de que la cuenta ya existe. Es habitual que el usuario intente recuperar la contraseña (por ejemplo, haciendo clic en el enlace ¿Olvidó su contraseña?), la restablezca y comience a funcionar normalmente. En un momento u otro, el atacante restablece la contraseña utilizando un canal alternativo, con lo que recupera el control de la cuenta. Este ataque también se conoce como emboscada de cuentas (*account ambushing*).

Intrusión en el entorno de nube y/o aprovechamiento de la interfaz de autenticación debido a una vulnerabilidad web

Un atacante puede explotar una vulnerabilidad web que permite penetrar en el entorno de la nube y/o aprovechar la interfaz de autenticación.

A continuación, se muestran algunos métodos de acción comunes de los atacantes:

01

Explotación de una vulnerabilidad web conocida, como las que figuran en la guía del Proyecto abierto de seguridad en aplicaciones web (OWASP, por sus siglas en inglés): **Web Security Testing Guide** (OWASP, 2020).

02

Mala configuración del mecanismo de gestión de sesiones, de modo que, aunque la cuenta de usuario se encuentre desactivada (*disabled account*), su respectivo *token* de acceso aún sea válido y permita acceder a servicios e información. Este problema ocurre frecuentemente al poner en práctica protocolos independientes, como OAuth 2.0 y OpenID Connect.

03

Ausencia de un mecanismo de validación, como una firma digital u otro mecanismo, para validar que el *token* de acceso no ha sufrido una modificación involuntaria o es un *token* que busca hacerse pasar por legítimo.

04

Uso de un protocolo para un fin inapropiado, como emplear OAuth 2.0 para la autenticación de usuarios, cuando su propósito es asignar autorización únicamente.

Uso de entornos de nube legítimos de los CSC como infraestructura de ataque contra entidades de terceros (*watering hole attack/LOTS*)

En los últimos años, numerosos atacantes comenzaron a extender sus capacidades técnicas a la nube pública, mediante la utilización de sitios web fiables y servicios legítimos para evitar la detección e identificación y al mismo tiempo disfrazar las comunicaciones de comando y control (C2, por sus siglas en inglés) como tráfico legítimo normal o mensajes inocentes que pasan por plataformas en línea (vivir de sitios de confianza [LOTS, por sus siglas en inglés]).

Como resultado, es habitual que los atacantes utilicen entornos de nube legítimos de CSC como infraestructura de ataque contra entidades de terceros.

A continuación, se muestran algunos ejemplos:

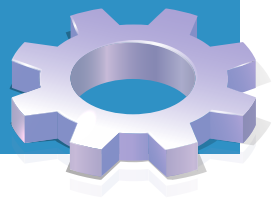
01

Como parte de una filtración de información, transferir la información organizacional a la base de datos de objetos en una nube pública que esté bajo el control del atacante. El filtrado de información es una táctica típica utilizada en los ataques de *ransomware*.

02

Establecer un servidor de C2 en un entorno de nube pública que se comunica con un *ransomware* activado en el entorno de la organización.

En numerosas ocasiones, estas técnicas permiten a los ciberatacantes eludir mecanismos de seguridad comunes, como la ubicación geográfica. Esto se debe a que es habitual que las medidas de seguridad y/o los usuarios finales confíen más en los sitios web almacenados en entornos de nube pública, especialmente cuando los nombres de los objetos mostrados al usuario (por ejemplo, parte de la URL) usan valores identificados como seguros (por ejemplo, el nombre de la organización o del CSP).



Ingeniería social a la luz de SaaS

A lo largo de los años, los atacantes han desarrollado varios métodos de acción con características únicas para los usuarios que utilizan plataformas SaaS. A continuación, se resumen varios cursos de acción comunes:

01

Enviar un mensaje de *phishing* a través de correo electrónico o servicio de mensajería instantánea que incluya una URL, a través de la cual se requiera que el usuario otorgue permisos al atacante utilizando el protocolo OAuth 2.0. De esta manera, frecuentemente los usuarios que reciben un mensaje varias veces aprueban la solicitud de otorgamiento de privilegios de acceso, por lo que el atacante consigue controlarlo con el tiempo. Incluso después de finalizar la sesión del usuario y también después de que haya cambiado su contraseña, la retención se mantiene hasta que se elimine manualmente.

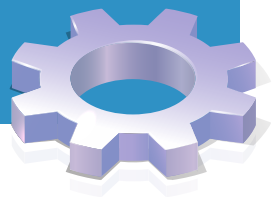
02

Publicar una aplicación suplantadora en el *marketplace* oficial, en un imitador o en un sitio web y luego utilizar un esquema de *phishing* o *vishing* para convencer al usuario de que descargue e instale la aplicación maliciosa. Una técnica similar sirve a los atacantes cuando distribuyen un complemento (*plug-in*) malicioso.

Naturalmente, la lista de vectores de ataque anterior no es exhaustiva. En vista de esto, se sugiere que cada CSC abra un banco de vectores de ataque que le correspondan, de acuerdo con su perfil de riesgo.

Para construir un banco de vectores de ataque, se recomienda utilizar fuentes de información aceptadas, por ejemplo:

- Publicaciones como el **Top Threats Working Group,** de la Cloud Security Alliance (CSA).
- Publicaciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), tales como **Threat Landscape.**
- Publicaciones de la organización OWASP, tales como **Cloud-Native Application Security Top 10 y OWASP Testing Guide.**
- Publicaciones de la organización MITRE, tales como **MITRE ATT&CK® Cloud Matrix** y **MITRE ATLAS.**
- SaaS Attack Techniques.
- Informes y publicaciones por encargo de proveedores de nube pública.
- Informes y publicaciones por encargo de empresas cibernéticas y de protección de la información, como empresas del sector de inteligencia sobre ciberamenazas (CTI, por sus siglas en inglés).



/04.

Formas aceptadas de reducir el riesgo como resultado de ciberataques en una nube pública

Este capítulo presenta formas aceptadas de reducir el riesgo como resultado de ciberataques en una nube pública, para lo cual las divide en las categorías del marco de ciberseguridad (CSF, por sus siglas en inglés) versión 2.0, del Instituto Nacional de Normas y Tecnología de los Estados Unidos (NIST, por sus siglas en inglés) (NIST, 2024) (Gráfico 4).

Gráfico 4. Categorías del marco de ciberseguridad 2.0

Cabe señalar que las formas aceptadas de reducir el riesgo revisadas en esta publicación no son exhaustivas y se centran en la amenaza del *ransomware*. La organización debe realizar un estudio periódico de riesgos y adaptar sus métodos de reducción de riesgos a los requisitos de la ley, la regulación, los requisitos contractuales y las necesidades del negocio.

El enfoque actualmente aceptado en materia de ciberseguridad y protección de la información es la adopción de principios de defensa informada contra amenazas (*threat-informed-defense*) y seguridad basada en evidencia (*evidence-based defense*).

Categoría de gobernanza empresarial (*govern*)

Consiste en establecer y monitorear la política y estrategia de la organización destinada a la gestión del riesgo cibernético.[4]

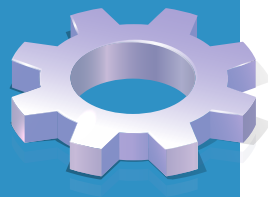
Estrategia de gestión de riesgos (GV.RM)

Se recomienda que la organización desarrolle una estrategia de gestión de riesgos en el ámbito de la nube, en la que defina claramente las prioridades, limitaciones, nivel de riesgo aceptado por la organización, supuestos de partida y principios claros a la hora de tomar decisiones sobre estos temas, y cómo manejar los riesgos (aceptación, rechazo, transferencia, reducción). La estrategia debe tener un mapeo y una referencia a todos los requisitos tal como los expresan las diversas partes interesadas dentro y fuera del CSC, incluyendo los clientes (consumidores) y proveedores.

También debe incorporar una referencia a situaciones de anidamiento en la nube utilizadas por el propio CSC o por otro CSP que actúa como proveedor secundario. Asimismo, se recomienda que incluya una revisión periódica de un plan de salida o terminación de la contratación con los CSP, en el que se estipulen criterios claros y actualizados sobre cuándo será necesario activarlo.

Se sugiere que la estrategia incluya un examen periódico sobre la necesidad de adquirir un seguro cibernético, al tiempo que se garantice que la póliza haga referencia al trabajo en un entorno de nube pública. Además, se recomienda que la estrategia establezca que el responsable de protección de datos (DPO, por sus siglas en inglés) integre las actividades de ciberseguridad y protección de la información, incluso como miembro permanente de los comités directivos pertinentes.[5]

Se recomienda que el director de seguridad de la información (CISO, por sus siglas en inglés) establezca una entidad designada para la gobernanza, gestión de riesgos y cumplimiento en la nube (GRC, por sus siglas en inglés).



Política (GV.PO)

Se recomienda que la política cibernética y de protección de la información incluya una referencia a los retos y riesgos de trabajar en un entorno de nube pública, mientras se aplican indicadores aceptados (como indicadores clave de control [KCI, por sus siglas en inglés], indicador de objetivo clave [KGI, por sus siglas en inglés], indicador clave de rendimiento [KPI, por sus siglas en inglés], indicador clave de riesgo [KRI, por sus siglas en inglés], objetivo y resultado clave [OKR, por sus siglas en inglés]) para examinar el proceso de implementación y nivel de eficacia de la estrategia de gestión de riesgos.

Seguridad de la cadena de suministro (GV.SC)[6]

Se recomienda que el CSC defina claramente los criterios para seleccionar la identidad del CSP, mientras realiza un examen preliminar y periódico de la efectividad de las herramientas nativas (*native tools*) contra el actual banco de vectores de ataque, que se deriva del perfil de riesgo de la organización.

A continuación, se muestran algunos ejemplos de los criterios:

01

Como condición para la contratación, el CSP deberá cumplir con los requisitos de certificación de Nivel 2 del registro de seguridad, confianza, garantía y riesgo (STAR, por sus siglas en inglés) de la CSA[7] o de Nivel 2 del Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP, por sus siglas en inglés)[8] y superiores, a la vez que se deberá verificar que el acuerdo cubra los recursos pertinentes para la actividad del CSC.

4. La interpretación de los nombres de las categorías está tomada del Cuestionario de Madurez de Defensa de las Pequeñas y Medianas Empresas, publicado por la INCD (2024b).
5. Para más información, véase: SaaS Governance Best Practices for Cloud (CSA, 2022) y la documentación sobre Cloud Adoption Framework (CAF) de los diferentes CSP: AWS cloud adoption framework: **https://aws.amazon.com/cloud-adoption-framework/**; Microsoft Cloud Adoption Framework for Azure: **https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/**; Marco de trabajo para la adopción de Google Cloud: **https://cloud.google.com/adoption-framework**; Cloud adoption framework for Oracle Cloud Infrastructure (OCI): **https://www.oracle.com/cloud/cloud-adoption-framework/**.
6. El documento ***Cadena de suministro: cuando todos los eslabones son fuertes, su organización está protegida*** se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/cadena-de-suministro-cuando-todos-los-eslabones-son-fuertes-su-organizacion-esta-protegida-mejores**.
7. Más información sobre CSA STAR, disponible en: **https://cloudsecurityalliance.org/star**.
8. Para conocer más sobre FedRAMP, visítese: **https://www.fedramp.gov/**.

02

El CSP muestra resiliencia financiera y el cumplimiento de los principios aceptados de gobernanza corporativa.

03

El CSP permite al CSC mantener la soberanía de la información.

04

El CSP permite la portabilidad de datos (*data portability*) entre diferentes CSP utilizando tecnología aceptada (como una API), al tiempo que admite estándares/formatos abiertos. Esta cuestión es esencial para las copias de seguridad y la continuidad del negocio.

05

El CSP da al CSC acceso a un equipo de seguridad de la información y ciberseguridad, con el fin de consultar y responder a problemas comunes.

06

El CSP ofrece a los CSC un servicio de exhibición de documentos electrónicos, que ayuda a realizar una investigación y verificar el cumplimiento de los requisitos de cumplimiento aceptados (*compliance*).

07

El CSP ofrece soporte para estándares abiertos ampliamente aceptados que ayudan a una gestión eficiente y eficaz, al tiempo que reducen la probabilidad de error al aplicar ajustes de configuración y políticas de seguridad, como por ejemplo, un sistema de gestión de identidades entre dominios (SCIM, por sus siglas en inglés).

Reconocimiento del modelo de responsabilidad compartida

El SRM es una piedra angular en la institucionalización del concepto de seguridad en la nube, y esto se debe a que define con claridad cuál es el compromiso del CSP en materia de ciberseguridad y protección de la información y la privacidad, y también el del CSC.

Cabe señalar que, aunque el nombre del modelo es responsabilidad compartida, muchos requisitos legales y reglamentarios ven al CSC como el único responsable de la ciberseguridad y protección de la información y privacidad. Por consiguiente, la transición al uso de los servicios del CSP no reemplaza ni elimina la responsabilidad exclusiva del CSC por estas cuestiones.

Antes de cerrar un acuerdo de contratación con un CSP, es importante que el CSC verifique el modelo de división de responsabilidad entre las partes y examine su adecuación al perfil de riesgo y nivel de riesgo aceptado por la organización. Dado que durante la contratación se producen cambios en este modelo, la dirección del CSC deberá examinar periódicamente las implicancias que de ello se derivan.

Categoría de identificación (*identify*)

Consiste en identificar el estado actual del riesgo cibernético para la organización.

Mapeo de activos (ID.AM)

Se recomienda que el CSC defina un proceso continuo para mapear activos (como información, *hardware*, *software*, sistemas, instalaciones, servicios, proveedores, personas, centros de datos, zonas, regiones, API), mientras analiza las dependencias entre ellos. Esto incluye que el CSC cuente con medios tecnológicos y otros aceptados que permitan la construcción de diagramas de flujo de datos (*data flow diagram*) con base en la situación real y el historial, así como en relación con el mapeo en tiempo real e histórico de procesos comerciales y/o operacionales (*process flow diagram*).

Dado que no existe una convención para la terminología utilizada por los distintos CSP, es importante crear un cuadro unificado para el mapeo de activos. Por ejemplo, esto sucede con el nombre usado para referirse a un entorno de red restringido en cada CSP. Así, en el entorno de Azure, se utiliza el nombre red virtual (VNeT, por sus siglas en inglés), en GCP y AWS se emplea nube privada virtual (VPC, por sus siglas en inglés) y en la *Oracle Cloud Infrastructure* (OCI, por sus siglas en inglés) se la llama red virtual en nube (VCN, por sus siglas en inglés).

Se recomienda activar los registros de VPC (normalmente no están habilitados de forma predeterminada) y también utilizar capacidades adicionales, como gestión de posturas de seguridad en la nube (CSPM, por sus siglas en inglés) y gestión de posturas de seguridad de datos (DSPM, por sus siglas en inglés). Esto garantizará que el mapeo de todos los activos pertinentes esté disponible para los tomadores de decisiones y el equipo de seguridad de la información y ciberseguridad, lo que puede ayudar a la detección de la existencia de *shadow IT*.

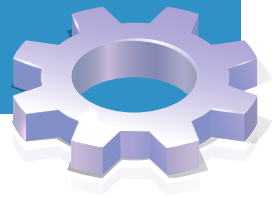
En el siguiente paso, es importante definir un nivel de sensibilidad/criticidad (análisis del impacto en el negocio [BIA, por sus siglas en inglés]) para cada activo, lo que ayudará en el camino a mejorar la eficacia y eficiencia de los procesos de seguridad, como la evaluación de riesgos y el plan de continuidad del negocio (BCP, por sus siglas en inglés) y plan de recuperación ante desastres (PRD, por sus siglas en inglés).

Debe tenerse en cuenta que el CSP puede permitir varias configuraciones de asociación de activos al sistema IAM[9] en la nube pública, donde cada configuración tiene sus propias ventajas e inconvenientes.

A continuación, se muestra una breve descripción general de las configuraciones comunes para asociar activos a la IAM en la nube pública:

- **Configuración de dispositivos registrados:** puede ser adecuada para activos de implementaciones del tipo "traiga su propio dispositivo" (BYOD, por sus siglas en inglés), pero le da al CSC un nivel bajo de comando y control.
- **Configuración de dispositivos vinculados:** es adecuada para activos propiedad del CSC y proporciona un nivel alto de comando y control.
- **Configuración de dispositivos vinculados híbridos:** es apropiada para una situación en la que una organización está en el proceso de transferir sus activos a una nube pública. Por lo general, esta configuración proporciona un nivel alto de comando y control.

Es importante que el CSC defina a nivel individual qué entidades están autorizadas a asociar activos con IAM y de qué manera pueden hacerlo, y establezca un proceso de control periódico para verificar que no haya activos inactivos o maliciosos.



9. El nombre IAM se acepta en la nube pública de AWS y OCI, mientras que en la nube pública de Azure se llama Entra ID y en GCP *Cloud Identity*.

Evaluación de riesgos (ID.RA)

Es recomendable asegurarse de que el proceso de evaluación de riesgos incluya referencias a las siguientes cuestiones:

- Vectores de ataque y tácticas, técnicas y procedimientos (TTP) de *ransomware*, y herramientas de ataque líderes.
- Detección oportuna de vulnerabilidades existentes tanto a nivel del entorno CSC, como a nivel del CSP.
- Uso de CTI para mejorar el nivel de resiliencia y el proceso de evaluación de riesgos.
- Realización de una evaluación de impacto sobre la privacidad (PIA, por sus siglas en inglés) de manera oportuna, de acuerdo con el esquema de la Autoridad de Protección de la Privacidad de Israel.[10]

Aspiración de mejora continua (ID.IM)

Se recomienda que el CSC realice ejercicios periódicos para examinar el nivel de competencia y preparación para hacer frente a un ciberincidente, y adopte medidas de medición aceptadas con el objetivo de aprender lecciones y esforzarse por lograr una mejora continua (INCD y BID, 2022).

Categoría de protección (*protect*)

Consiste en implementar protecciones para prevenir o reducir el riesgo cibernético.

Gestión de identidad, autenticación y control de acceso (PR.AA)

Autenticación multifactor (MFA)

Implementar un factor adicional en la autenticación al conectarse al entorno de nube pública proporciona una capa de protección crucial y valiosa. Un mecanismo de autenticación que incluye solo un nombre de usuario y contraseña está sujeto a fuertes restricciones de seguridad y es un eje de penetración más simple para un atacante. La activación de un factor de autenticación adicional mediante un subprograma específico que admite un mecanismo de reto/respuesta (*challenge/response*) en tiempo real dificulta la conexión para un tercero malicioso.

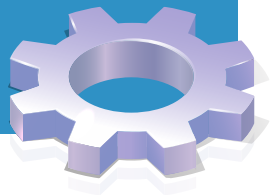
10. La Autoridad publica una guía de referencia metodológica para examinar el impacto sobre la privacidad, una herramienta que ayuda a las organizaciones de la economía a evaluar y reducir los riesgos existentes para la privacidad (Autoridad de Protección de la Privacidad de Israel, 2022): **https://www.gov.il/he/pages/taskir_privacy_news**.

En el caso de cuentas de administrador con altos privilegios o usuarios con un rol sensible (por ejemplo, con amplio acceso a información personal), se recomienda utilizar tarjetas de autenticación de *hardware* que soporten el estándar de identidad rápida en línea II (FIDO II, por sus siglas en inglés), que ofrecen un mejor nivel de inmunidad contra ataques como AiTM.

Cabe señalar que, según la experiencia, exigir la finalización exitosa de una autenticación multifactor como condición antes de completar una operación sensible (como desactivar el mecanismo de administración de versiones en el contenedor *bucket* S3) es una medida de seguridad efectiva y económica.

El uso de una contraseña de acceso permanente y una contraseña temporal en un mensaje de texto (SMS) o correo electrónico no constituye una autenticación multifactor, sino una verificación en dos pasos (2SV, por sus siglas en inglés).

En vista de esto, es recomendable asegurarse de que se aplique el uso de un mecanismo MFA a todos los usuarios, como por ejemplo, usar una contraseña fija en combinación con autenticación biométrica o una tarjeta inteligente que contenga una clave privada.



Uso de políticas de acceso condicional (*conditional access policies*)

Las políticas de acceso condicional otorgan al CSC la capacidad de aplicar procesos de control de acceso individuales, también conocidos como autenticación basada en riesgos (*risk based authentication*) y autenticaciones continuas (*continuous authentications*).

En este marco, es posible comprobar si el usuario y la propiedad (como el punto final) se encuentran dentro de parámetros aceptados antes del proceso de autenticación y durante toda la actividad (*session*), y también si el usuario se ha autenticado exitosamente en el origen.

A continuación, se muestran algunos parámetros habituales:

- (Contexto de) usuario y ubicación
- Aplicación
- Riesgo en tiempo real (inteligencia sobre amenazas, puntuación de riesgo de lavado de dinero, etc.)
- Dispositivo, que incluye la comprobación del estado de la ciberhigiene
- Recurso de destino (máquina virtual, información, etc.)

De esta manera, es habitual que una política de acceso condicional permita aplicar las siguientes reglas:

- Permiso de acceso
- Bloqueo de acceso
- MFA requerida
- Acceso limitado
- Restablecimiento de contraseña
- Monitoreo de acceso

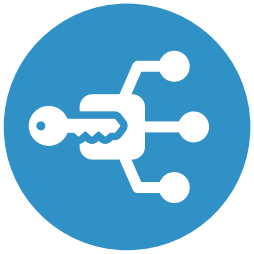
El uso de una política de acceso condicional ofrece un equilibrio entre las necesidades operativas y las de seguridad, lo que aumenta la probabilidad de que el usuario que se conecta al entorno de la nube esté autorizado y provenga de un entorno "saludable".

Control de acceso y política de acceso en una nube pública

En numerosos ataques, el atacante logra afianzarse aprovechando una configuración deficiente (*misconfiguration*) de los permisos de acceso a los recursos existentes en una nube pública.

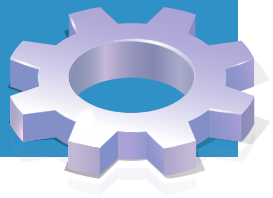
Es habitual que los CSP permitan la aplicación de permisos en dos niveles:

- Control de acceso aplicado a usuarios y entidades a través del sistema IAM.
- Política de acceso aplicada a recursos (como a un contenedor *bucket* S3) que a menudo permite eludir las restricciones aplicadas en el nivel de control de acceso.



En vista de esto, es importante tener un conocimiento profundo de los métodos de trabajo del proveedor de la nube y saber cuál es el enfoque en caso de una contradicción de las definiciones de control de acceso a la política de acceso. Además, es fundamental aplicar los principios de mínimo privilegio, necesidad de saber, necesidad de ver y separación de funciones (SoD, por sus siglas en inglés), y se recomienda que las organizaciones con un entorno complejo ayuden con una solución de administración de derechos de infraestructura en la nube (CIEM, por sus siglas en inglés) o equivalente. Algo que probablemente reduzca la probabilidad de que se produzca un error humano que resulte en un ciberincidente o una infracción. También se recomienda que organizaciones de todo tipo hagan uso de la solución CSPM para monitorear la situación de seguridad en tiempo real y detectar brechas, como la exposición innecesaria de recursos a Internet.

En numerosas ocasiones, en la nube pública es posible aplicar un rol de implementaciones cruzadas (*cross-deployments role*), como los roles de cuentas cruzadas (*cross-account*) al trabajar con AWS, que amplían el alcance de acceso de las cuentas de usuario. Algo que, en ocasiones, permite el acceso desde el entorno CSC de un organismo al entorno del CSC de otro organismo.



Aseguramiento de secretos (*secrets*)

El alcance del uso de secretos en un entorno de nube es alto, por lo que la divulgación de un secreto a una parte no autorizada puede fácilmente terminar en un ciberincidente considerable.

En vista de esto, se recomienda que los CSC adopten los siguientes puntos:

- Establecer y hacer cumplir procedimientos de trabajo que prohíban a los usuarios almacenar secretos en configuraciones no aprobadas.
- Definir procesos de trabajo ordenados para gestionar el ciclo de vida de los secretos, lo que incluye centrarse en un proceso de reemplazo oportuno y reducir la participación humana al mínimo posible.
- Adoptar mecanismos de almacenamiento de secretos de acuerdo con las recomendaciones del CSP, sujeto al cumplimiento de los requisitos de estándares aceptados, como las normas federales de tratamiento de la información: FIPS 140-3 nivel 2 y superiores. Por ejemplo, KMS o HSM.
- Usar herramientas de búsqueda integradas y de otros tipos para detectar continuamente la existencia de secretos en distintos recursos, incluyendo el código fuente.
- Implementar prácticas de detección de secretos (*secrets detection*) en el canal (*pipeline*) de CI/CD (como por ejemplo, realizar una comprobación durante el proceso de envío del código [*code commit*]) y evitar la continuación del proceso de compilación (*build process*) hasta que se aplique el parche necesario.

Uso del mecanismo de gestión de acceso temporal (*just-in time admin*)

Es habitual que los CSP permitan a los usuarios poderosos (como los administradores de red que acceden al panel de administración del CSP) obtener acceso temporal a los activos (*just-in time admin*), lo que reduce la ventana de tiempo válida para llevar a cabo actividades maliciosas, como robo de identidad. Además, algunos CSP permiten la aplicación de mecanismos de seguridad adicionales, como un requisito para obtener la aprobación de dos aprobadores independientes (*dual control*) antes de otorgar acceso al entorno de producción. El uso de estos mecanismos eleva significativamente el nivel de dificultad a la hora de realizar un ataque que tendrá un efecto lateral, como por ejemplo, la propagación del *ransomware* o la eliminación de activos existentes en el CSP.

Configuración de cuentas de emergencia (*break glass accounts*)

Se recomienda configurar cuentas de emergencia que puedan usarse en caso de necesidad. Para proteger estas cuentas, se debe aplicar MFA y aceptar restricciones adicionales, como otorgar acceso solo desde direcciones de protocolo de Internet (IP, por sus siglas en inglés) específicas. Además, es importante monitorear continuamente estas cuentas en caso de que un atacante consiga hacerse con ellas.

Sensibilización y formación (PR.AT)

Si bien los procesos de TI en el entorno de la nube tienen cierta similitud con los que existen en las infraestructuras organizacionales locales (*on-premises*), hay una gran variación en los métodos de trabajo, oferta de plataformas y herramientas accesibles que permiten un trabajo rápido (*agile*) en una configuración distribuida a través de fronteras territoriales. Sin embargo, es habitual que los funcionarios operativos y de seguridad no comprendan cabalmente las implicancias que se derivan de ello.

Ante esto, es importante promover la sensibilización y capacitación de las partes involucradas en los procesos informáticos para mejorar la optimización del proceso de gestión de riesgos y aplicación de los controles necesarios, además de reducir la probabilidad de que se produzca un ciberincidente significativo por error humano (*misconfiguration*).

En relación con este punto, hay varias fuentes de información útiles y gratuitas, entre ellas, las publicaciones desarrolladas por la INCD, la CSA[11], el NIST[12], el Center for Internet Security (CIS)[13] y proveedores de nube reconocidos, las cuales pueden encontrarse en el anexo de esta publicación.

Resiliencia de la infraestructura tecnológica (PR.IR)

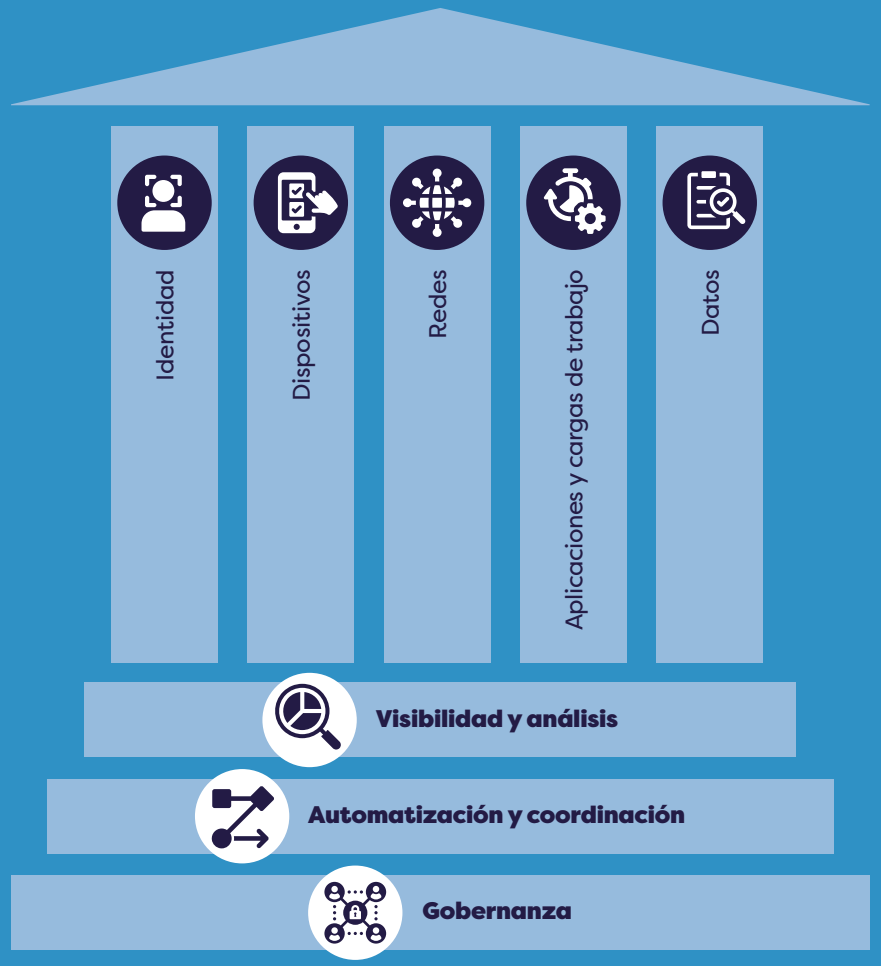
Puesta en práctica de un modelo de madurez confianza cero en la nube (*zero-trust maturity model*)

El concepto de seguridad actual, también conocido como modelo de confianza cero, se basa en el principio "nunca confíes, siempre verifica". Es decir, no existe ninguna computadora o entidad en la que se pueda confiar ciegamente y, por lo tanto, debe ser verificada continuamente.

La organización estadounidense CISA ha desarrollado un modelo de madurez de cuatro niveles que permite a las organizaciones adoptar gradualmente este principio, que se aplica a cinco pilares (Gráfico 5).

11. Más información sobre CSA en: **https://cloudsecurityalliance.org/**.
12. Puede accederse a las publicaciones del NIST en: **https://www.nist.gov/cybersecurity**.
13. Para conocer más sobre el CIS, visítese: **https://www.cisecurity.org/**.

Gráfico 5. Pilares básicos del modelo de confianza cero según el modelo de madurez de CISA



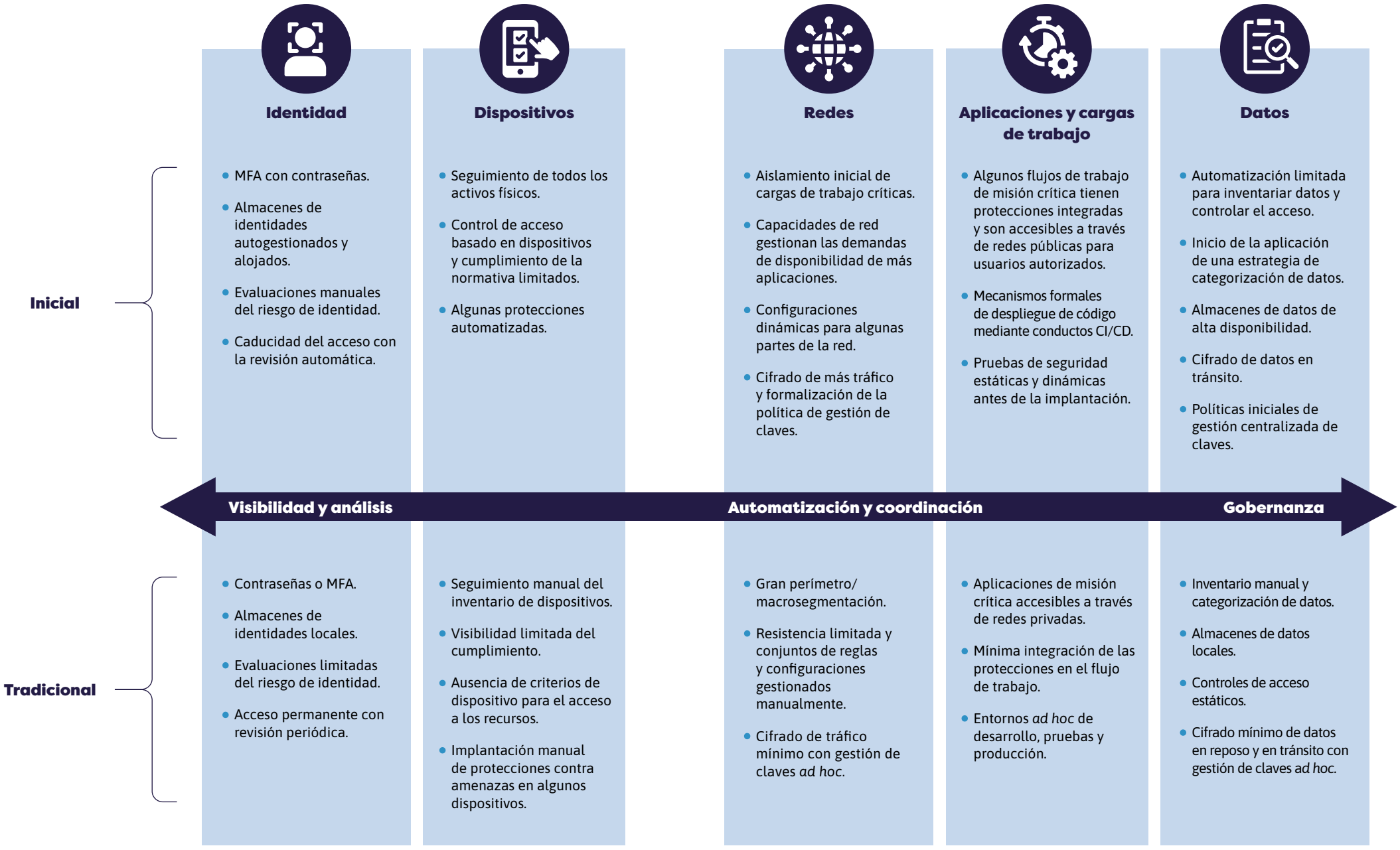
Fuente: CISA (2023).

El Cuadro 5 muestra los cuatro niveles del modelo de madurez. Allí se puede observar que pasar de un nivel a otro aumenta la visibilidad y comprensión situacional acerca del grado de exposición, al tiempo que brinda recomendaciones claras sobre los controles que se deben aplicar para aumentar el nivel de resiliencia.

Cuadro 5. Niveles de madurez según el modelo de confianza cero de CISA

	Identidad	Dispositivos	Redes	Aplicaciones y cargas de trabajo	Datos
Óptimo	• Validación continua y análisis de riesgos. • Integración de identidades en toda la empresa. • Acceso automatizado adaptado a las necesidades.	• Análisis continuo de activos físicos y virtuales, incluida la gestión automatizada de los riesgos de la cadena de suministro y las protecciones integradas contra amenazas. • Acceso a los recursos depende del análisis de riesgos de los dispositivos en tiempo real.	• Microperímetros distribuidos con controles de acceso *just-in-time* y *just-enough* y resiliencia proporcionada. • Evolución de las configuraciones para satisfacer las necesidades del perfil de la aplicación. • Integración de las mejores prácticas para la agilidad criptográfica.	• Aplicaciones disponibles en redes públicas con acceso autorizado continuo. • Protección contra ataques sofisticados en todos los flujos de trabajo. • Cargas de trabajo inmutables con pruebas de seguridad integradas en todo el ciclo de vida.	• Inventario de datos continuo. • Categorización y etiquetado automatizados de datos en toda la empresa. • Disponibilidad de datos optimizada. • Bloqueo de filtraciones (prevención de fugas de datos [DLP, por sus siglas en inglés]). • Controles de acceso dinámicos. • Cifrado de datos en uso.
	Visibilidad y análisis		**Automatización y coordinación**		**Gobernanza**
Avanzado	• MFA a prueba de *phishing*. • Consolidación e integración segura de almacenes de identidades. • Evaluaciones automatizadas del riesgo de identidad. • Acceso en función de las necesidades/sesiones.	• Mayoría de los activos físicos y virtuales se rastrean. • Cumplimiento de la normativa implementado con protecciones integradas contra amenazas. • Acceso inicial a los recursos depende de la postura del dispositivo.	• Ampliación de los mecanismos de aislamiento y resistencia. • Adaptación de las configuraciones en función de las evaluaciones automatizadas de los perfiles de riesgo de las aplicaciones. • Cifrado del tráfico de red aplicable y gestión de la emisión y rotación de claves.	• Mayoría de las aplicaciones de misión crítica disponibles en redes públicas para usuarios autorizados. • Protecciones integradas en todos los flujos de trabajo de las aplicaciones con controles de acceso basados en el contexto. • Equipos coordinados de desarrollo, seguridad y operaciones.	• Inventario de datos automatizado con seguimiento. • Categorización y etiquetado coherentes, escalonados y específicos. • Almacenes de datos redundantes y de alta disponibilidad. • DLP estático. • Acceso automatizado basado en el contexto. • Cifrado de datos en reposo.
	Visibilidad y análisis		**Automatización y coordinación**		**Gobernanza**

▼ (continúa)



Fuente: CISA (2023).

Debido a su brevedad, esta publicación no puede revisar el modelo de madurez en su totalidad, pero presenta varios puntos importantes para su adopción por parte del CSC.

Planificación adecuada de una jerarquía común de recursos en un entorno de nube pública

Es habitual que los proveedores de la nube construyan una jerarquía de recursos, cuyo propósito es permitir la separación de entornos, la compartimentación individual y la reducción de la zona de daño (*blast zone*) en caso de un ciberincidente u otro incidente inusual.

El modelo común contiene una superorganización, bajo la cual se pueden definir grupos que a su vez pueden contener uno o más entornos de implementación. De esta manera, los entornos que comparten un mismo grupo pueden compartir una política conjunta que se aplicará mediante herencia (como una obligación o una opción modificable) desde el nivel de la superorganización o al nivel del propio grupo.

Además, se acepta que una política se puede aplicar a nivel del entorno de implementación, de acuerdo con la política superior descrita.

El Gráfico 6 presenta una jerarquía común de recursos en un entorno de nube pública.

Gráfico 6. Jerarquía común de recursos en un entorno de nube pública

Fuente: CSA (2024).

Cuadro 6. Terminología aceptada de los principales proveedores de nube

Implantación	Grupo	Organización	Proveedor de servicios en la nube
Cuentas	Unidad organizativa	Organización	AWS
Subcompartimento	Compartimento raíz	Arrendamiento	OCI
Proyectos	Carpetas	Organizaciones	GCP
Suscripciones	Grupo de recursos	Inquilino	Microsoft Azure

Fuente: Elaborado sobre la base conceptual de la CSA (2024).

A continuación, se muestran algunos puntos para la correcta planificación de la jerarquía de recursos en una nube pública, incluyendo la definición de la zona de aterrizaje:

01

Se recomienda utilizar el *well-architected framework* para la correcta planificación de la jerarquía organizacional, teniendo en cuenta los retos operativos y de seguridad. Algunos de los proveedores de la nube proporcionan a los CSC herramientas (como *account factory*) que permiten implementar la jerarquía recomendada y construir una zona de aterrizaje (*landing zone*), al tiempo que reducen la necesidad de establecer manualmente la jerarquía de recursos (tanto durante el establecimiento inicial como cuando es necesario recuperarse en caso de emergencia). Es habitual que las herramientas utilicen infraestructura como código (IaC, por sus siglas en inglés) y, por tanto, pueden ayudar en la recuperación ante desastres.

02

Es recomendable asegurarse de que se utilicen protocolos y servicios que no contengan una vulnerabilidad conocida (como IMDS v1.0), y que no sea posible establecer nuevos recursos que utilizan protocolos y servicios con una vulnerabilidad conocida.

03

Se sugiere aplicar una política que defina de antemano dónde se pueden establecer nuevos recursos a nivel físico y lógico y dónde se pueden mover los recursos existentes. Esto facilitará la puesta en práctica de principios aceptados para una gobernanza de la información eficaz y eficiente.

04

Se recomienda diseñar la política de seguridad organizacional (como las políticas de control de servicios [SCP, por sus siglas en inglés] en AWS) y los procesos de autorización, de manera de minimizar la posibilidad de un error humano que cause exposición. En este aspecto, existe preferencia por el uso de política como código (PaC, por sus siglas en inglés).

05

Se sugiere planificar la política operativa, como la relativa a los nombres de las etiquetas y la ubicación permitida para el establecimiento de nuevos recursos, de modo que ayude a reducir los errores humanos que pueden conducir a la exposición.

06

Se recomienda verificar la transferencia de los registros de seguridad a un entorno de implementación (*deployment*) específico, que tendrá un alto nivel de compartimentación.

07

Como regla general, es poco frecuente que el equipo de tecnologías de la información y las comunicaciones (TIC) del CSC normalmente realice operaciones a nivel de organización y/o haga uso de entidades de este nivel (como cuentas de usuarios con altos privilegios). Por consiguiente, es necesario asegurarse de que el monitoreo cibernético cubra este tema. Es necesario aplicar la SoD, de modo que un agente administrativo no pueda realizar cambios a este nivel.

08

Al conectar una VPC a otra VPC (y similares), se recomienda utilizar tecnología que transmita la información en el plano posterior del CSP, de modo de asegurarse de que la información no pase por Internet, por ejemplo, AWS PrivateLink.

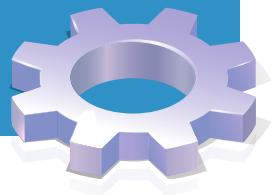
09

Es recomendable asegurarse de que al crear un nuevo recurso o al transferir un recurso existente a otra implementación, se le apliquen automáticamente los requisitos de seguridad aceptados, como una política para implementar actualizaciones de seguridad, ejecutar registros que normalmente no están activos y enviar una copia de ellos al repositorio de almacenamiento centralizado (*data lake*) y/o al sistema de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés), de manera de implementar un agente de plataforma de protección de la carga de trabajo en la nube (CWPP, por sus siglas en inglés).

10

Es recomendable asegurarse de aplicar una política para evitar la eliminación o modificación de recursos confidenciales (*resource lock*).

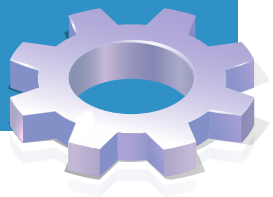
El resto de la publicación incluye una referencia al tema de mantenimiento de copias de seguridad y aseguramiento de la información, con lo que se amplía el tema sobre la planificación adecuada de una jerarquía común de recursos en un entorno de nube pública.



Diseñar una arquitectura para una plataforma SaaS que se ejecuta sobre un CSP

Uno de los retos comunes es que las organizaciones que desean utilizar una plataforma SaaS que se ejecuta sobre un CSP no son suficientemente conscientes de los problemas importantes que allí puede haber, lo que puede crear graves brechas de seguridad. Por ejemplo, la diferenciación entre distintos clientes que comparten los mismos recursos de la plataforma SaaS suele ser un talón de Aquiles. Las organizaciones interesadas en construir una plataforma SaaS que se ejecute en un CSP tampoco son conscientes de que los CSP ofrecen diferentes tecnologías, como VPC Endpoints y el uso de una línea de comunicación específica entre el sitio del cliente y la red CSP (como AWS Direct Connect), lo que reduce considerablemente la superficie de ataque. Se recomienda utilizar las guías por encargo de los CSP que incluyen explicaciones e instrucciones sobre cómo configurar y administrar una plataforma SaaS.

Al planificar una arquitectura para una plataforma SaaS, es recomendable asegurarse de que se haga referencia al uso de cortafuegos de aplicaciones web/autoprotección de aplicaciones en tiempo de ejecución/protección de aplicaciones web y API (WAF/RASP/WAAP, por sus siglas en inglés) como control compensatorio. También se sugiere que el CSC utilice la solución de gestión de posturas de seguridad de SaaS (SSPM, por sus siglas en inglés) como control compensatorio, y que no confíe exclusivamente en el sistema de seguridad del CSP.[14]



14. Para más información, véase Design SaaS on AWS, disponible en: **https://aws.amazon.com/saas/design/**.

Implementación de medidas aceptadas para hacer frente al *malware*

Se recomienda implementar medidas aceptadas para hacer frente al *malware*, tales como CWPP, en todas las puertas de enlace (*gateways*) de entrada/salida de información, así como en los propios recursos. Para eso, deben considerarse las siguientes cuestiones:

01

En numerosas ocasiones, el fabricante de la solución CWPP es un CSP en sí mismo y, en otras oportunidades, se utiliza el anidamiento en la nube cuando se trata de soluciones de seguridad de terceros.

02

Es necesario asegurarse de que la solución CWPP transfiera los registros lo antes posible al sistema de monitoreo, esto a la luz del hecho de que la vida útil de los recursos (como los contenedores) es corta en el entorno de la nube pública.

03

Es importante que el CSC cuente con una solución de seguridad capaz de dar respuesta a la itinerancia (*roaming*) de activos entre diferentes entornos, como infraestructuras organizativas locales, un entorno de nube pública y trabajo desde casa.

04

Es recomendable asegurarse de que la solución elegida pueda proporcionar una respuesta de seguridad óptima al trabajar en una configuración BYOD, por ejemplo, puesta en práctica de capacidades de seguridad aceptadas en una solución de gestión de dispositivos móviles/gestión de la movilidad empresarial (MDM/EMM, por sus siglas en inglés).

05

Se sugiere asegurarse de que la solución elegida sea capaz de producir análisis forense digital a partir de los distintos recursos, para que se pueda llevar a cabo una investigación eficaz.

06

Al recibir archivos en las puertas de enlace de entrada/salida se recomienda incorporar comprobaciones de desarme y reconstrucción de contenidos (CDR, por sus siglas en inglés) (o blanqueamiento) aceptadas.

07

Es importante asegurarse de que la solución elegida sea capaz de proporcionar una respuesta eficaz contra las amenazas de día cero y de día uno.

08

Es necesario asegurarse de que la solución elegida presente los resultados de acuerdo con la última versión del marco MITRE ATT&CK, y también que el fabricante mantenga un nivel óptimo de cobertura en relación con sus últimas versiones.

Implementar medidas comunes para hacer frente a los ataques DDoS

Se recomienda implementar medidas comunes para hacer frente a los ataques DDoS. Para eso, pueden utilizarse herramientas integradas en el entorno CSP y/o de un tercero, y deben considerarse las siguientes cuestiones:

01

Es recomendable asegurarse de que la solución elegida proporcione una respuesta óptima a las distintas familias de ataques DDoS (como ataques volumétricos, ataques de protocolo y ataques a la capa de aplicación).

02

Es importante que la herramienta elegida incluya un mecanismo de monitoreo continuo para detectar ataques DDoS y tomar acciones que permitan al CSC continuar con la rutina de las actividades comerciales y acciones operativas para neutralizar la infraestructura del atacante.

03

En numerosas ocasiones, los CSP ofrecen varios niveles de seguridad contra ataques DDoS, por lo que se recomienda que el CSC adopte un nivel de seguridad que incluya monitoreo continuo y servicio de tratamiento individual ante incidentes inusuales por parte del CSP, como la neutralización de la infraestructura del atacante.

04

El uso de una CDN y la capacidad de ajustar automáticamente la cantidad y tamaño de los recursos informáticos (*autoscaling*) es un medio eficaz y eficiente para reducir el efecto de un ataque DDoS. En vista de eso, estas capacidades deben adoptarse al planificar e implementar la arquitectura, y mientras se realizan mejoras periódicas de acuerdo con la actualización del panorama de amenazas.

Segmentación y segregación

La aplicación de principios aceptados de segmentación de red es un medio eficaz que dificulta que los atacantes realicen movimientos laterales (*lateral movements*) para obtener un control lateral de los activos. A continuación, se presentan algunos puntos importantes para implementar la partición de red:

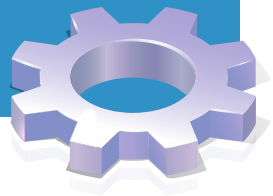
01

Se recomienda configurar la política de reglas para que todo el tráfico esté bloqueado de forma predeterminada (denegar por defecto). Dado que algunos CSP adoptan una política en la que el tráfico hacia el exterior está activo de forma predeterminada, es necesario cambiar las definiciones de reglas predeterminadas durante el establecimiento del entorno y los diversos recursos.

02

Limitar correctamente la conectividad entre los componentes básicos de la red y los distintos recursos permite la segmentación y dificulta que un atacante se afiance. Para ello, es importante planificar adecuadamente la VPC/VNet, así como la lista de control de acceso a la red (NACL, por sus siglas en inglés) y los grupos de servicios (*service groups*), mediante una examinación periódica de la situación existente en relación al perfil de riesgo. En este sentido, la recomendación aceptada de los principales CSP es implementar la microsegmentación, de modo que cada activo opere en un entorno de red específico, al cual se permitirá el acceso según el principio de mínimo privilegio (PoLP, por sus siglas en inglés).

Es recomendable asegurarse de que el CSP asigne a cada VPC (o su equivalente) un identificador de red de área local virtual extensible (VXLAN, por sus siglas en inglés) o un identificador de encapsulamiento de virtualización de red genérica (Geneve, por sus siglas en inglés) específico. El uso de una red de área local virtual (VLAN, por sus siglas en inglés) para la segmentación de redes no se considera efectivo en la actualidad.



03

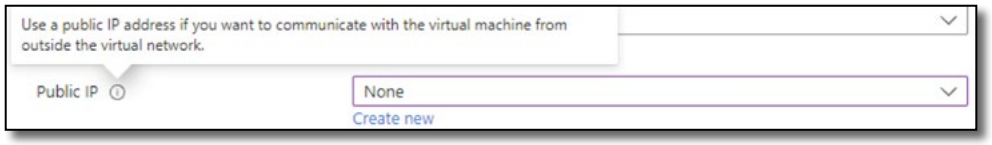
Se recomienda que las organizaciones relativamente grandes y/o aquellas con un entorno complejo y/o información confidencial hagan uso de un cortafuegos de nueva generación (NGFW, por sus siglas en inglés) específico, que estará ubicado en el centro de tránsito de la red (*network transit hub*), para que las políticas de control de acceso puedan aplicarse de manera centralizada y así obtener un alto nivel de visibilidad.

04

Se recomienda asignar direcciones IP no enrutables a recursos que no sean necesarios para el acceso directo a Internet.

A continuación, la Imagen 1 muestra un ejemplo de cómo aplicar la configuración anterior (*none*) al crear una nueva máquina virtual en Azure.

Imagen 1. Configuración al crear una máquina virtual en Azure



05

Se recomienda realizar un registro del tráfico para mejorar la visibilidad. Por lo general, esto puede conseguirse al activar un puerto espejo (*port mirroring*) en el nivel de recursos (por ejemplo, una máquina virtual) y copiar el tráfico al sensor.

Gestionar cambios y aplicar ajustes de configuración

Los procesos de gestión de cambios y aplicación de ajustes de configuración son la piedra angular de los procesos de TI, por lo que su correcta aplicación debería ayudar al CSC a reducir la probabilidad de errores humanos que puedan causar un ciberincidente.

Como parte de esto, se recomienda que el CSC examine la implementación de los siguientes puntos:

01

Examen continuo del estado de seguridad del entorno en relación con una línea de base aceptada. Mediante un examen continuo del entorno en relación con una línea de base aceptada, como el *CIS Benchmark*, es posible localizar brechas de seguridad, como las leyes de cortafuegos permisivas.

02

Uso de herramientas integradas para mantener los ajustes de configuración aprobados. Al utilizar herramientas integradas en el entorno de la nube, como AWS Config, es posible detectar anomalías/cambios no autorizados en los ajustes de configuración (*drifting*), y realizar una restauración al estado deseado de forma automática o semiautomática.

03

Uso de IaC. El uso de IaC puede ayudar a garantizar que el entorno esté en el estado deseado y que de ser necesario pueda realizarse la recuperación rápida de un desastre mediante el establecimiento de un nuevo entorno y la transferencia a este de la información.

04

Política de gestión de contraseñas. Se recomienda que una política de gestión de contraseñas impida usar contraseñas predeterminadas y evite el uso contraseñas que se hayan filtrado en el pasado. Se sugiere adoptar una política que requiera contraseñas largas y únicas mientras se verifica que la contraseña no aparezca en bases de datos de contraseñas comunes, por ejemplo en repositorios de contraseñas previamente filtradas, predeterminadas o débiles, y tablas arcoíris (*rainbow tables*), y cuando sea necesario verificar que el proceso de reemplazo de contraseña se realice de forma automática.

05

Cumplimiento del uso de mecanismos aceptados para proteger los secretos. El uso de mecanismos de seguridad aceptados, como KMS, para proteger los secretos aumenta la probabilidad de que los atacantes no puedan acceder abiertamente a ellos. Es importante verificar que el proceso de desarrollo seguro requiera que todas las versiones de *software* (incluyendo las que están en fase de desarrollo y prueba) hagan uso de estos mecanismos de forma predeterminada. Como control compensatorio, se recomienda realizar comprobaciones periódicas del código fuente y de los activos para detectar el almacenamiento de secretos contrarios a la política corporativa.

06

Impedir el acceso a las interfaces de gestión. Se recomienda bloquear de forma predeterminada el acceso a las interfaces de gestión (como RDP y SSH) de activos, como una máquina virtual y un contenedor (*container*). Como alternativa a conectarse a una máquina virtual, puede utilizar Bastion Host u otra solución segura.

Seguridad de la arquitectura sin servidor (*serverless*)

La arquitectura sin servidor ofrece capacidades operativas avanzadas, que normalmente están disponibles para todos los CSC de forma predeterminada. Con el fin de reducir la posibilidad de aprovechamiento de la arquitectura sin servidor, se recomienda adoptar los siguientes puntos:

- Documentar el ciclo de vida de la actividad de funciones.
- Otorgar privilegios bajos (*least privilege*) a la función, mientras se verifica que este principio también se aplica cuando hay una cadena entre diferentes funciones, por ejemplo, una función que llama a otra función.
- Garantizar que no sea posible implementar un ataque de serialización contra la función.
- Controlar y supervisar los componentes de *software* integrados en la función.
- Asegurarse de que los componentes de *software* de las funciones estén incluidos en el proceso organizacional destinado a detectar y manejar vulnerabilidades de seguridad.

Desarrollo seguro (*secure development*)

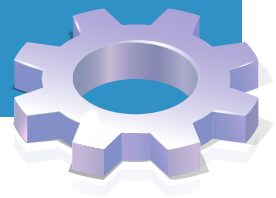
Se recomienda que un CSC que desarrolle *software* y/o lo adquiera de un tercero y/o adopte código abierto garantice que cumple con los requisitos aceptados para un desarrollo seguro, tales como:

- Seguro por diseño y seguro por defecto *(secure by design and secure by default)*.
- Privacidad desde el diseño y privacidad por defecto (*privacy by design and privacy by default*).

En este sentido, se recomienda que el CSC adopte las recomendaciones de desarrollo del CSP y verifique que el servicio o producto cumpla con los requisitos aceptados, como el estándar de verificación de seguridad en aplicaciones (ASVS, por sus siglas en inglés) nivel tres de OWASP,[15] y el estándar de verificación de seguridad en aplicaciones móviles (MASVS, por sus siglas en inglés) nivel tres de OWASP.[16]

Se recomienda que el CSC tenga una copia actualizada de la lista de materiales de *software* (SBOM, por sus siglas en inglés) de los componentes que utiliza. También se sugiere que los CSC que utilizan plataformas SaaS establezcan a nivel contractual que el CSP les proporcionará una lista de materiales de *software* como servicio (SaaSBOM, por sus siglas en inglés) para cada versión.

Entonces el CSC podrá integrar el SBOM/SaaSBOM en su proceso de gestión de vulnerabilidades, lo que a su vez contribuirá a la existencia de un proceso de gestión de riesgos informado.[17]



15. Para más información sobre OWASP ASVS, véase **https://owasp.org/www-project-application-security-verification-standard/**.
16. Puede leerse más sobre OWASP MASVS en **https://mas.owasp.org/MASVS/**.
17. Para más información, véase NIST (2022): **https://csrc.nist.gov/pubs/sp/800/218/final**; CISA SBOM **(https://www.cisa.gov/sbom)**; y CISA Open Source Security (**https://www.cisa.gov/opensource**).

Aseguramiento de las capacidades de inteligencia artificial

El uso de una nube pública brinda a los CSC un fácil acceso a capacidades avanzadas de inteligencia artificial (IA). Ya sea el uso del servicio IA generativa como base para un chatbot que brinde una respuesta de servicio al cliente, acceso a infraestructura y herramientas que permitan la adaptación de modelos existentes a las distintas necesidades del negocio o desarrollo de nuevos modelos desde cero, y similares. Ante esto, es importante que el CSC se asegure de haber implementado y activado durante todo el ciclo de vida medidas de seguridad aceptadas para proteger las capacidades de IA que utiliza. Se recomienda que el CSC cuente con una copia actualizada de la lista de materiales de IA (AIBOM, por sus siglas en inglés) de los componentes de IA que utilice. Luego, el CSC podrá integrar el AIBOM en su proceso de gestión de vulnerabilidades, lo que a su vez contribuirá a la existencia de un proceso de gestión de riesgos informado.[18]

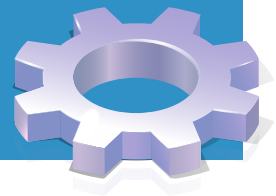
Control sobre el registro y uso de aplicaciones, complementos (*plug-in*) y *marketplace*

Se recomienda que el CSC tome medidas aceptadas para controlar el registro y el uso de aplicaciones, complementos y *marketplace*. Esto incluye adoptar una política de bloqueo por defecto (*deny by default*) y permitir el registro y uso de aplicaciones, complementos y *marketplace* a nivel individual. Del mismo modo, se sugiere que los permisos otorgados al equipo de desarrollo para registrar nuevas aplicaciones (incluyendo las versiones alfa, beta, etc.) no les posibiliten distribuir la aplicación y el complemento al entorno de producción y/o al entorno real, sin obtener aprobación previa de acuerdo con el proceso de gestión de cambios aprobado por el CSC.

18. Para más información, véase NIST (2023a): **https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development**; NIST (2023b): **https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook**; ISO/IEC 42001:2023 (**https://www.iso.org/standard/81230.html**); MITRE ATLAS: **https://atlas.mitre.org/**; CSA. (2024): **https://cloudsecurityalliance.org/artifacts/ai-model-risk-management-framework**.

Debe tenerse en cuenta que muchas plataformas SaaS permiten de forma predeterminada a los usuarios acceder al *marketplace*, lo que les da la opción de descargar nuevas aplicaciones, nuevos complementos y/o agregar nuevas funcionalidades. De esta manera, en algunos casos la información organizacional puede pasar a través de ellos a un tercero, como por ejemplo un CSP secundario.

En vista de esto, es recomendable asegurarse de que antes de comenzar a utilizar la plataforma SaaS, el CSC defina una política clara de seguridad de la información y ciberseguridad, que delinee un proceso ordenado para aprobar el uso de aplicaciones y agregar nuevas funcionalidades.



Seguridad de la plataforma (PR.PS)

Reducción de la superficie de ataque (*attack surface*) y endurecimiento

Se recomienda tomar periódicamente acciones aceptadas para la reducción de la superficie de ataque y el endurecimiento. Esto incluye considerar las siguientes cuestiones:

01

Reducir el número de interfaces de gestión accesibles desde Internet, tanto a nivel de las interfaces de gestión del CSP, como a nivel de las distintas plataformas. Como alternativa, pueden utilizarse Bastion Host y otras soluciones aceptadas.

02

Instalar actualizaciones de seguridad de manera oportuna y con una frecuencia adecuada al perfil de riesgo. En general, se recomienda instalar actualizaciones de seguridad en propiedades directamente expuestas a Internet hasta 24 horas después de su publicación.

03

Utilizar herramientas como CIS Benchmark para identificar brechas de seguridad en el entorno del CSC y cerrarlas lo antes posible.

04

Endurecer las plataformas según sus metodologías aceptadas, tales como CIS (nivel 2 como mínimo)[19] y las guías de implementación técnica de seguridad de la Agencia de Sistemas de Información de Defensa (DISA STIG, por sus siglas en inglés)[20] (nivel 2 como mínimo).

05

Eliminar y neutralizar componentes y servicios de *software* que no son necesarios para la actividad comercial rutinaria, incluyendo los servicios para compartir archivos.

06

Verificar que la seguridad de las plataformas cubre las TTP pertinentes mientras se ponen en práctica los mecanismos de seguridad necesarios de acuerdo con la Matriz del marco de detección, denegación y disrupción que potencia la defensa de la red (D3FEND, por sus siglas en inglés).[21]

Aseguramiento de máquinas virtuales y contenedores

En general, la percepción en el entorno de la nube es que un recurso (como una máquina virtual y contenedores), excepto la información en sí, es temporal (*ephemeral*). Otra percepción habitual es que un activo/infraestructura en el entorno de producción no realiza cambios (*immutable*), sino que los cambios necesarios para su aplicación se llevan a cabo mediante la asimilación de una nueva propiedad y la eliminación de la antigua. La adopción de estos conceptos permite al CSC reducir la superficie de ataque y obtener la capacidad de recuperarse más rápido en caso de un ciberincidente o fallo operativo.

Además, es importante aplicar procesos de protección a los activos, como cerrar las interfaces de gestión y evitar la posibilidad de iniciar sesión localmente. Todo esto reduce la ventana de oportunidad del atacante y es un paso importante para mejorar la resiliencia organizacional.

Como control compensatorio, las organizaciones pueden hacer uso de CWPP y otras soluciones de seguridad.

Otra cuestión es el control y seguimiento del proceso de elección de las imágenes para incrustar, con el fin de garantizar que estas no contengan código malicioso. Por consiguiente, se recomienda que el CSC trabaje con un registro de contenedores/imágenes confiable y que, como parte del proceso CI/CD, se verifique la fiabilidad de los componentes del *software* utilizando herramientas aceptadas, como gestión de la seguridad de las aplicaciones (ASPM, por sus siglas en inglés).

Aseguramiento de interfaces API

Para proteger las interfaces API, se recomienda adoptar las siguientes medidas:

01

Minimización de la exposición. Evitar que las interfaces API del CSC queden expuestas directamente al mundo mediante el uso de API GW, que aplica una política de seguridad aceptada. Esto incluye:

- **A** Aplicar una verificación de esquema (*schema*) y contenido de acuerdo con una lista predefinida de parámetros (*allowlist*).
- **B** Imponer un método de autenticación fuerte según el perfil de riesgo. A continuación, se muestran algunos ejemplos:
  - Una API que esté destinada a M2M utilizará una seguridad de la capa de transporte mutua (mTLS, por sus siglas en inglés).
  - Una API que esté destinada a una implementación H2M requerirá el uso de MFA.
- **C** Hacer cumplir el método de gestión de *tokens* según el perfil de riesgo. Por ejemplo:
  - Firmar digitalmente un *token* o utilizar otra técnica de seguridad.
  - Usar un *token* que no cree una brecha de seguridad. Por ejemplo, por regla general, un *token* web de notación de objetos JavaScript (JWT, por sus siglas en inglés) puede utilizarse en una actividad en el entorno interno del CSC, pero no con usuarios ubicados fuera de este entorno (como un cliente que se conecta al sitio web desde su estación final en el hogar).
- **D** Limitar la cantidad de solicitudes en un período de tiempo determinado a las que una API específica puede responder (*API throttling*).

19. Más información sobre CIS Benchmarks disponible en: **https://www.cisecurity.org/cis-benchmarks**.

20. Pueden encontrarse las STIG de DISA en: **https://public.cyber.mil/stigs/**.

21. Véase la matriz D3FEND en: **https://d3fend.mitre.org/**.

E Limitar la cantidad de solicitudes que un solo cliente puede realizar a una API específica en un período de tiempo específico (*rate limiting*).

F Limitar el acceso a la API por ubicación geográfica (*geolocation*).

G Aplicar un modelo de gestión de permisos de acceso según sea necesario, como el control de acceso detallado (*fine-grained access control*).

H Documentar las solicitudes y remitirlas para su análisis por parte del equipo cibernético y de protección de la información.

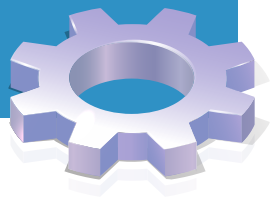
02

Aseguramiento de secretos. Utilizar los medios recomendados por el proveedor de la nube para almacenar los secretos.

03

Desarrollo seguro. Asegurarse que las API se desarrollen de acuerdo con los principios aceptados para el desarrollo seguro y que cada versión se pruebe utilizando herramientas automatizadas aceptadas (por ejemplo, pruebas estáticas de seguridad de aplicaciones/análisis de composición de *software*/pruebas dinámicas de seguridad de aplicaciones/pruebas interactivas de seguridad de aplicaciones [SAST/SCA/DAST/IAST, por sus siglas en inglés]), revisiones de código (*code reviews*) y pruebas de resiliencia. Esto se debe a que la seguridad del proceso de gestión de *tokens* y sesiones es de gran importancia. Es posible utilizar estándares aceptados, como OpenAPI, para validar la implementación efectiva.

Se recomienda asegurarse de que la herramienta SCA admita escanear bibliotecas de código abierto que estén almacenadas claramente (*clear*), y también bibliotecas almacenadas en formato binario (*binary*), como código aceptado.



Uso del servicio de acceso seguro Edge

Se recomienda que las organizaciones que utilizan varios servicios en la nube y/o operan desde una gran cantidad de sucursales, examinen la posibilidad de utilizar la solución de servicio de acceso seguro Edge (SASE), que es la alternativa a la solución VPN tradicional. El uso de la solución SASE permite aplicar una política de seguridad de forma centralizada, con lo que se obtiene un alto nivel de visibilidad, además de mejorar la experiencia del cliente (UX, por sus siglas en inglés). Esto puede verse reflejado en la respuesta a sus solicitudes desde la granja de servidores cercana a su ubicación geográfica, lo que asegura un bajo tiempo de respuesta. Una razón igualmente importante para preferir el uso de SASE es que, en los últimos años, se descubrieron importantes brechas de seguridad en muchas soluciones VPN tradicionales, cuya corrección llevó mucho tiempo. Incluso se ha descubierto más de una vez que la modificación publicada no es efectiva y/o genera un daño comercial significativo. Asimismo, en numerosas ocasiones se constata que el parche no corrige el problema fundamental que muchas veces surge de no adoptar enfoques aceptados al desarrollar la solución VPN, como *secure by design* y *secure by default*. Por consiguiente, es posible encontrar una repetición de problemas de seguridad derivados del mismo problema fundamental.

Aseguramiento de la plataforma para enviar mensajes (como correo electrónico) en la configuración SaaS

Se acepta que el CSP proporcione una infraestructura para enviar mensajes (por ejemplo, correo electrónico) en una configuración SaaS. Aquí la plataforma, por lo general, podrá permitir dos configuraciones de trabajo:

- Aplicación a aplicación (A2A, por sus siglas en inglés).
- Aplicación a persona (A2P, por sus siglas en inglés).

Para reducir la posibilidad de que se aproveche una plataforma de envío de mensajes en configuración SaaS, se recomienda adoptar las siguientes medidas:

- Verificar de forma periódica que la lista de destinatarios se ajusta a las necesidades de negocio del CSC.
- Comprobar de forma periódica que la configuración de publicación y suscripción (Pub/Sub), incluyendo las aplicaciones/servicios que pueden interactuar, satisface las necesidades comerciales del CSC.

- Aplicar medidas de seguridad habituales en el envío/recepción, como activar el mecanismo de autenticación de mensajes basada en dominios, informes y conformidad (DMARC, por sus siglas en inglés) y configurar un registro indicador de marca para la identificación de mensajes (BIMI, por sus siglas en inglés), así como filtrado de spam y *malware*.

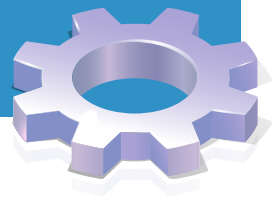
- Aplicar una definición clara de los tipos de mensajes y características aceptadas (como tamaño y frecuencia de envío).

- Realizar pruebas periódicas de muestreo para verificar que el contenido de los mensajes no incluye información inusual.

Aseguramiento de la infraestructura organizacional local

Se recomienda tomar medidas aceptadas para proteger las infraestructuras organizativas locales, lo que incluye los puestos directivos y el sistema de gestión de identidad (como *Active Directory* [AD]). Asimismo, para mejorar el nivel de visibilidad, se recomienda implementar una solución de agente de seguridad de acceso a la nube (CASB, por sus siglas en inglés) en los accesos de enlace a redes públicas, como Internet. Esto es algo que también puede ayudar a afrontar las amenazas que surgen de las actividades de *shadow IT*.

A la hora de implementar una infraestructura de federación, es recomendable asegurarse de que los servidores expuestos a Internet estén protegidos mediante WAF/WAAP.



A continuación, el Recuadro 1 presenta ejemplos de ataques comunes contra AD, frente a los que se recomienda que el CSC verifique la existencia de un nivel adecuado de resiliencia.

Recuadro 1. Ejemplos de ataques comunes contra DA

- AD Enumeration (Enumeración AD)
- AdminCount (AdminCount)
- adminSDHolder (adminSDHolder)
- ASREPRoast / Authentication Server Response (AS-REP) Roasting (ASREPRoast / Respuesta del servidor de autenticación [AS-REP] Roasting)
- BloodHound Reconnaissance (Reconocimiento BloodHound)
- DCShadow (DCShadow)
- DCSync (DCSync)
- Default/Hard-coded Credentials (Credenciales por defecto/codificadas)
- Diamond Ticket (Ticket diamante)
- Forge IPv6 Gateway (Pasarela IPv6 falsificada)
- Golden Ticket (Billete dorado)
- Kerberoasting (Kerberoasting)
- LDAP Anonymous Login (Binding) (Inicio de sesión anónimo de protocolo ligero de acceso a directorios)
- LDAP Injection (Inyección LDAP)
- Local Loop Multicast Name Resolution (LLMNR) Poisoning (Envenenamiento de la resolución de nombres de multidifusión de bucle local)
- MachineAccountQuota Compromise (Compromiso de MachineAccountQuota)
- Misuse Access Control List (ACL) Misconfiguration (Uso indebido de lista de control de acceso. Configuración incorrecta)
- NBT-NS Poisoning (Envenenamiento de NetBIOS sobre TCP/IP)
- NTDS.dit Extraction (Extracción NTDS.dit)
- NTLM Relay (Retransmisión NT LAN Manager)
- Pass-the-Hash (PtH) (Ataque Pass-the-Hash)
- Pass-the-Ticket (PtT) (Ataque Pass-the-Ticket)
- Password Spraying (Rociado de contraseñas)
- PetitPotam NTLM Relay Attack on an Active Directory Certificate Services (AD CS) (Ataque de retransmisión NTLM PetitPotam en un servicio de certificados de *Active Directory* [AD CS])
- SAML Golden Attack (Ataque Golden SAML)
- SID History Injection Attack (Ataque de inyección de historial identificador de seguridad)
- Silver Ticket (Ticket plateado)
- Skeleton Key Attack (Ataque Skeleton Key)
- Unconstrained delegation (Delegación no restringida)
- Wdigest: Extracting Passwords in Cleartext (Wdigest: Extracción de contraseñas en texto claro)

Nota: La lista anterior no es exhaustiva de ataques frente a los que el CSC debe garantizar la existencia de un nivel adecuado de resiliencia.

A continuación, se muestran algunos puntos a la hora de implementar un CASB:

01

Asegurarse de que la arquitectura de implementación esté en línea.

02

Garantizar que el tráfico cifrado se abra antes de que llegue al usuario, con el objetivo de localizar y frustrar amenazas en el medio cifrado.

03

Asegurarse de que la solución elegida sea capaz de localizar aplicaciones punto a punto (P2P, por sus siglas en inglés) comunes y, en consecuencia, aplicar una política de seguridad acorde con los requisitos del CSC. Esto incluye responder a aplicaciones que usan WinSocket, Reverse Tunnel y Web 3.0 (como aplicaciones que usan el protocolo del sistema de archivos interplanetario [IPFS, por sus siglas en inglés]).

04

Asegurarse de que la solución seleccionada tenga capacidad de análisis del comportamiento de usuarios y entidades (UEBA, por sus siglas en inglés).

05

Asegurarse de que la solución seleccionada tenga capacidad DLP.

06

Asegurarse de que la solución seleccionada tenga capacidad de aislamiento remoto del navegador (RBI, por sus siglas en inglés).

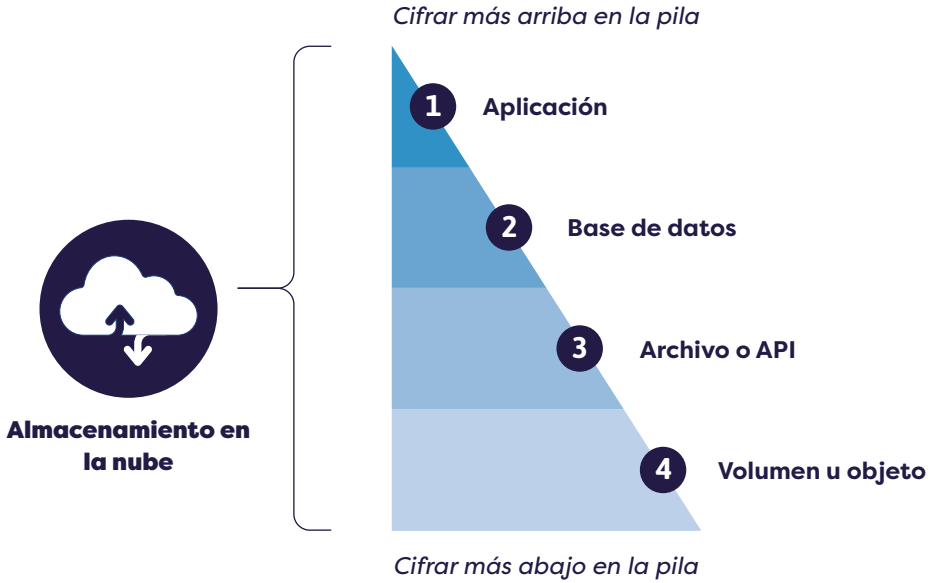
Aseguramiento de la información (PR.DS)

Cifrado de información en la nube

El uso de cifrado es un medio eficaz para reducir la capacidad de un ciberincidente en general, y de un incidente de *ransomware* en particular. En vista de esto, es necesario asegurarse de que por defecto la información almacenada en la nube esté cifrada durante todo su ciclo de vida. De esta manera, al integrar principios de seguridad aceptados, como SoD, es posible definir que la clave de cifrado no será accesible de forma rutinaria para la cuenta del usuario, de modo que incluso si un atacante lograra robar una identidad o filtrar la información fuera del entorno CSC, su capacidad para descifrar la información será baja.

El cifrado en la nube se puede realizar en varios niveles, como se muestra en el Gráfico 7, por lo cual el CSC debe examinar el método de cifrado en relación con su perfil de riesgo.

Gráfico 7. Capas en las que puede aplicarse el cifrado para asegurar la información

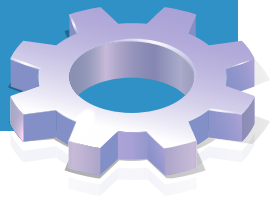


Fuente: CSA (2024).

Recuadro 2. Tecnología de computación confidencial (*confidential computing*)

La computación confidencial o secreta es una tecnología de computación en la nube que brinda protección de la información durante el procesamiento/tiempo de ejecución. El principio de funcionamiento de esta tecnología se basa en asignar un entorno seguro para el procesamiento de la información (*trusted execution environment*) a nivel de la unidad central de procesamiento (CPU, por sus siglas en inglés), donde solo los componentes de *software* que hayan sido aprobados por el CSC puedan acceder al proceso de procesamiento y a sus productos.

Se recomienda utilizar esta tecnología como control compensatorio al trabajar con bases de datos sensibles.



Prevenir el filtrado de información (DLP)

Dado que es habitual que los atacantes filtren información organizacional a servidores en Internet antes de realizar el cifrado de la información y presentar la demanda de pago, implementar medidas aceptadas para evitar la filtración de información puede reducir la capacidad del atacante para lograr su objetivo. Como mínimo, pueden ser una fuente importante de telemetría que ayude al CSC a detectar el ataque en ciernes, antes de que el atacante haya comenzado a realizar operaciones de cifrado.

Además, aplicar un proceso ordenado para la gobernanza de datos (*data governance*) a nivel del CSC puede ayudar a localizar la ubicación de la información, clasificarla y mejorar las medidas de seguridad para evitar el filtrado de información. Asimismo, permite demostrar que el CSC cumple con los requisitos de cumplimiento aceptados (*compliance*). Muchos requisitos legales y reglamentarios imponen al CSC la responsabilidad de gestionar este tipo de procesos por motivos distintos a la ciberseguridad y protección de la información, como la protección de la privacidad, de la propiedad intelectual y de la seguridad.

Tecnologías que preservan y mejoran la privacidad (*privacy-enhancing technologies*)

Las tecnologías de mejora de la privacidad (PET, por sus siglas en inglés) incluyen una amplia variedad de soluciones de *hardware* y *software* diseñadas para permitir la maximización del valor de la información personal (comercial, científica y social) administrada por una organización, al tiempo que se reduce el riesgo para la privacidad del interesado y la seguridad de esta información (Ministerio de Justicia, s.f.). Una de las soluciones más conocidas es el enmascaramiento de información confidencial, como la de la tarjeta de crédito.

La implementación de PET en el entorno del CSC es un medio eficaz y eficiente para reducir el efecto de daño durante un ataque de *ransomware*. A diferencia de las infraestructuras organizativas locales, donde se requiere que la organización implemente una solución de forma completa y la mantenga en el tiempo, una parte importante de los CSP ofrecen soluciones administradas que se pueden implementar en un tiempo relativamente corto y sin la necesidad de grandes inversiones.

Puesta en práctica del principio de minimización de datos (*data minimization*)

Realizar un proceso oportuno para examinar el estado de la información y tomar acciones proactivas para reducir el exceso de activos (por ejemplo, información, máquinas virtuales antiguas) es un medio eficaz y eficiente de reducir el efecto de un ataque de *ransomware* en el entorno del CSC. Más allá de eso, la puesta en práctica de este principio incluye una serie de ventajas, como el cumplimiento de los requisitos legales y reglamentarios pertinentes y la reducción de los costos continuos por el consumo de servicios en la nube.

Mantenimiento de copias de seguridad y aseguramiento de la información

En ciertos casos, entidades externas pueden estar involucradas en el resguardo de la información en caso de eliminación o cifrado de información, principalmente durante ataques de *ransomware*, pero no exclusivamente en esas ocasiones. Tener y mantener copias de seguridad es un paso clave para recuperarse ante incidentes de este tipo. Las siguientes son medidas importantes para el mantenimiento de copias de seguridad y el aseguramiento de la información:

01

Realización de controles de estado periódicos. Lo más importante al trabajar con copias de seguridad es realizar controles de estado periódicos. La copia de seguridad debe incluir una restauración completa de los activos a un entorno de prueba específico (*sandbox*), y luego se deben realizar pruebas de normalidad a nivel operativo, como simular el acceso de los usuarios al entorno e introducir/recuperar información.

02

Detección de la existencia de *malware* en las copias de seguridad. Esto debe hacerse mediante la búsqueda oportuna de información en la copia de seguridad, utilizando firmas actuales (*retro hunting*), y a través del uso de capacidades de investigación más avanzadas, como ejecutar en un entorno de prueba específico (*sandbox*).

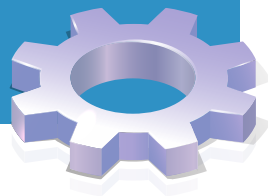
03

Detección de anomalías en las copias de seguridad. Esto incluye una correlación con las copias de seguridad históricas, como un volumen de copias de seguridad anormal, cambios en el nivel de entropía de los archivos en comparación con el nivel anterior y cambios poco claros en las extensiones de los archivos.

04

Almacenamiento de copias de seguridad de forma protegida. Es habitual que, como parte de un ataque de *ransomware*, se intenten eliminar, interrumpir o cifrar las copias de seguridad. En vista de esto, se recomienda usar los servicios de recuperación ante desastres (DR, por sus siglas en inglés) integrados en el CSP, y utilizar los servicios de archivo del CSP para almacenar las copias de seguridad de modo que normalmente estén en modo de solo lectura (similar al principio de escritura única, lectura múltiple [WORM, por sus siglas en inglés] tradicional). Además, es importante definir el control de acceso para que solo se pueda acceder a licencias específicas. Si es posible, se recomienda definir que el acceso a las copias de seguridad requiera la aprobación previa de aprobadores independientes.

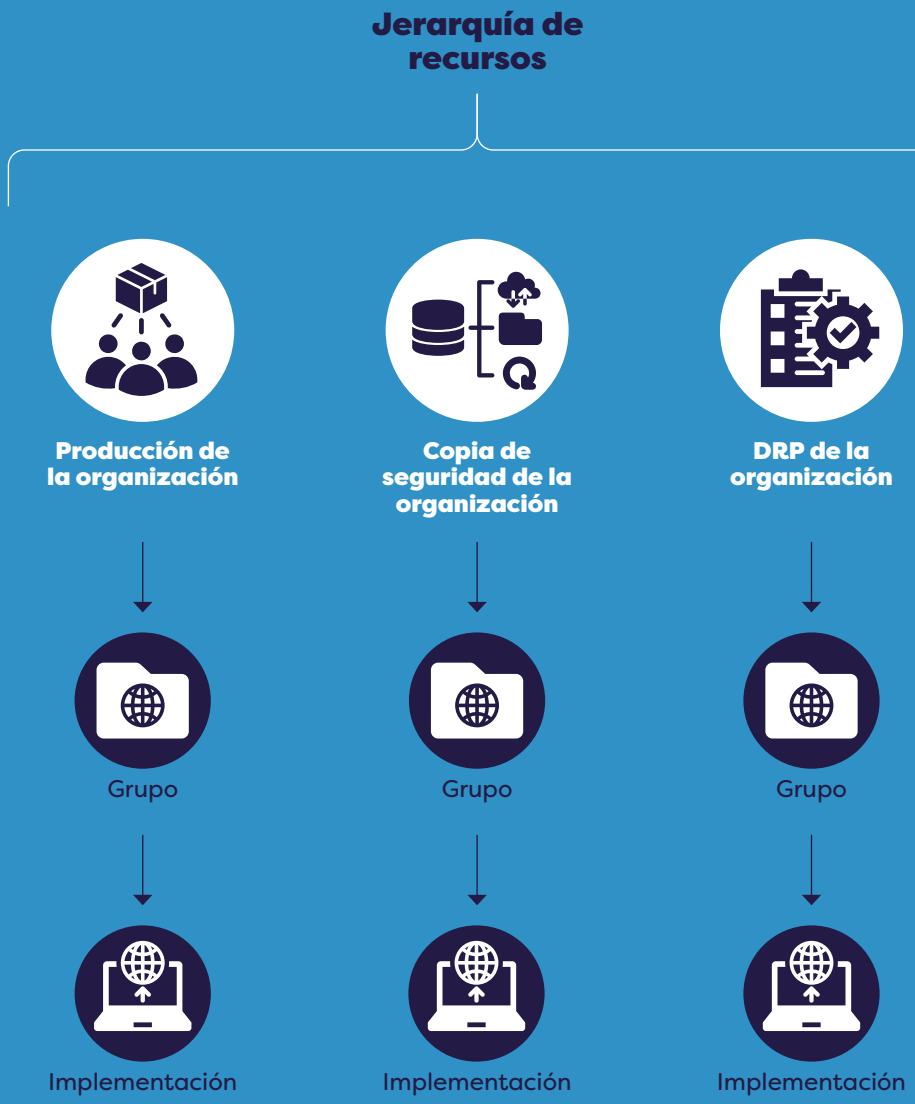
Se recomienda reducir al máximo la posibilidad de ejecutar *software* o herramientas en el entorno donde se almacena la copia de seguridad para evitar la posibilidad de ejecutar un *ransomware* guardado en las copias de seguridad. Una operación de este tipo puede deberse, entre otras cosas, a un error humano, sobremotivación del equipo de informática que desea realizar una rápida recuperación o intención maliciosa.



05

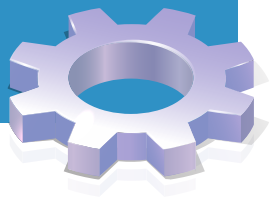
Asignación jerárquica de recursos específica para almacenar copias de seguridad. Se recomienda asignar recursos de manera jerárquica, específica e independiente para almacenar las copias de seguridad, de modo que, incluso si un atacante lograra tomar el control de la jerarquía de recursos de producción y/o de recursos del plan de recuperación ante desastres (DRP, por sus siglas en inglés) y/o las posiciones de los administradores del sistema, su capacidad para dañar la integridad de las copias de seguridad sería lo más baja posible. Esto incluye utilizar *hardware* específico para los puestos de administradores del sistema, uso de medios de autenticación independientes (como una tarjeta de *hardware* FIDO II específica) o similares (Gráfico 8).

Gráfico 8. Diagrama común de jerarquía de recursos recomendada



En general, la recomendación es asignar una jerarquía específica e independiente para almacenar copias de seguridad que no es la jerarquía DRP. Los principales objetivos de esta recomendación son los siguientes:

- Verificar que las copias de seguridad no se dañarán incluso en el caso de transferir activos con un *ransomware* activo desde el entorno de producción al entorno DRP.
- Verificar que las copias de seguridad no se dañarán en caso de restaurar la información en la copia de seguridad y ejecutarla.



En caso de temerse una amenaza interna (*insider threat*), se recomienda considerar que el enfoque de la jerarquía de recursos específicos para almacenar las copias de seguridad esté restringido únicamente a un equipo de TIC específico, que no trabaje de manera rutinaria con la jerarquía de recursos de producción y la jerarquía de recursos de DRP. Por ese motivo, deben aplicarse pruebas de confiabilidad aceptadas en todas las etapas de la contratación.

Para más información, véase: ***Recomendaciones de defensa: la amenaza interna.***[22]

06

Bloqueo de copias de seguridad a lo largo del tiempo (*retention lock*). Se recomienda definir la imposibilidad de eliminar y/o cambiar la información en la copia de seguridad por un período de X días, mediante el uso de un mecanismo de bloqueo de archivos y/u otros métodos aceptados en una nube pública.

07

Gestión de versiones para copias de seguridad. Se sugiere definir versiones para la información en la copia de seguridad, de modo que sea posible revertirla, en caso de ser necesario.

22. El documento ***Recomendaciones de defensa: la amenaza interna*** se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/recomendaciones-de-defensa-la-amenaza-interna-adaptacion-de-la-organizacion-en-el-ciberespacio**.

08

Copia de seguridad frecuente. Una copia de seguridad con la mayor frecuencia posible (como una copia de seguridad continua) optimiza el tiempo y la capacidad de recuperación de incidentes con *ransomware*. Las copias de seguridad de varias semanas o meses de antigüedad tienen una capacidad significativamente menor que las copias de seguridad que se realizan con frecuencia.

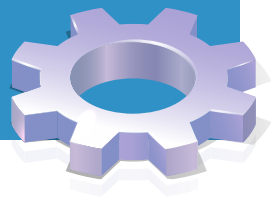
09

Caracterización del contenido para la copia de seguridad. La caracterización anticipada de los tipos de información para la copia de seguridad también ayuda a hacer frente a un incidente de ataque que desactive el almacenamiento en línea. Almacenar archivos es importante, pero también lo es realizar copias de seguridad de los ajustes de configuración, bases de datos y otros tipos de información, aunque no sea intuitivo.

10

Activación de un mecanismo de gestión de versiones (*file versioning*). Una solución más sencilla y accesible, pero al mismo tiempo menos completa, es activar un mecanismo de gestión de versiones que conserve las versiones anteriores de todos los archivos. De este modo, si se realiza un cambio en los propios archivos, las versiones anteriores de los archivos pueden restaurarse mediante un mecanismo de gestión de versiones. Este mecanismo no proporciona una solución integral y suficiente para proteger todo tipo de información del CSC, y es frecuente que no impida que un atacante que haya obtenido acceso a los datos de autenticación de un usuario legítimo pueda realizar modificaciones incontroladas, como el borrado de información. Esto es así especialmente en situaciones en las que el CSC ha definido que desactivar un mecanismo de gestión de versiones requiere la finalización exitosa de la autenticación multifactor.

Un error frecuente entre los CSC es asumir que el CSP es responsable de realizar copias de seguridad de la información corporativa y el fenómeno es aún más frecuente cuando los CSC utilizan la plataforma SaaS. Ante esto, cabe aclarar que por regla general el CSP no es responsable de las copias de seguridad, que son responsabilidad total del CSC, a menos que el acuerdo de contratación entre las partes establezca lo contrario. En cualquier caso, se recomienda que el propio CSC realice pruebas adecuadas de las copias de seguridad periódicamente para asegurarse de que puedan utilizarlas según sea necesario.[23]



Replicación de información

Es posible replicar la información existente en un entorno del CSC en otro entorno CSC. Ante tales situaciones, se recomienda adoptar las siguientes medidas:

01

Uso de replicación asincrónica. Permite aumentar la probabilidad de que, en caso de cifrado de información en una copia, otra copia de la información en posesión del CSC no se cifre inmediatamente. La ventana de tiempo hasta que se completa la replicación asincrónica permite al CSC localizar el ataque y realizar procesos de DR de manera más efectiva y eficiente.

02

Replicación a otra región u otro CSP. Realizar la replicación a otra región y/o CSP puede ayudar considerablemente en el caso de que se exploten vulnerabilidades en la infraestructura del CSP principal que brinden al atacante la capacidad de alterar o eliminar información de manera lateral.

03

Activación de un mecanismo de gestión de versiones. Es similar a lo detallado en el punto 2.

23. Para más información, véase Protección de copias de seguridad en la nube, de la INCD (2024): **https://www.gov.il/he/pages/alert_1795** (en hebreo) e Integración de los principios de ciberseguridad en los procesos de copias de seguridad y recuperación, de la INCD (2021): **https://www.gov.il/he/pages/backup_restore** (en hebreo).

Categoría de detección (*detect*)

Consiste en la detección y análisis de ciberataques y anomalías.

Monitoreo continuo (DE.CM)

Fuentes de telemetría para el cibermonitoreo

Como parte de la preparación para un ciberincidente y análisis de la postura de seguridad, es importante definir de antemano las fuentes para la recopilación de telemetría. En este sentido, es necesario integrar herramientas de terceros como CSPM (SSPM en el caso de monitoreo de plataforma SaaS) y DSPM para completar la cobertura.

Por lo general, el proveedor de la nube permite transferir información en la configuración de incidente (*event*) y/o blog (*log*). La transferencia de información en esta configuración suele ser casi en tiempo real, pero el alcance de la información es limitado. Por el contrario, la transferencia de información en un blog suele ser más lenta, pero mucho más completa, lo cual es fundamental para realizar una investigación óptima.

Es importante predefinir estos incidentes y establecer registros pertinentes en relación con el perfil de riesgo. Esto se debe a que sin su activación preliminar puede no ser posible realizar una investigación efectiva de forma retrospectiva y, por tanto, que exista una dificultad real para llevar a cabo el control de daños, localizar el vector de ataque, etc. Al respecto, la Autoridad de Protección de la Privacidad de Israel publicó una guía para implementar el punto 10 del Reglamento de Seguridad de la Información: mantenimiento de documentación y registros (Autoridad de Protección de la Privacidad de Israel, 2024).

Como regla general, se recomienda aplicar las definiciones tal como aparecen en la documentación oficial del proveedor de nube correspondiente, por ejemplo, Well-Architected Framework y Cloud Adoption Framework.

El Cuadro 7 muestra las fuentes de telemetría comunes en una nube pública.

Cuadro 7. Fuentes comunes de recopilación de telemetría en plataformas en la nube

Registros del plano de gestión	Registros de servicio	Registros de recurso	Herramientas en la nube
• Fuente crítica dada la importancia de proteger el plano de gestión.	• Pasarela API: registros de acceso. • Almacenamiento: registros de acceso. • Red: registros de flujo de la VPC. • Función/sin servidor: registros de actividad. • Equilibrador de carga en la nube: registros de actividad. • Servidor de nombres de dominio (DNS, por sus siglas en inglés) en la nube: registros de consulta. • WAF/cortafuegos en la nube: registros de actividad.	• Carga de trabajo: registros de instancias y máquinas virtuales. • Registros de cambios de configuración. • Registros de invocación de funciones en la nube. • Registros de transacciones de bases de datos. • Registros de acceso a archivos de almacenamiento de objetos. • Registros de instantáneas e imágenes (almacenamiento en bloque).	• CSPM. • CASB. • Plataforma de protección de aplicaciones nativas de la nube (CNAPP, por sus siglas en inglés). • SSPM. • DSPM. • Análisis IAM. • Detección y respuesta en la nube.

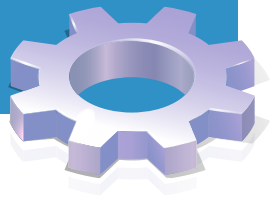
Fuente: CSA (2024).

Se recomienda transferir la información recopilada de las diversas fuentes de telemetría lo antes posible a un *data lake* o un sistema SIEM. A su vez, esto puede frustrar la posibilidad de que un atacante perjudique la capacidad del CSC para investigar y detectar incidentes inusuales. Asimismo, se recomienda conservar la información extraída de las fuentes de telemetría por un período de al menos un año, aunque según los requisitos y regulación se le puede requerir al CSC[24] conservar la información por un período mayor.

Además, a la lista de fuentes incluidas en el Cuadro 7 se debe añadir una referencia a las fuentes que contienen información del tipo de operaciones financieras (FinOps, por sus siglas en inglés).

Debe tenerse en cuenta que numerosos registros no están activados por defecto en el entorno de la nube, como DNS y Flow Logs.

Ante esto, deben definirse previamente los tipos de registros necesarios para el seguimiento y respuesta a la información y a los ciberincidentes, así como asegurarse de que se extraigan de los distintos activos y se transfieran al *data lake* o al sistema SIEM.



24. Véanse también, por ejemplo, el Reglamento de Protección de la Privacidad (Aseguramiento de la Información) de 2017, la Ley de Archivos de 1955, el Reglamento de Salud Pública (Mantenimiento de Registros) de 1976 y otras directrices regulatorias.

Recuadro 3. Detección como código (*detection as code*)

La detección como código es un enfoque estratégico que integra estructuralmente la protección de la información y los mecanismos de detección cibernética en el ciclo de vida del desarrollo de *software*. Al tratar los controles de seguridad como código, las organizaciones pueden automatizar la implementación, gestión de la configuración y mantenimiento de las medidas de seguridad durante todo el proceso de desarrollo. Este enfoque está en línea con la filosofía de desarrollo, seguridad y operaciones (DevSecOps, por sus siglas en inglés) y reúne la seguridad de la información y la ciberseguridad como una parte integrada del proceso de desarrollo, en lugar de tratarlo como un paso separado e independiente. Como resultado, las organizaciones pueden desarrollar capacidades de detección avanzadas (como reglas, heurísticas y modelos de aprendizaje automático para la detección de anomalías) y adoptar principios de DevSecOps que reducen la necesidad de realizar pruebas manuales, lo que a su vez disminuye el tiempo necesario para desarrollar e implementar nuevas capacidades de seguridad.

Análisis de incidentes anormales (DE.AE)

El proceso de análisis de incidentes inusuales en una nube pública incluye características similares a las que existen en infraestructuras organizativas locales, pero también otras que son exclusivas de este entorno.

A continuación, se presentan varias pautas para analizar incidentes inusuales en un entorno de nube pública:

01

La tasa de alertas, el alcance de los registros y su variedad deberían ser significativamente mayores que los de las infraestructuras organizativas locales.

02

Por lo general, la tasa de transferencia de registros de los recursos al sistema de monitoreo es menor que la de las alertas. Por consiguiente, el CSC debe prepararse con anticipación para afrontar el lapso de tiempo hasta que los registros llegan al sistema de monitoreo, lo que en ocasiones requiere realizar un análisis y sacar conclusiones con información faltante.

03

El proceso de monitoreo de la gestión de identidades, autenticación y control de acceso es un reto de primer nivel al trabajar en una configuración de nube híbrida y en un entorno multinube (*multi-cloud*). Ante esto, se debe verificar que el CSC cuente con procesos, tecnologías y personas capaces de dar una respuesta adecuada a este reto.

04

Para realizar un proceso de normalización de la información recibida, es habitual que se requieran pasos previos, como construir un conector y definir un mapeo de esquema. Este problema plantea un reto importante, especialmente al trabajar con una configuración multinube.

05

Es necesario realizar análisis de la superficie de ataque y ajustes de configuración de forma continua. Esto se debe a que es habitual que los ajustes de configuración deficientes en el entorno de la nube sean un vector de intrusión común para los atacantes.

06

Se recomienda monitorear continuamente la fiabilidad e integridad de los archivos, lo que incluye detección de anomalías, cambios en el nivel de entropía de los archivos en comparación con el nivel anterior, cambios poco claros en las extensiones de los archivos y la existencia de *malware* conocido en los archivos.

07

Se sugiere monitorear todos los componentes de la infraestructura, incluso si normalmente no están activados. Por ejemplo, detectar la adición y ejecución de una nueva función en una arquitectura sin servidor (*serverless*). En el caso de una plataforma SaaS, definir un nuevo proceso de copia de seguridad o agregar un nuevo destino para almacenar copias de seguridad.

08

Se recomienda utilizar capacidades de IA para la ciberseguridad y protección de la información, lo que incluye su uso como herramienta de apoyo a la toma de decisiones y de acuerdo con una política organizacional para el uso de IA.

09

Se sugiere integrar una solución de orquestación, automatización y respuesta de seguridad (SOAR, por sus siglas en inglés) para construir *playbooks* de casos/respuestas, de modo que la necesidad de intervención humana sea lo más baja posible. Como parte de esto, se recomienda crear un canal de investigación de *malware* (*malware investigation pipeline*) para automatizar los procesos de prueba.

10

Realizar una correlación con fuentes de ciberinteligencia puede ayudar a responder rápidamente a amenazas conocidas, así como a lograr una comprensión situacional (*situational awareness*).

11

El tiempo necesario para la detección y el análisis de anomalías debe ser lo más breve posible; unos cuantos segundos, como máximo.

Incluso en los casos en que el CSC tiene un límite de recursos que impide la compra de herramientas avanzadas, es posible detectar incidentes inusuales utilizando medidas relativamente simples, como las siguientes:

- Detección de una anomalía en las comunicaciones que puede reflejarse en volúmenes de tráfico anormales.
- Descubrimiento de una anomalía en el consumo financiero de servicios del CSP. Para eso, se recomienda que el equipo de ciberseguridad y protección de la información integre en esta actividad al responsable en el tema de FinOps.
- Detección de procesos anormales de creación, lectura, actualización y eliminación (CRUD, por sus siglas en inglés), como por ejemplo un usuario que modifica más de X archivos por hora.
- Descubrimiento de modificaciones en el proceso de copias de seguridad y almacenamiento de información.
- Detección de la creación de nuevas cuentas de usuario o múltiples fallos en el proceso de acceso.
- Inicio de una aplicación a Internet desde recursos que no tengan una necesidad comercial para realizar este tipo de aplicación.
- Comienzo de tráfico desde posiciones de usuarios fuera del horario laboral normal en cualquier sitio/país donde operen los empleados de CSC.

- Detección de la accesibilidad de y a activos desde direcciones IP o dominios de baja reputación (como direcciones asociadas con campañas de ataque conocidas/adversarios e infraestructuras enemigas o direcciones IP que prestan servicios de proxy).

- Uso de las capacidades de seguridad integradas en el entorno de la nube, como definir que la escritura visible de información confidencial en un recurso (por ejemplo, secretos e información de identificación personal/información de salud protegida [PII/PHI, por sus siglas en inglés]) dará como resultado el envío de una alerta al equipo de seguridad de la información y ciberseguridad.

Análisis del nivel de madurez del sistema del centro de operaciones de seguridad

Se recomienda utilizar el modelo centro de operaciones de seguridad-modelo de madurez de capacidades (SOC-CMM, por sus siglas en inglés)[25] para examinar el nivel de madurez del sistema SOC. Por lo general, se sugiere utilizar una nube pública solo después de que el CSC u otra entidad en su nombre (como un servicio de detección y respuesta gestionadas [MDR, por sus siglas en inglés]) haya logrado alcanzar al menos el nivel de madurez cuatro y mantener este nivel durante un período de tiempo razonable.

Categoría de respuesta (*respond*)

Consiste en tomar acciones cuando se detecta un ciberincidente.

Gestión de incidentes (RS.MA)

En vista de que el CSC puede verse atrapado en algún momento en un ciberincidente en la nube, es importante tener una preparación previa para la respuesta a incidentes (IR *readiness*, por sus siglas en inglés). Esto incluye que el CSC adopte las siguientes medidas:

- Verificar que el entorno de la nube ha sido diseñado de manera conforme al NIST Cloud Computing Forensic Reference Architecture.[26]

- Activar de manera preliminar las fuentes de telemetría adecuadas, incluyendo el reenvío de alertas y registros a un SIEM central o *data lake*.

25. Más información sobre SOC-CMM disponible en: **https://www.soc-cmm.com/**.

26. Para conocer más acerca de NIST Cloud Computing Forensic Reference Architecture, visítese: **https://csrc.nist.gov/pubs/sp/800/201/final**

- Verificar que el CSC posea conocimientos y herramientas adecuadas para los procesos de IR en la nube.

- Comprobar que el CSC cuente con un diagrama de arquitectura y mapeo de activos actualizado, de acuerdo con su nivel de criticidad/sensibilidad.

- Realizar prácticas periódicas de procesos de IR en entorno de nube, integrando a socios pertinentes, tales como una empresa de IR.

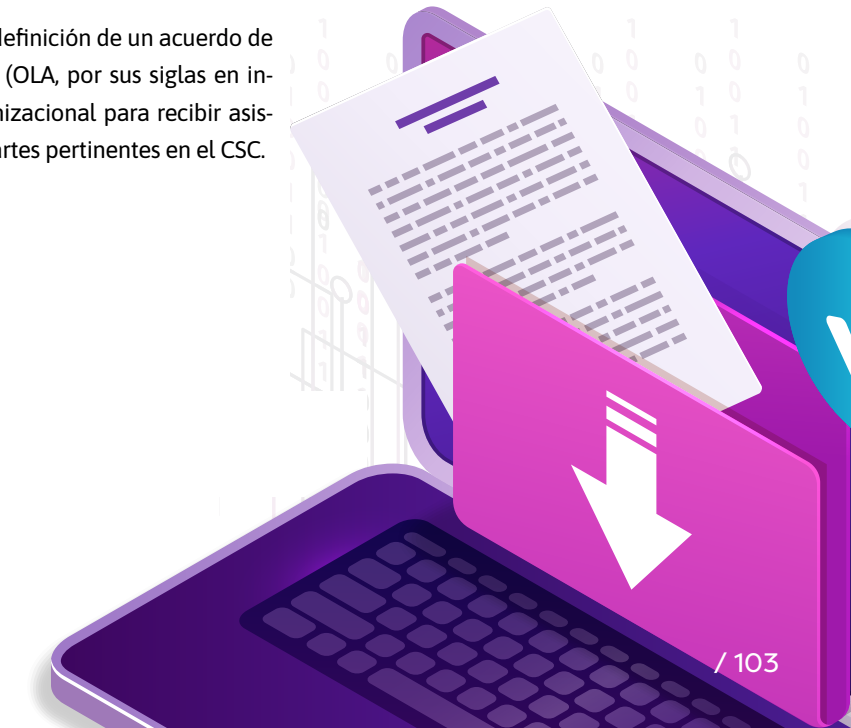
- Verificar que existe un acuerdo de contratación con el CSP, que incluya la posibilidad de operar el equipo de IR por encargo de este, de conformidad con un SLA claro.

- Comprobar la definición de un acuerdo de nivel operativo (OLA, por sus siglas en inglés) intraorganizacional para recibir asistencia de las partes pertinentes en el CSC.

- Verificar que el CSC cuente con un medio de pago alternativo para poder adquirir servicios del CSP con el que trabaje habitualmente o un CSP alternativo, si fuese necesario.

- Comprobar que el CSC tenga un entorno específico (por ejemplo, uno de implementación específico) en el que se hayan instalado medidas de análisis forense digital y respuesta a incidentes (DFIR, por sus siglas en inglés) con anticipación como parte de la preparación para un ciberincidente.

- Verificar que el CSC posee los conocimientos y capacidad para hacer un uso óptimo del servicio de descubrimiento electrónico (eDiscovery) del CSP.



- Comprobar la definición de cuentas de usuario designadas unicamente para la gestión de incidentes y el análisis forense digital.

- Si fuese necesario, verificar la concesión de privilegios de acceso a nivel de rol de implementaciones cruzadas (*cross-deployments*) mientras se aplican principios aceptados como *least privilege, need to know, need to see*.

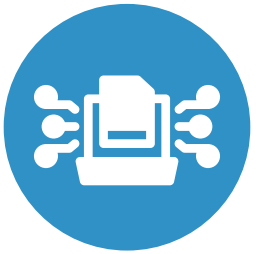
- Brindar acceso temporal mediante el uso de un mecanismo de acceso temporal (*just-in time admin*) y un servicio de *token* de seguridad (STS, por sus siglas en inglés), al tiempo que se limita el acceso únicamente para los activos pertinentes para la investigación.

- En el caso de activos temporales (como un contenedor), es necesario verificar de antemano que el activo envíe todos los registros pertinentes al sistema de monitoreo antes de su eliminación o apagado. De lo contrario, al eliminar o desactivar el activo puede perderse información de valor para la investigación.

- Adherir una etiqueta específica a los recursos que se requieran para realizar investigaciones y análisis forenses, de modo que el control y documentación del proceso de IR puedan llevarse a cabo de manera óptima. Un ejemplo de etiquetado es el siguiente: Forense_Fecha.

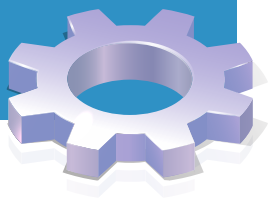
- Verificar que la política de seguridad aplicable a los recursos de la nube (como las políticas de control de servicios) no impide la capacidad de realizar investigaciones y análisis forenses.

Si fuese necesario, el CSC puede recurrir a una empresa de IR externa. En este caso es importante que la empresa conozca en profundidad el entorno y realice prácticas periódicas y conjuntas con el CSC. Del mismo modo, es fundamental definir un SLA claro con la empresa de IR. En este sentido, el SLA debe prever una referencia clara a situaciones extremas, como por ejemplo, un incidente que afecte simultáneamente a varios clientes de la empresa de IR.



Es recomendable asegurarse de que el plan de respuesta incluya referencias a los casos en los que un ciberincidente comenzó en el entorno de nube pública del CSC y pasó a infraestructuras organizativas locales y/u otro entorno de nube pública del CSC, y viceversa.

La experiencia muestra que, a fin de mantener un alto nivel de competencia y preparación, el CSC debe analizar con mucha frecuencia su capacidad para construir un cronograma de investigación multidimensional para controles de incidentes de este tipo, mientras recopila datos de una gran cantidad de fuentes bajo el principio de cadena de evidencia.



Informes y comunicación durante un incidente (RS.CO)

Se recomienda verificar que el CSC tenga un proceso ordenado para informar y comunicar durante un incidente. A continuación, se muestran algunos puntos importantes al respecto:

- Se recomienda relevar periódicamente si existe la obligación de informar a uno o más reguladores en el país de origen donde opera el CSC.

- Se sugiere verificar periódicamente si existe la obligación de informar a uno o más reguladores en el país en el que se almacene y/o procese la información del CSC.

- Se recomienda notificar al CSP cuando ocurra un ciberincidente, ya que con frecuencia el acuerdo de vinculación otorga al CSP la opción de bloquear la actividad del CSC en caso de anomalías y/o de temerse daños a un tercero.

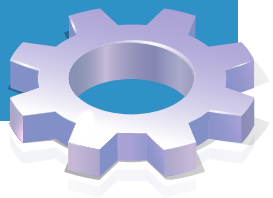
- Se sugiere comprobar que el CSC cuente con un canal de comunicación alternativo para la gestión de ciberincidentes, de modo que en caso de un ataque sea posible generar información y comunicarse para el manejo del incidente.

Mitigación del impacto del ciberincidente (RS.MI)

A continuación, se detallan algunos puntos para reducir el impacto de un ciberincidente en un entorno de nube pública:

- Como regla general, en una nube pública no hay necesidad de reparar activos dañados, como una máquina virtual o un contenedor. En lugar de esto, es posible almacenar una copia de los activos afectados para su investigación y puede iniciarse una copia en un entorno limpio utilizando IaC u otro método aceptado.
- Se recomienda integrar una solución SOAR para construir *playbooks* de casos y respuestas, de modo que la necesidad de participación humana sea lo más baja posible. En caso de falta de recursos para adquirir una solución SOAR, pueden utilizarse funciones en una arquitectura sin servidor con el fin de realizar procesos de respuesta básicos, como desconectar un activo dañado del entorno de producción o enviar una notificación al equipo de información y ciberprotección.
- Las herramientas de seguridad integradas en la nube pública permiten implementar un control compensatorio en poco tiempo en comparación con las infraestructuras organizativas locales.

Un problema frecuente es que, durante un ciberincidente, el CSC o sus agentes pueden hacer uso de servicios de investigación en línea, como un entorno de prueba específico (*sandbox*). Debe considerarse la implicancia de exponer información organizacional a estos servicios, ya que puede conducir a violaciones relacionadas con la privacidad, la propiedad intelectual o la exposición de la existencia de la investigación a un atacante.



Categoría de recuperación (*recover*)

Consiste en restaurar activos y procesos que resultaron dañados como resultado de un ciberincidente.

Ejecución de un plan de recuperación ante incidentes (RC.RP)

Es sumamente importante que un BCP y un PRD incluyan una referencia al trabajo con la nube, al tiempo que aludan a los retos especiales que resultan de dicho entorno. Esto incluye que el CSC practique periódicamente, al menos una vez al año, la posibilidad de crear un entorno totalmente desde cero, y la continuación de la actividad empresarial desde dicho entorno durante al menos diez días naturales.

Comunicación durante las operaciones de recuperación ante incidentes (RC.CO)

Se recomienda poner al día periódicamente a las partes interesadas pertinentes sobre el estado de las operaciones de restauración. Asimismo, se sugiere asignar a las partes interesadas en cuestión un tablero (*dashboard*) personalizado en el panel de gestión del CSP, que les permita monitorear directamente el estado de las operaciones de restauración.[27]

27. Para más información sobre la gestión de ciberincidentes, consúltese: NIST SP 800-61 Rev. 3 (Initial Public Draft). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, de NIST: **https://csrc.nist.gov/pubs/sp/800/61/r3/ipd**; Cloud Incident Response Framework, de CSA: **https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework**; Best Practices for Cyber Crisis Management, de ENISA: **https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management**.

/05.
Lista de verificación

Cuadro 8. Lista de verificación con las formas de reducir riesgos que figuran en el documento

Nombre de la categoría	Nombre de la subcategoría	Estado de implementación
Gobernanza empresarial (*govern*)	Estrategia de gestión de riesgos (GV.RM)	☐
	Política (GV.PO)	☐
	Seguridad de la cadena de suministro (GV.SC)	☐
Identificación (*identify*)	Mapeo de activos (ID.AM)	☐
	Evaluación de riesgos (ID.RA)	☐
	Aspiración de mejora continua (ID.IM)	☐
Protección (*protect*)	Gestión de identidad, autenticación y control de acceso (PR.AA)	☐
	Sensibilización y formación (PR.AT)	☐
	Aseguramiento de la información (PR.DS)	☐
	Seguridad de la plataforma (PR.PS)	☐
	Resiliencia de la infraestructura tecnológica (PR.IR)	☐
Detección (*detect*)	Monitoreo continuo (DE.CM)	☐
	Análisis de incidentes anormales (DE.AE)	☐
Respuesta (*respond*)	Gestión de incidentes (RS.MA)	☐
	Informes y comunicación durante un incidente (RS.CO)	☐
	Mitigación del impacto del ciberincidente (RS.MI)	☐
Recuperación (*recover*)	Ejecución de un plan de recuperación ante incidentes (RC.RP)	☐
	Comunicación durante las operaciones de recuperación ante incidentes (RC.CO)	☐

Referencias

- Autoridad de Protección de la Privacidad de Israel. 2024. Guía para la implementación del art. 10 del Reglamento de Aseguramiento de la Información: mantenimiento de documentación y registros, 29 de septiembre de 2024. Disponible en: **https://www.gov.il/he/pages/takana10d**.
- Capital One. s.f. Información sobre el Incidente Cibernético en Capital One. Disponible en: **https://www.capitalone.com/digital/facts2019/es/**.
- Cyentia Institute. 2024. Information Risk Insights Study RANSOMWARE, A Detailed Analysis of the Frequency and Impact of Ransomware Events. Disponible en: **https://www.cyentia.com/iris-ransomware/**.
- Check Point. 2023. MOVEit Vulnerability Weaponized in Ransomware Attack. Disponible en: **https://blog.checkpoint.com/security/moveit-vulnerability-weaponized-in-ransomware-attack/**.
- CISA (Agencia de Ciberseguridad y Seguridad de las Infraestructuras). 2023. Zero Trust Maturity Model, abril. Disponible en: **https://www.cisa.gov/zero-trust-maturity-model**.
- CSA (Cloud Security Alliance). 2022. SaaS Governance Best Practices for Cloud Customers, 10 de octubre. Disponible en: **https://cloudsecurityalliance.org/artifacts/saas-governance-best-practices-for-cloud-customers**.
- ————. 2023. MOVEit Exploit & Ransomware Attack: Why SaaS Security Is Critical During a Cyberattack, agosto. Disponible en: **https://cloudsecurityalliance.org/blog/2023/11/08/moveit-exploit-ransomware-attack-why-saas-security-is-critical-during-a-cyberattack**.
- ————. 2024. Security Guidance for Critical Areas of Focus in Cloud Computing v5, 15 de julio. Disponible en: **https://cloudsecurityalliance.org/artifacts/security-guidance-v5**.
- Culafi, A. 2023. CloudNordic loses most customer data after ransomware attack. Disponible en: **https://www.techtarget.com/searchsecurity/news/366549773/CloudNordic-loses-most-customer-data-after-ransomware-attack**.
- Frichette, N. 2022. A confused deputy vulnerability in AWS AppSync. Disponible en: **https://securitylabs.datadoghq.com/articles/appsync-vulnerability-disclosure/**.
- GitGuardian. 2024. The State of Secrets Sprawl 2024, GitGuardian. Disponible en: **https://www.gitguardian.com/state-of-secrets-sprawl-report-2024**.
- Goldman, J. 2014. Code Spaces Destroyed by Cyber Attack. Disponible en: **https://www.esecurityplanet.com/networks/code-spaces-destroyed-by-cyber-attack/**.
- Google Cloud. s.f. UNC3944 Targets SaaS Applications. Disponible en: **https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications**.
- INCD (Dirección Nacional de Ciberseguridad de Israel). 2021. Aprovechamiento de la dependencia de software (*Software Dependencies*) para realizar ataques. 16 de febrero. Disponible en: **https://www.gov.il/he/pages/dependencies**.
- ————. 2024a. El coste económico de los ciberataques en Israel: 12 mil millones de NIS por año, abril. Disponible en: **https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024**.
- ————. 2024b. Cuestionario de Madurez de Defensa de las Pequeñas y Medianas Empresas.
- INCD (Dirección Nacional de Ciberseguridad de Israel) y BID (Banco Interamericano de Desarrollo). 2022. Práctica cibernética: creación y edición de ejercicios de ciberseguridad para organizaciones. Disponible en: **https://publications.iadb.org/es/practica-cibernetica-creacion-y-edicion-de-ejercicios-de-ciberseguridad-para-organizaciones-mejores**.
- Reiner, S. 2017. Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps. Disponible en: **https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps**.
- Invictus. 2024. Ransomware in the cloud. Disponible en: **https://www.invictus-ir.com/news/ransomware-in-the-cloud**.

- Laceworks Labs. 2022. AndroxGh0st – the python malware exploiting your AWS keys. Disponible en: **https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys**.
- Manage Engine. 2024. Understanding the Okta supply chain attack of 2023: A comprehensive analysis. Disponible en: **https://blogs.manageengine.com/it-security/2024/01/25/understanding-the-okta-supply-chain-attack-of-2023-a-comprehensive-analysis.html**.
- Matan, L. 2024. CloudImposer: Executing Code on Millions of Google Servers with a Single Malicious Package. Tenable. Disponible en: **https://www.tenable.com/blog/cloudimposer-executing-code-on-millions-of-google-servers-with-a-single-malicious-package**.
- Microsoft Threat Intelligence. 2023. Detecting and mitigating a multi-stage AiTM phishing and BEC campaign. Disponible en: **https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/**.
- Ministerio de Justicia, s.f. Cuadro No. 31 - Empresas de nueva creación por turnos privados - tendencias y retos. Disponible en: **https://govextra.gov.il/media/o15lb2gr/table-31.pdf** (en hebreo).
- Morgan, S. 2024. The World Will Store 200 Zettabytes of Data By 2025. *Cybercrime Magazine*. Disponible en: **https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025**.
- Netwrix, s.f. Golden SAML Attack. Disponible en: **https://www.netwrix.com/golden_saml_attack.html**.
- NIST (Instituto Nacional de Normas y Tecnología). 2011. NIST SP 800-145 - The NIST Definition of Cloud Computing, NIST. Septiembre de 2011. Disponible en: **https://csrc.nist.gov/pubs/sp/800/145/final**.
- ————. 2022. NIST SP 800-218. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, febrero. Disponible en: **https://csrc.nist.gov/pubs/sp/800/218/final**.
- ————. 2024a. NIST Cybersecurity Framework (CSF) 2.0, 26 de febrero. Disponible en: **https://www.nist.gov/cyberframework**.
- ————. 2024b. NIST SP 800-201. NIST Cloud Computing Forensic Reference Architecture, julio. Disponible en: **https://csrc.nist.gov/pubs/sp/800/201/final**.
- OWASP (Proyecto abierto de seguridad en aplicaciones web). 2020. Web Security Testing Guide. Disponible en: **https://owasp.org/www-project-web-security-testing-guide/**.
- Richter, F. 2024. Amazon Maintains Cloud Lead as Microsoft Edges Closer, Statista. Disponible en: **https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers**.
- SSO Circle. 2016. Microsoft Office365 SAML Vulnerability: Authentication Bypass. Disponible en: **https://www.ssocircle.com/en/2361/microsoft-office365-saml-vulnerability-authentication-bypass/**.
- Toulas, B. 2024. New Mamba 2FA bypass service targets Microsoft 365 accounts. Disponible en: **https://www.bleepingcomputer.com/news/security/new-mamba-2fa-bypass-service-targets-microsoft-365-accounts/**.
- Yair, O. s.f. One Drive. Double Agent. Disponible en: **https://i.blackhat.com/BH-US-23/Presentations/US-23-Yair-One-Drive-Double-Agent-Clouded-OneDrive-Turns-Sides.pdf**.
- Whittaker, Z. 2023. Danish cloud host says customers 'lost all data' after ransomware attack. Disponible en: **https://techcrunch.com/2023/08/23/cloudnordic-azero-cloud-host-ransomware/**.

Anexo

Publicaciones de la Dirección Nacional de Ciberseguridad de Israel (incluidos dentro de esta serie de guías de buenas prácticas en ciberseguridad)

- Integración de principios de ciberseguridad en los procesos de respaldo y recuperación (de próxima publicación).
- Práctica cibernética: creación y edición de ejercicios de ciberseguridad para organizaciones. Disponible en: **https://publications.iadb.org/es/practica-cibernetica-creacion-y-edicion-de-ejercicios-de-ciberseguridad-para-organizaciones-mejores**.
- Recomendaciones de defensa: la amenaza interna. Disponible en: **https://publications.iadb.org/es/recomendaciones-de-defensa-la-amenaza-interna-adaptacion-de-la-organizacion-en-el-ciberespacio**.

Publicaciones de la Dirección Nacional de Ciberseguridad de Israel (en hebreo)

- Aseguramiento de copias de seguridad en la nube, 29 de agosto de 2024: **https://www.gov.il/he/pages/alert_1795**.
- El coste económico de los ciberataques en Israel: 12 mil millones de NIS por año, abril de 2024: **https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024**.
- Aprovechamiento de la dependencia de software (*Software Dependencies*) para realizar ataques, 16 de febrero de 2021: **https://www.gov.il/he/pages/dependencies**.
- Concepto nacional en cibernética para prepararse y gestionar situaciones de crisis, 6 de noviembre de 2018: **https://www.gov.il/he/pages/cybercrisispreparedness**.
- Golden SAML: ampliación de un ataque desde la red corporativa a los recursos de la nube, 22 de noviembre de 2017: **https://www.gov.il/BlobFolder/reports/saml/he/SAML-CERT-IL-W-365.pdf**.

Publicaciones de la Agencia Nacional de Tecnología Digital de Israel (en hebreo)

- Documento de gestión de riesgos, cumplimiento y control en la nube (GRC), 21 de enero de 2024: **https://www.gov.il/he/pages/grcnews**.
- Un modelo operativo en la nube gubernamental en términos de procesos y cambio en la organización, 23 de noviembre de 2023: **https://www.gov.il/he/pages/operatingmodel_news**.
- Estrategia gubernamental para la nube, 11 de diciembre de 2022: **https://www.gov.il/he/pages/strategy_1**.

Publicaciones de la Autoridad de Protección de la Privacidad de Israel (en hebreo)

- Una nueva guía para la implementación del artículo 10 del Reglamento de Aseguramiento de la Información: mantenimiento de documentación y registros, 29 de septiembre de 2024: **https://www.gov.il/he/pages/takana10d**.

- Los retos en la transición a la nube de bases de datos y sistemas de bases de datos, 5 de septiembre de 2024: **https://www.gov.il/he/pages/cloud_databases**.

- Orientación sobre el papel de la dirección en el cumplimiento de las obligaciones corporativas según el Reglamento de Protección de la Privacidad (aseguramiento de la información), 3 de septiembre de 2024: **https://www.gov.il/he/pages/the_board_role**.

- Una amplia enmienda a la Ley de Protección de la Privacidad, la más completa que se ha realizado en la ley desde su promulgación hace 43 años, que aumenta las herramientas de aplicación y los poderes de la Autoridad de Protección de la Privacidad de Israel: **https://www.gov.il/he/pages/13_amendment**.

- Una guía de referencia metodológica para realizar una revisión del impacto de la privacidad, una herramienta que ayudará a las organizaciones de la economía a evaluar y reducir los riesgos para la privacidad, 23 de noviembre de 2022: **https://www.gov.il/he/pages/taskir_privacy_news**.

Publicaciones de otros organismos gubernamentales de Israel (en hebreo)

- Principios, política, regulación y ética en el campo de la inteligencia artificial 2023, Ministerio de Innovación, Ciencia y Tecnología. 14 de diciembre de 2023: **https://www.gov.il/he/pages/ai_23**.

- Computación en la nube (Instr. 362), Supervisión de Bancos. 13 de junio de 2022: **https://www.boi.org.il/roles/supervisionregulation/nbt/nbt362/**.

- Gestión de la ciberseguridad (Instr. 361), Supervisión de Bancos. 30 de septiembre de 2021: **https://boi.org.il/roles/supervisionregulation/nbt/nbt361/**.

Publicaciones de organismos gubernamentales de fuera de Israel

Alemania

- Criteria catalogue C5: **https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html**

Australia

- Information security manual (ISM): **https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism**.

- Our cloud information governance policy: **https://www.naa.gov.au/about-us/who-we-are/accountability-and-reporting/our-cloud-information-governance-policy**.

Estados Unidos

- Cloud gov: **https://cloud.gov**.

- Dod cloud computing security: **https://public.cyber.mil/dccs/**.

- The federal risk and authorization management program (fedramp): **https://www.fedramp.gov/**.

Reino Unido

- Cloud security guidance, NCSC: **https://www.ncsc.gov.uk/collection/cloud**.

Unión Europea

- EU cloud certification scheme: **https://ec.europa.eu/newsroom/cipr/items/713799/en**.

Publicaciones de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA)

- CISA and NSA release cybersecurity information sheets on cloud security best practices, 7 de marzo de 2024: **https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices**.
- Guide to securing remote access software, 6 de junio de 2023: **https://www.cisa.gov/resources-tools/resources/guide-securing-remote-access-software**.
- Zero trust maturity model, abril de 2023: **https://www.cisa.gov/zero-trust-maturity-model**.
- Protecting against malicious use of remote monitoring and management software, 26 de enero de 2023: **https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a**.
- CISA releases JCDC remote monitoring and management (RMM) cyber defense plan, 16 de agosto de 2023: **https://www.cisa.gov/news-events/alerts/2023/08/16/cisa-releases-jcdc-remote-monitoring-and-management-rmm-cyber-defense-plan**.
- Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations, 15 de abril de 2021: **https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a**.
- Free tools for cloud environments: **https://www.cisa.gov/resources-tools/resources/free-tools-cloud-environments**.
- Open source vulnerabilities (OSV): **https://www.cisa.gov/resources-tools/services/open-source-vulnerabilities-osv**.
- Software bill of materials (SBOM): **https://www.cisa.gov/sbom**.
- Cisa #stopransomware: **https://www.cisa.gov/stopransomware**.

Publicaciones de la Cloud Security Alliance (CSA)

- Zero Trust Guiding Principles v1.1, 9 de marzo de 2024: **https://cloudsecurityalliance.org/artifacts/zero-trust-principles-v-1-1**.
- Top threats to cloud computing 2024, 5 de agosto de 2024: **https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024**.
- AI model risk management framework, 23 de julio de 2024: **https://cloudsecurityalliance.org/artifacts/ai-model-risk-management-framework**.
- Security guidance for critical areas of focus in cloud computing v5, 15 de julio de 2024: **https://cloudsecurityalliance.org/artifacts/security-guidance-v5**.
- How to design a secure serverless architecture, 23 de octubre de 2023: **https://cloudsecurityalliance.org/artifacts/how-to-design-a-secure-serverless-architecture**.
- Moveit exploit & ransomware attack: why SAAS security is critical during a cyberattack, 11 de agosto de 2023: **https://cloudsecurityalliance.org/blog/2023/11/08/moveit-exploit-ransomware-attack-why-saas-security-is-critical-during-a-cyberattack**.
- SaaS governance best practices for cloud customers, 10 de octubre de 2022: **https://cloudsecurityalliance.org/artifacts/saas-governance-best-practices-for-cloud-customers**.
- SaaS security and misconfigurations report, 4 de abril de 2022: **https://cloudsecurityalliance.org/artifacts/saas-security-and-misconfigurations-report**.
- Cloud incident response framework, 5 de abril de 2021: **https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework**.

Publicaciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

- ENISA Threat Landscape 2024: **https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024**.
- Best Practices for Cyber Crisis Management: **https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management**.

Publicaciones de la Organización Internacional de Normalización (ISO)

- Cybersecurity — guidelines for internet security.
- ISO/IEC 42001:2023. Information technology - Artificial intelligence - Management system: **https://www.iso.org/standard/81230.html**.
- ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems – Requirements.
- ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls.
- ISO/IEC 27018:2019. Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- ISO/IEC 27701:2019. Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines.
- ISO/IEC 27017:2015. Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

Publicaciones de la organización MITRE

- D3FEND. A knowledge graph of cybersecurity countermeasures: **https://d3fend.mitre.org/**.
- MITRE ATT&CK framework: **https://attack.mitre.org/**.
- Threat modeling with ATT&CK v1.0.0: **https://center-for-threat-informed-defense.github.io/threat-modeling-with-attack/**.
- MITRE ATLAS: **https://atlas.mitre.org/**.
- MITRE Engage: **https://engage.mitre.org/**.

Publicaciones del Instituto Nacional de Normas y Tecnología (NIST)

- NIST SP 800-63-4 (2nd Public Draft). Digital Identity Guidelines: **https://csrc.nist.gov/pubs/sp/800/63/4/2pd**.
- NIST SP 800-201. NIST cloud computing forensic reference architecture, julio de 2024: **https://csrc.nist.gov/pubs/sp/800/201/final**.
- NIST SP 800-61 rev. 3 (initial public draft). Incident response recommendations and considerations for cybersecurity risk. Management: a CSF 2.0 community profile, 3 de abril de 2024: **https://csrc.nist.gov/pubs/sp/800/61/r3/ipd**.
- NIST SP 1800-28. Data confidentiality: identifying and protecting assets against data breaches, febrero de 2024: **https://csrc.nist.gov/pubs/sp/1800/28/final**.
- NIST cybersecurity framework (CSF) 2.0, 26 de febrero de 2024: **https://www.nist.gov/cyberframework**.

- NIST SP 800-82 rev. 3. Guide to operational technology (OT) security, septiembre de 2023: **https://csrc.nist.gov/pubs/sp/800/82/r3/final**.
- NIST AI RMF playbook, 30 de marzo de 2023: **https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook**.
- NIST AI RMF v1.0, enero de 2023: **https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development**.
- NIST IR 8374. Ransomware risk management: a cybersecurity framework profile, febrero de 2022: **https://csrc.nist.gov/pubs/ir/8374/final**.
- NIST SP 800-218. Secure software development framework (SSDF) version 1.1: recommendations for mitigating the risk of software vulnerabilities, febrero de 2022: **https://csrc.nist.gov/pubs/sp/800/218/final**.
- NIST SP 1800-25. Data integrity: identifying and protecting assets against ransomware and other destructive events, diciembre de 2020: **https://csrc.nist.gov/pubs/sp/1800/25/final**.
- NIST SP 1800-11 series. Data integrity: recovering from ransomware and other destructive events, septiembre de 2020: **https://www.nccoe.nist.gov/data-integrity-recovering-ransomware-and-other-destructive-events**.
- NIST SP 800-53 rev. 5. Security and privacy controls for information systems and organizations, septiembre de 2020: **https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final**.
- NIST IR 8006. NIST cloud forensic science challenges, agosto de 2020: **https://csrc.nist.gov/projects/cloud-forensics**.
- NIST SP 800-145. The NIST definition of cloud computing, septiembre de 2011: **https://csrc.nist.gov/pubs/sp/800/145/final**.
- NIST cloud computing reference architecture, 8 de septiembre de 2011: **https://www.nist.gov/publications/nist-cloud-computing-reference-architecture**.

Publicaciones del Proyecto abierto de seguridad en aplicaciones web (OWASP)

- OWASP Application security verification standard (ASVS): **https://owasp.org/www-project-application-security-verification-standard/**.
- OWASP MASVS (mobile application security verification standard): **https://mas.owasp.org/MASVS/**.
- OWASP Top 10 API security risks – 2023: **https://owasp.org/API-Security/editions/2023/en/0x11-t10/**.
- OWASP Top 10 CI/CD security risks: **https://owasp.org/www-project-top-10-ci-cd-security-risks/**.
- OWASP Cloud-native application security top 10: **https://owasp.org/www-project-cloud-native-application-security-top-10/**.

Publicaciones del instituto SANS

- SANS cloud security exchange 2024 eBook - Cloud security: first principles and future opportunities, agosto de 2023: **https://www.sans.org/white-papers/cloud-security-first-principles-future-opportunities/**.
- Cybersecurity in the age of the cloud, febrero de 2020: **https://www.sans.org/media/cloud-security/eBook_cloud-security.pdf?msc=cloudsecuritylp**.
- Incident management 101 preparation and initial response (aka identification), enero de 2005: **https://www.sans.org/white-papers/1516/**.

Publicaciones de proveedores de nube pública reconocidos

Amazon Web Services (AWS)

- AWS cloud adoption framework (AWS CAF): **https://aws.amazon.com/cloud-adoption-framework/**.
- Protecting against ransomware. Mitigate ransomware for your organization with AWS: **https://aws.amazon.com/es/security/protecting-against-ransomware/**.
- Design SaaS on AWS: **https://aws.amazon.com/saas/design/**.

Microsoft Azure

- Microsoft Cloud Adoption Framework for Azure: **https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/**.
- Ransomware protection in Azure: **https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-protection**.
- ENISA information assurance framework: **https://learn.microsoft.com/en-us/compliance/regulatory/offering-enisa**.

Google Cloud Platform (GCP)

- Framework de adopción de Google Cloud: **https://cloud.google.com/adoption-framework**.
- Prácticas recomendadas para mitigar ataques de ransomware con Google Cloud: **https://cloud.google.com/architecture/bps-for-mitigating-ransomware-attacks**.
- Standardizing privileged access architecture for multi-cloud v2.0: **https://services.google.com/fh/files/misc/standardizing-privileged-access-architecture-for-multi-cloud.pdf**.

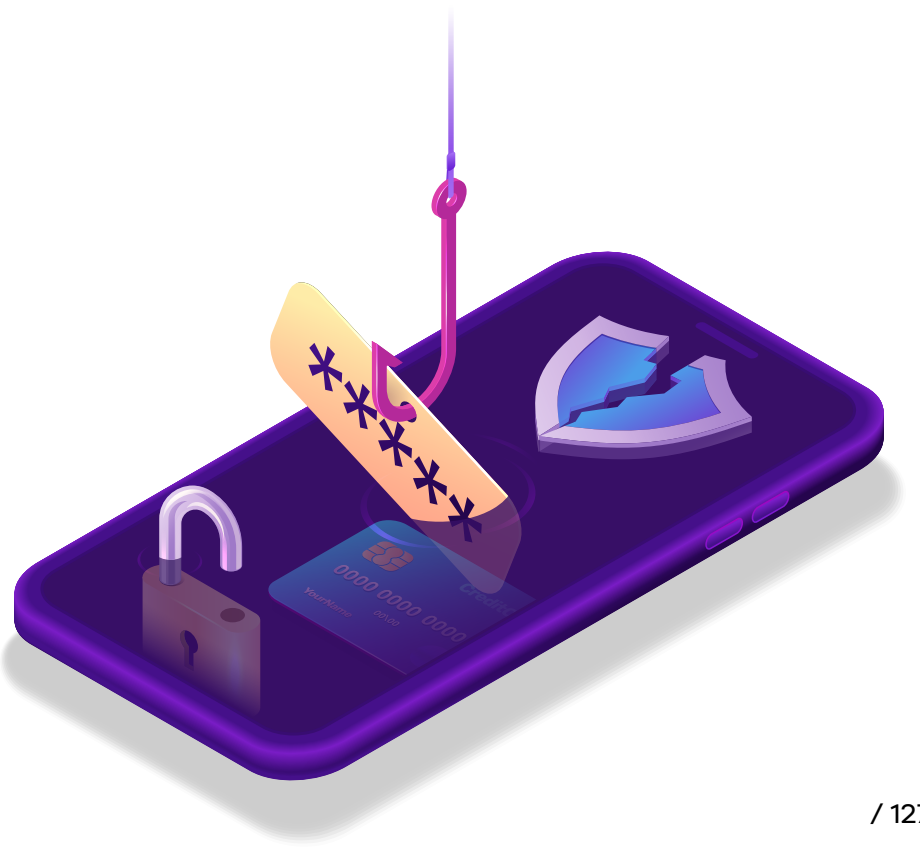
Oracle Cloud Infrastructure (OCI)

- Cloud adoption framework for Oracle Cloud Infrastructure (OCI): **https://www.oracle.com/cloud/cloud-adoption-framework/**.
- CISO perspectives: advanced cyber-resilience in OCI. Protecting your tenancy against ransomware style threats: **https://www.ateam-oracle.com/post/ciso-perspectives-protecting-your-oci-tenancy-against-ransomware-attacks**.
- Oracle Cloud Infrastructure (OCI) security best practices: **https://docs.oracle.com/en-us/iaas/Content/Security/Reference/configuration_security.htm**.

Publicaciones de otros autores

- A detailed analysis of the frequency and impact of ransomware events, Cyentia: **https://www.cyentia.com/iris-ransomware/**.
- The state of security in cloud native development 2024, CNCF: **https://www.cncf.io/blog/2024/09/26/the-state-of-security-in-cloud-native-development-2024/**.
- Best practices for cloud ransomware protection in 2024, SentinelOne: **https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-ransomware-protection/**.
- New mamba 2fa bypass service targets microsoft 365 accounts, Bleeping Computer: **https://www.bleepingcomputer.com/news/security/new-mamba-2fa-bypass-service-targets-microsoft-365-accounts/**.
- Using honeytokens to detect (AiTM) phishing attacks on your microsoft 365 tenant, Zolder: **https://zolder.io/blog/using-honeytokens-to-detect-aitm-phishing-attacks-on-your-microsoft-365-tenant/**.
- How to protect against AiTM/Evilginx phishing attacks, Cognisys: **https://cognisys.co.uk/blog/how-to-protect-against-aitm-evilginx-phishing-attacks/**.

- X-force report reveals top cloud threats: AiTM phishing, business email compromise, credential harvesting and theft, IBM: **https://www.ibm.com/blog/x-force-cloud-threat-landscape/**.
- Best practices for securing active directory, Microsoft Learn Challenge: **https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory**.
- Amazon Web Services (AWS) data breaches: full timeline through 2023, Firewall Times: **https://firewalltimes.com/amazon-data-breach-timeline/**.
- Ransomware in the cloud: breaking down the attack vectors, Paloalto: **https://www.paloaltonetworks.com/blog/prisma-cloud/ransomware-data-protection-cloud/**.
- Cloud governance – definition, framework, and principles, TATA: **https://www.tatacommunications.com/knowledge-base/cloud-governance/**.
- The global state of CPS security 2024: business impact of disruptions, Claroty: **https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions**.
- Cyberattacks and security of cloud computing: a complete guideline, MDPI: **https://www.mdpi.com/2073-8994/15/11/1981**.
- Detecting and mitigating Active Directory compromises, Gobierno de Australia: **https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/detecting-and-mitigating-active-directory-compromises**.
- HackTricks: **https://book.hacktricks.xyz/**.
- Incident response in Google Cloud: forensic artifacts, Sygnia: **https://www.sygnia.co/blog/gcp-incident-response/**.
- Announcing 'Cirrus' – new opensource tool to combat google cloud incident response challenges, Sygnia: **https://www.sygnia.co/blog/new-opensource-tool-to-combat-google-cloud-incident-response-challenges/**.
- SaaS attack techniques, GitHub: **https://github.com/pushsecurity/saas-attacks**.
- Economic denial of sustainability (EDoS) mitigation approaches in cloud: analysis and open challenges, IEEE Xplore: **https://ieeexplore.ieee.org/document/8167135**.
- Multi-cloud security: key challenges and effective practices from experts, Tech Magic: **https://www.techmagic.co/blog/multi-cloud-security**.
- Public cloud security breaches: **https://www.breaches.cloud/**.



En los últimos años puede observarse una tendencia creciente en la que cada vez más organizaciones trasladan la gestión de sus recursos e información a servicios de nube pública, cuyos beneficios incluyen la colaboración entre las partes interesadas (*stakeholders*), agilidad, flexibilidad, disponibilidad y reducción de costes. Sin embargo, la transición al uso de una nube pública atrae no solo a los clientes y organizaciones, sino también a quienes buscan aprovecharse de estas plataformas. No sorprende que en años recientes se identifiquen cada vez más campañas en las que actores maliciosos realizan ataques de secuestro de datos (*ransomware*) contra entidades que utilizan estas tecnologías.

En vista de esto, es necesario que las organizaciones que utilizan los servicios de nube pública tomen las medidas adecuadas para reducir el riesgo de un ciberincidente, incluyendo el *ransomware*. La finalidad de esta publicación es proporcionar información centralizada, dirigida a las autoridades de ciberseguridad y protección de la información acerca de las ciberamenazas en general, y la amenaza de *ransomware* en particular, y también presentar estudios de caso para fomentar la sensibilización sobre la amenaza de *ransomware* y las formas de reducir el riesgo existente, con el objetivo de que las organizaciones puedan adoptar las recomendaciones y ajustar su plan de seguridad anual para hacer frente a estos 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

Volumen B: Un enfoque técnico

- **B.01** Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)
- **B.02** Seguridad de infraestructuras Access Point Name (APN)
- **B.03** Endurecimiento de sistemas informáticos
- **B.04** Reducción de riesgos de ciberseguridad en cámaras de videovigilancia
- **B.05** Reducción de los riesgos de ciberseguridad en los puntos finales de la organización
- **B.06** Seguridad de sistemas de planificación de recursos empresariales (ERP)
- **B.07** Preparación y respuesta ante un ataque de *ransomware* en la organización
- **B.08** Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.09** Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.10** Seguridad de infraestructuras de voz sobre protocolo de internet (VoIP)
- **B.11** Autenticación multifactor avanzada ante amenazas de ciberseguridad
- **B.12** Principales amenazas de ciberseguridad de las plataformas de asistencia remota a usuarios
- **B.13** Prevención y respuesta ante un secuestro de Border Gateway Protocol (BGP Hijacking)
- **B.14** Preparación ante ataques distribuidos de denegación de servicio (DDoS)
- **B.15** Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)
- **B.16** Ciberseguridad por medio de sistemas de gestión de dispositivos móviles (MDM/EMM)
- **B.17** Seguridad en la transferencia gestionada de archivos (MFT)
- **B.18** Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)
- **B.19** Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí
- **B.20** Seguridad de los sistemas multimedia
- **B.21** Integración de principios de ciberseguridad en los procesos de respaldo y recuperación
- **B.22** Protección de los servicios de nube pública ante amenazas de *ransomware*

Volumen C: Desarrollo seguro de *software*