Trabajando en "Las Nubes"

DOI: 10.29236/sistemas.n171a2

Sandra Rueda

Por sus beneficios, el uso de la tecnología de nube ha aumentado de forma consistente en los últimos años, sin embargo, esta tecnología también ha creado nuevos retos de ciberseguridad. Este artículo ofrece recomendaciones para facilitar el aseguramiento de servicios en "las nubes".

La organización NIST (*National Institute of Standards and Technology*) define Cómputo en la Nube como "*un modelo para habilitar acceso ubicuo, conveniente y por demanda a un conjunto compartido de recursos configurables de cómputo que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de administración mínimo"* (Mell & Grance, 2011). Entre las ventajas de esta tecnología podemos mencionar, reducir el costo de la infraestructura tecnológica y

su mantenimiento, mejorar la capacidad de responder a cambios en la demanda de recursos y ampliar la posibilidad de conexión a servicios vía internet.

Considerando estas ventajas, no sorprende que el uso de servicios en la nube haya crecido de forma consistente en los últimos años. La Figura 1 muestra la inversión realizada por diferentes empresas, desde 2017, en tecnología de nube y se puede observar un crecimiento consistente en el valor de la inversión. Los valores estimados para la inversión en 2024 y 2025 son US$675430 millones de dólares ($675,43 *US billions*) y US$824760 millones de dólares ($824,76 *US billions*) respectivamente (Statista, 2024).

Gartner por su parte pronostica un crecimiento del 22,1% en el valor de las inversiones para 2025 (Gartner, 2024). Con base en estos datos podemos afirmar que el valor de la inversión y el número de empresas consumidoras de tecnología de nube seguirá creciendo en los próximos años.

Principales Retos para Asegurar un Servicio en la Nube

El amplio uso de tecnología de nube justifica el trabajo de los expertos para garantizar la seguridad y privacidad de datos y servicios en ese contexto. Entre los principales retos que las empresas deben enfrentar cuando deciden migrar un servicio a la nube podemos identificar: asumir el modelo de responsabilidad compartida, manejar el aumento de la superficie de ataque y la pérdida de visibilidad y responder a los requerimientos de privacidad y cumplimiento.

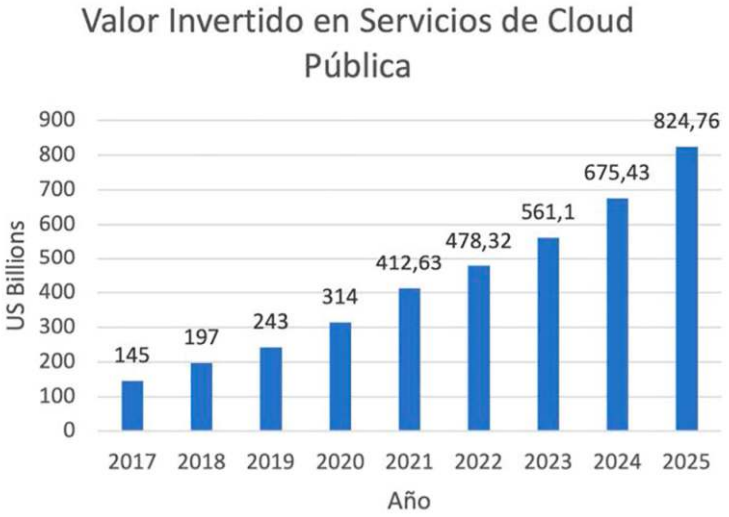

Figura 1. Inversión en Servicios de Cloud Pública (datos de Statista).

Asumir el modelo de responsabilidad compartida. Las empresas medianas y pequeñas, y algunas grandes, creen que migrando sus servicios a la nube transfieren al proveedor la responsabilidad de resolver los problemas de seguridad, pero, esta creencia es errónea. Al migrar los servicios a la nube la responsabilidad no se transfiere completamente, se distribuye, dando lugar a un modelo de responsabilidad compartida. Esto ocurre porque la migración no cambia los requerimientos de seguridad de un servicio o un conjunto de datos, los requerimientos de confidencialidad, integridad, disponibilidad y privacidad se conservan, pero las soluciones deben ser implementadas de forma compartida por el proveedor y la empresa que compra el servicio de nube.

La distribución de responsabilidades varía dependiendo del modelo de servicio; Infraestructura como Servicio, Plataforma como Servicio y Software como Servicio implican variaciones en las responsabilidades de proveedores y clientes. Google Cloud (Google Cloud, s.f.), Microsoft Azure (Microsoft, 2023) y otros proveedores de nube tienen sus propias versiones del modelo de responsabilidad compartida, los nombres de las capas usadas varían un poco, pero todos comparten el concepto fundamental: tanto el proveedor como el cliente son responsables del despliegue seguro de un servicio en la nube. Como consecuencia, la empresa que despliega un servicio en la nube debe identificar sus responsabilidades, entre las cuales podemos mencionar dos tareas que el cliente siempre debe asumir: (i) la identificación de los requerimientos de seguridad de sus datos y servicios, y (ii) hacer (o contratar) un análisis de riesgos para verificar que los requerimientos de seguridad están siendo gestionados de forma apropiada.

Manejar el aumento en la exposición de los datos y servicios. Un servicio de nube da mayor conexión a los usuarios gracias al uso de protocolos de comunicación estándar que facilitan la conexión vía internet con dispositivos como servidores, computadores de escritorio, laptops, tabletas y teléfonos celulares inteligentes. Por otro lado, los atacantes pueden usar está misma capacidad de acceso para desplegar ataques vía internet. La empresa que despliega un servicio en la nube es responsable de evaluar el riesgo asociado, decidir cómo manejarlo y definir las políticas de seguridad correspondientes. Además, dependiendo del modelo de servicio, debe implementar controles en las capas que estén bajo su responsabilidad.

Manejar la pérdida de visibilidad. El control de una empresa sobre su infraestructura y mecanismos en una instalación local (*on-premise*) es completo, pero cuando migra un servicio a la nube mueve sus recursos fuera del alcance de su red y transfiere parte del control al pro-

veedor. Además, un servicio en la nube permite a los empleados conectarse desde cualquier parte, a cualquier hora y con diferentes dispositivos. Con el auge de trabajo remoto desde la pandemia de COVID-19, estas características son ideales, sin embargo, las empresas pueden perder visibilidad sobre cómo y cuándo se usa su información y, como los recursos en la nube están fuera del alcance de una red corporativa, las herramientas tradicionales no sirven para monitorear los recursos protegidos.

Manejar los requerimientos de privacidad y cumplimiento. La privacidad se define como el derecho de todos los individuos a controlar lo que se sabe y se almacena sobre ellos mismos. Las regulaciones sobre protección de datos personales son consecuencia de este derecho y su cumplimiento debe ser una de las prioridades de cualquier empresa que recopile, almacene y procese los datos de sus usuarios, tanto por el aspecto legal como por principios éticos dado que las regulaciones protegen aspectos sensibles de las personas (International Telecommunication Union-ITU, 2012). Adicionalmente, al mover datos a la nube, hay que considerar que serán almacenados en centros de datos distribuidos en diferentes sitios geográficos y, por otro lado, algunos países tienen regulaciones que establecen restricciones sobre los sitios de procesamiento y almacenamiento de datos sensibles y datos personales de sus ciudadanos, como en el caso de la limitación geográfica de GDPR (*General Data Protection Regulation*) de la Unión Europea (Intersoft Consulting, s.f.).

Aunque los proveedores de nube ofrecen herramientas que permiten satisfacer estándares de cumplimiento, es responsabilidad de los clientes identificar la regulación que deben cumplir, como PCI DSS (P*ayment Card Industry Data Security Standard*) o GDPR (*General Data Protection Regulation*), y definir e implementar políticas y controles que protejan sus datos de fugas y usos no autorizados y permitan cumplir con la regulación.

Incidentes Recientes

El reporte de seguridad en nube para 2024 de Cybersecurity Insiders y Check Point indica que 61% de las empresas con servicios de nube reportan haber sufrido incidentes de seguridad durante los últimos 12 meses, lo cual representa un incremento de 24% con respecto al año anterior. 23% de los encuestados no están seguros o no pueden reportar los incidentes y solo 16% dicen que no hubo incidentes (Check Point y Cybersecurity Insiders, 2024).

Entre los principales problemas de seguridad que conducen a incidentes están:

- Errores de configuración. Estos errores son una de las principales causas de problemas de se-

guridad y fugas de datos. Ocurren por desconocer las características de una infraestructura de nube, no comprender el alcance/limitaciones de los controles de seguridad, y por la heterogeneidad de despliegues multinube (Check Point, s.f.). Estos errores incluyen fallas en: la gestión de vulnerabilidades, en el uso de autenticación multifactor, en la configuración del control acceso y en la configuración de las interfaces de conexión a los servicios de nube (Check Point, s.f.) (THALES, 2024).

- Secuestro de cuentas. Algunos usuarios tienen contraseñas débiles y las usan en varios servicios. Esto facilita que un atacante logre acceso no autorizado a una cuenta legítima y la use para robar datos, sin que los administradores del servicio lo noten. (Check Point, s.f.)
- Mecanismos no controlados para compartir datos. La tecnología de nube está diseñada para facilitar la tarea de compartir datos e incluye la posibilidad de crear un enlace que se envía por correo electrónico para dar acceso a un recurso, sin necesidad de autenticación. Este mecanismo permite que el enlace sea reenviado múltiples veces y dificulta controlar quién tiene acceso a un recurso (Check Point, s.f.)
- Ciberataques. Los servicios en nube son un objetivo atractivo para un atacante porque la infraestructura subyacente ofrece un alto nivel de conectividad vía internet, lo cual facilita el intento de acceso con un costo muy bajo. Además, tienen una alta probabilidad de presentar errores de configuración y almacenan gran cantidad de datos que pueden ser valiosos (Check Point, s.f.) (THALES, 2024). Adicionalmente, como la configuración de la infraestructura es estándar es posible que una técnica de ataque pueda repetirse con una alta probabilidad de éxito, de hecho, en 2023 Mandiant y VMware remediaron una vulnerabilidad de día cero; esta situación probó que los atacantes tienen los ambientes de nube entre sus objetivos (Google Cloud, 2024)

Factores Adicionales

Además de los retos mencionados, hay tres factores que amplifican la problemática de seguridad que se debe enfrentar al migrar servicios a la nube: herramientas específicas, falta de expertos y complejidad del ambiente.

Herramientas Específicas. Las herramientas que ofrecen los proveedores de nube para implementar políticas de seguridad son diferentes de las herramientas usadas en infraestructuras locales. Esto significa que el equipo de seguridad debe familiarizarse con herramientas nuevas, y a menudo complejas por la gran cantidad de opciones de configuración, identificando el alcance de estas y cómo gestionarlas.

Falta de Expertos. Asegurar servicios en la nube es diferente de asegurarlos en una instalación local (*on-premise*) y los equipos de seguridad deben ser conscientes.

Estas diferencias incluyen el conjunto de riesgos, dado que hay mayor exposición de los recursos, un participante adicional que puede tener privilegios (el proveedor de servicios) y un conjunto diferente de herramientas. El reporte de seguridad en nube para 2024 de Cybersecurity Insiders y Check Point menciona que 76% de los encuestados han enfrentado la falta de profesionales expertos en seguridad en contextos de nube (Check Point y Cybersecurity Insiders, 2024). The Cloud Security Alliance (CSA) también incluyó la falta de conocimientos y experiencia como uno de los principales retos para 2023. (Cloud Security Alliance, 2023)

Complejidad del Ambiente. Es común que un cliente decida construir un ambiente híbrido o multinube, el primero combina una nube pública y una privada, o una nube pública y una instalación local, mientras el segundo ambiente combina dos o más proveedores de nube. Estas combinaciones ofrecen la posibilidad de distribuir cargas de trabajo de forma flexible con base en las necesidades de la organización y en las ventajas del proveedor, como precio, capacidad de procesamiento y distribución geográfica. Sin embargo, los equipos de seguridad deben enfrentar un nivel de complejidad mayor al que se enfrenta en una instalación local en todas las combinaciones. Esta complejidad es resultado de las diferencias de funcionalidad, interfaces y herramientas en cada plataforma, agrava la pérdida de visibilidad y hace más difícil la tarea de asegurar los servicios y datos en la nube. (Check Point y Cybersecurity Insiders, 2024) (THALES, 2024)

Recomendaciones

El Centro Nacional para la Ciberseguridad del Reino Unido hace las siguientes recomendaciones tradicionales para escoger, configurar y usar servicios de nube de forma segura: proteger los datos en tránsito, proteger los activos en almacenamiento y en procesamiento, identificar las técnicas de aislamiento de clientes, usar un framework para gobernanza de la seguridad, implementar técnicas para operar y manejar los servicios de forma segura, considerar el acceso del personal del proveedor, diseñar, desarrollar y desplegar los servicios de forma segura, considerar la seguridad de la cadena de suministros, administrar usuarios, manejar identidad y autenticación, proteger las interfaces externas, asegurar los sistemas de administración, auditar y alertar, y usar seguridad por defecto. (National Cyber Security Centre, s.f.)

Además de estos principios tradicionales, con base en las amenazas y retos identificados más re-

cientemente, es recomendable tener en cuenta (ISC2 y Cybersecurity Insiders, 2024) (Google Cloud, 2024):

- Automatizar. Usar herramientas automatizadas para evaluar configuración y comportamiento y monitorear en tiempo real para detectar amenazas y responder rápidamente.
- Incorporar IA (Inteligencia Artificial). La rápida evolución de la IA generativa ofrece a los atacantes una nueva herramienta para mejorar sus técnicas. Los expertos en seguridad deberían usar esta misma tecnología para mejorar su capacidad de prevención, detección y respuesta.
- Mejorar la protección de datos. Usar cifrado, control de acceso y técnicas de prevención de fuga de datos para proteger información sensible.
- Invertir en entrenamiento y certificación. Ofrecer entrenamiento que permita a los equipos de seguridad entender los retos de seguridad en la nube y diseñar y construir arquitecturas apropiadas para las necesidades de la organización.
- Adoptar un modelo de confianza cero. El modelo busca proteger los recursos, suponiendo que la confianza nunca debe asignarse implícitamente y debe evaluarse continuamente.
- Construir un plan de respuesta a incidentes. Este plan debe adaptarse a las características de un servicio en nube para responder eficazmente a un incidente de seguridad.

Desplegar un servicio seguro en nube puede ser una tarea compleja que debe abordarse de forma organizada; entendiendo las responsabilidades asociadas, capacitándose y aprendiendo sobre las características de la infraestructura de nube, las herramientas disponibles y los retos presentes, y apoyándose en recomendaciones de centros reconocidos y expertos.

Referencias

Statista. (2024). *Public cloud services end-user spending worldwide from 2017 to 2024*. Retrieved from Estadísticas: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/)

Mell, P., & Grance, T. (2011, September). The NIST Definition of Cloud Computing (Special Publication 800-145).

Intersoft Consulting. (n.d.). Retrieved Junio 2024, from GDPR: https://gdpr-info.eu/art-3-gdpr/

ISC2 y Cybersecurity Insiders. (2024). *2024 Cloud Security Report*.

International Telecommunication Union-ITU. (2012). *Privacy in Cloud Computing*.

Check Point y Cybersecurity Insiders. (2024). *2024 Cloud Security Report*.

Check Point. (n.d.). *Top 15 Cloud Security Issues, Threats and Concerns*. Retrieved Junio 2024, from Check Point Cyber Hub: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

THALES. (2024). *2024 Cloud Security Study*.

Cloud Security Alliance. (2023, Abril). *Top Cloud Security Challenges in 2023*. Retrieved Junio 2024, from Cloud Security Alliance: https://cloudsecurityalliance.org/blog/2023/04/14/top-cloud-security-challenges-in-2023

Google Cloud. (2024). *Insights for Future Planning. Google Cloud*. (n.d.). Shared responsibilities and shared fate on Google Cloud. Retrieved Junio 2024, from Cloud Architecture Center: https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

Microsoft. (2023). *Responsabilidad compartida en la nube*. Retrieved Junio 2024, from Documentación de los aspectos básicos de la seguridad en Azure: https://learn.microsoft.com/es-es/azure/security/fundamentals/shared-responsibility

National Cyber Security Centre. (n.d.). *The Cloud Security Principles*. Retrieved Junio 2024, from Cloud Security Guidance: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

Gartner. (2024, Mayo). *Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024*. Retrieved Junio 2024, from Gartnet Newsroom: https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024

Sandra Rueda: *Profesora asociada en el Departamento de Ingeniería de Sistemas y Computación de la Universidad de los Andes, Colombia. Ph.D. Computer Science and Engineering, The Pennsylvania State University, Estados Unidos. Sus áreas de investigación son seguridad de sistemas de software, análisis y generación automática de políticas de control de acceso y ciberseguridad en plataformas emergentes como IoT y móviles.*