accenture

Una Nube Segura

Cómo acelerar la resiliencia y hacer que tu transformación a cloud-first sea segura desde el principio

Contenido

Nubes de tormenta en el horizonte

Ahora más que nunca, las organizaciones deben priorizar un enfoque "cloud first" para lograr una transformación con agilidad y a escala. Pero, tal como su nombre lo sugiere, cada nueva instancia de la nube pública tiene el potencial de generar una tormenta de seguridad.

Los Proveedores de Servicios Cloud (Cloud Service Providers o CSPs) han trabajado mucho para asegurar su infraestructura y mejorar las características de su seguridad nativa, innovando para crear y lanzar nuevas funcionalidades a un ritmo cada vez más rápido. Sin embargo, estos proveedores no son responsables de mantener una sólida postura de seguridad en un ambiente cloud. Es poco probable que cuando se crea una nueva instancia de cloud la configuración predeterminada satisfaga los requisitos básicos de seguridad de cualquier operación de negocios. Cada organización sigue siendo responsable de aplicar las herramientas para asegurar el entorno que crean—y las aplicaciones que desarrollan—para usarlas en la nube.

> **La seguridad suele percibirse como el mayor inhibidor de una transformación cloud-first, pero en realidad puede ser su mayor acelerador.**

Un aluvión de disrupciones

Muchas empresas se han sentido atraídas por la eficiencia, la elasticidad y la innovación que ofrece la nube. Sin embargo, el 2020 se destaca como el año en el cual las organizaciones, en todas las industrias, tuvieron un recordatorio poderoso y directo de la importancia de la resiliencia, agilidad, adaptabilidad y escalabilidad de los sistemas.

A pesar de esta llamada de atención sin precedentes, y la promesa de que cloud satisfaría las nuevas demandas, menos del 40% de las empresas manifiesta que están logrando todo el valor que esperaban de sus inversiones en cloud.[1]

Si bien la nube ofrece nuevas oportunidades para modernizar servicios y transformar operaciones, el riesgo de seguridad y cumplimiento sigue siendo la mayor barrera para adoptar la tecnología cloud. Combinada con la complejidad de los ambientes híbridos y multi-cloud y la escasez de conocimientos, estas preocupaciones pueden **convertirse en obstáculos importantes para lograr una transformación cloud-first.**

Proporcionar seguridad en la nube no es un ejercicio fácil, del tipo "lift and shift". Exige una intención estratégica, un modelo de gobierno flexible, la alineación —de la organización de TI y el negocio—y la implementación alineada con la tolerancia a los riesgos de toda la empresa.

> **Los líderes de seguridad pueden ayudar a proporcionar mejores resultados para el negocio y hacer que la transformación a cloud-first sea segura por diseño.**

DESAFÍO 1:

Debilidades en el gobierno y cumplimiento de la seguridad

El riesgo de la seguridad y el cumplimiento es la mayor barrera para aprovechar los beneficios de cloud, según el 65% de los altos ejecutivos de TI.[2] Los CISO deben poder comunicar un marco transparente de riesgos de gobierno, junto con un estricto monitoreo y remediación de anomalías, para mantener el cumplimiento.

DESAFÍO 2:

Abordar proactivamente la complejidad de una configuración segura

Las estrategias cloud están evolucionando y muchas organizaciones ya cuentan con un enfoque híbrido y multi-cloud. Sin embargo, según señaló la National Security Agency: "La mala configuración de los recursos cloud sigue siendo la vulnerabilidad más prevalente."[3] Se deben definir los activos y los controles de configuración al inicio y usar configuración automática para lograr una migración exitosa a la nube que tenga la seguridad incorporada desde el principio.

DESAFÍO 3:

Encontrar y retener las habilidades adecuadas

La automatización ayudar a mitigar la escasez de talento, pero las organizaciones deben ser más creativas para garantizar la existencia del conocimiento adecuado. El personal con conocimiento de seguridad cloud es escaso. En nuestro estudio, el 30% de las organizaciones líderes con mejor desempeño proporcionó capacitación a más de tres cuartos de los usuarios cuando fue necesario, comparado con tan solo el 9% de las demás[4] Los equipos de seguridad deben desarrollar la mentalidad adecuada, junto con las políticas, los procesos y procedimientos de seguridad apropiados para gestionar eficazmente un ambiente cloud seguro.

Gobierno y cumplimiento de la seguridad

En una época de adopción acelerada de cloud, el gobierno y el cumplimiento de las políticas pueden verse fácilmente eclipsados por la necesidad de moverse con rapidez y facilitar el negocio. Sin embargo, es posible lograr una supervisión constante de la seguridad y la privacidad, incluso durante períodos de rápida transformación.

Gobierno transparente

A medida que las empresas adoptan múltiples entornos cloud y los proveedores crean y lanzan nuevos servicios a un ritmo cada vez mayor, la seguridad sigue siendo tan importante como siempre. Sin embargo, ya sea que se trate de herramientas, procesos o incluso requisitos de conocimientos, la protección de los entornos cloud es substancialmente diferente de la protección que se aplica a los entornos on premise.

Las organizaciones aún precisan desarrollar o adquirir la habilidad de controlar y monitorear todos sus entornos cloud para identificar anomalías y luego remediarlas para mantener el cumplimiento.

Cumplimiento proactivo

Al definir nuevas políticas y procedimientos, configurar el marco apropiado, identificar los controles relevantes y crear una arquitectura de referencia específica para la nube, una organización puede aprovechar con mayor seguridad y rapidez el flujo continuo de los nuevos servicios que ofrecen los proveedores de servicios cloud para desarrollar nuevas capacidades y mejorar las decisiones de negocios.

No es suficiente con enviar alertas para identificar vulnerabilidades. Colocar barreras de seguridad con aceleradores prediseñados para servicios cloud nativos puede mitigar el riesgo antes de que ocurran los incidentes. La funcionalidad de bloqueo o auto reparación permite la aplicación continua y automática de políticas en apoyo de las regulaciones de la industria y los estándares aplicables a nivel empresa.

Seguridad proactiva de la nube

Una arquitectura de referencia tiene seis pilares clave que definen los requisitos mínimos para que las organizaciones coloquen workloads en la nube de forma segura.

Qué deberías hacer:

Asegurar la plataforma

Diseñar e implementar controles de seguridad básicos para crear "zonas de aterrizaje" seguras en la plataforma del proveedor de la solución cloud.

Asegurar los servicios

Diseñar templates de PaaS seguros y reutilizables de los proveedores de soluciones cloud con controles de seguridad integrados.

Integrar herramientas y operaciones

Combinar la plataforma y los servicios para integrar las herramientas de seguridad existentes del cliente con los procesos y procedimientos operativos a nivel empresa.

Cómo deberías hacerlo:

Gestión de acceso de identidad

Detallar los roles autorizados para operar en el entorno y qué tareas pueden hacer.

Seguridad de las redes

Asegurar la conectividad con centros de datos on-premise y usar un modelo de seguridad de red del tipo "hub and spoke".

Configuración segura de la nube

Asegurar políticas de configuración segura en "zonas de aterrizaje" y aplicar controles de seguridad en la plataforma del proveedor de servicios cloud.

Abordar el talento

Existe una escasez de talento, tanto en aspectos de seguridad como de cloud, que se amplifica al buscar profesionales con capacidades de seguridad específicas para la nube. La alta demanda y la oferta limitada obligan a los CISO a ser creativos para atraer y retener las habilidades necesarias para lograr una exitosa migración a cloud.

Cambio de mentalidad

Dado que es difícil adquirir este conocimiento, algunos CISO están buscando profesionales de SecOps de infraestructuras tradicionales con habilidades nativas on premise para tener éxito en cloud. Lo más importante que puede determinar el éxito o fracaso de esa transición es el deseo de cambiar. Cambiar de mentalidad a veces es el mayor obstáculo al que se enfrentan los profesionales de seguridad tradicionales.

Extender las habilidades de seguridad

La comunidad de desarrolladores surge como un lugar prometedor para encontrar talento en seguridad. Los desarrolladores comienzan a reconocer que los conocimientos de seguridad constituyen un valor adicional que pueden incorporar a sus conocimientos actuales. A medida que la distribución de los controles de seguridad llega a los desarrolladores que trabajan con infraestructura automatizada y repositorios de aplicaciones, las capacidades de seguridad se extienden naturalmente a otras áreas del negocio.

Estrategia cloud-first

Las estrategias de migración a cloud están evolucionando y son cada vez más complejas. El foco original "lift and shift" en máquinas virtuales puntuales ha dado lugar a entornos de computación híbridos y multi-cloud, con alto uso del Platform-as-a-Service.

Lograr la transparencia en este entorno complejo no es sencillo, sino que constituye un imperativo para monitorear un entorno de computación en rápida evolución.

Sin una estrategia formal y un gobierno sólido, las líneas de negocios individuales pueden desarrollar iniciativas que generen trabajo redundante, soluciones con controles duplicados, mala comunicación, mayores costos, mayor tiempo para obtener valor y lo que es más importante, un enfoque de seguridad reactivo.

> **Los líderes de seguridad deben considerar las cuatro dimensiones de la complejidad que influencian los resultados de su estrategia.**

Las cuatro dimensiones de la complejidad

#1 **Comprar versus desarrollar:** ¿Cuánto de nativo? ¿Cómo hacen los terceros para mantenerse al día con los servicios de los proveedores de servicios cloud en constante evolución?

#2 **Apto para un propósito:** ¿Cómo seleccionar un modelo/ proveedor cloud en base a la funcionalidad de las aplicaciones y la intersección de la seguridad?

#3 **Multi-cloud:** ¿Cuándo debería replicar los controles de seguridad en lugar de abstraerlos?

#4 **Escala y mantenimiento:** consistencia en las operaciones de seguridad.

Mover la seguridad a la izquierda

Si bien mitigar los riesgos y proteger los datos en la nube es una prioridad, se debe integrar la seguridad de manera consistente. Con demasiada frecuencia, la seguridad se agrega al final de la migración a cloud-first y esto puede demorar los resultados para el negocio, o incluso tener que rehacer todo el trabajo.

La nube precisa diferentes herramientas y habilidades que las instalaciones on-premise. Se debe tratar como el resto del ciclo de desarrollo de software. Se deben realizar cambios de la misma manera que en cualquier aplicación: haciendo el check in y check out del código.

Si no logramos "mover la seguridad a la izquierda", generaremos mala alineación y gobierno, procesos manuales, herramientas legacy y brechas que alentarán a los ejecutivos a considerar la seguridad como la función que frena al negocio.

> **En realidad, en la carrera hacia la nube, los líderes de seguridad son los mayores campeones.**

"Necesitamos una sola lámina de vidrio para ver nuestras vulnerabilidades, pero ahora muchas empresas con instancias multi-cloud están mirando a través de un mosaico."

Kris Burkhardt
Accenture CISO

Una nube segura puede facilitar mejores resultados de negocios

La seguridad de la nube puede facilitar mejores resultados de negocios, al ser:

Rápida

Usar aceleradores nativos de los proveedores de servicios cloud que faciliten la implementación de capacidades y controles de seguridad en cuestión de minutos u horas, en lugar de meses.

Sin fricción

Incorporar la seguridad a las soluciones, procesos de negocios y equipos operativos.

Escalable

Aplicar la automatización y los procesos de auto reparación para reducir los pasos manuales y derribar el modelo tradicional de incorporación de recursos a la dotación para permitir que las organizaciones escalen.

Proactiva

Establecer controles preventivos para bloquear la aparición de incidentes de seguridad accidentales o maliciosos.

Económica

Seguridad incorporada desde el inicio para evitar los costos adicionales incurridos al tener que rehacer el trabajo.

Caso de estudio: Accenture

El 95% de las aplicaciones de Accenture ya está en la nube respaldadas por la economía de la plataforma. Comparadas con las soluciones tradicionales de seguridad que dependían demasiado de los proveedores, las nuevas soluciones de seguridad nativas de cloud que ofrece Accenture permiten lograr:

- Una estrategia de equipos y fuerzas de trabajo para optimizar el actual modelo operativo onshore-offshore
- Trabajar de manera inteligente aplicando Infrastructure as Code reduce el traslado de los empleados a las instalaciones de los clientes y la duración de las implementaciones.
- Formas digitales de trabajar para generar **colaboración, innovación, flexibilidad y el propósito de generar valor**
- Reducción del gasto relacionado con la obtención de talento, mediante una mejor atracción y retención

70%
Reducción de costos de desarrollo

30-70%
Ahorros en comparación con soluciones SIEM as-a-Service

3x
Mayor velocidad de desarrollar y poner en producción operaciones versus las herramientas de seguridad legadas

20-40%
Reducción en los costos de ejecución de operaciones, comparado con el enfoque legado

50%
de reducción del tiempo promedio para la puesta en producción de las operaciones

1 Día
Tiempo que se demora para comenzar la incorporación y obtener valor para el cliente

Además de nuestra experiencia para emprender una transformación cloud-first hemos anunciado una inversión de US$3.000 millones para ayudar a nuestros clientes a forjar, migrar, construir y operar sus empresas en la nube, así como obtener los beneficios relacionados con el valor para el negocio, la velocidad, el costo, el talento y la innovación.[5]

Empoderar al CISO

Considera el progreso de tu transformación hacia una nube segura, preguntándote:

• ¿A dónde deberíamos enfocar nuestras inversiones en la nube pública? (considerar factores tales como: cloud native, identidad, gobierno de datos, seguridad de las redes, etc.)

• ¿Cómo afectó el COVID-19 nuestras prioridades y objetivos con respecto al eCommerce y nuestra presencia online y qué impacto tuvo en la demanda de escalar en la nube?

• ¿Queremos migrar a un modelo “lift and shift” o modernizar/refactorizar a arquitecturas de aplicaciones modernas, como los microservicios, al mismo tiempo?

Lo positivo de cloud

En nuestra experiencia, los cuatro pasos siguientes pueden guiar cualquier migración a cloud-first e introducir seguridad, con velocidad y escala, desde el principio.

Conocer tu postura frente a la seguridad en la nube

Identificar brechas rápidamente y establecer una arquitectura alineada con los riesgos y una hoja de ruta para determinar las bases de la seguridad en cloud que optimicen las actuales inversiones en tecnología.

Automatizar la seguridad nativa

Mejorar el "time to value" y automatizar la implementación de barreras de seguridad con aceleradores prediseñados para servicios cloud native, que incluyan: AWS, Microsoft Azure y Google Cloud.

Ser proactivo con el cumplimiento

Optimizar la detección y agilizar las operaciones de seguridad de la nube. Mitigar el riesgo con funciones de auto reparación ejecutadas en forma nativa dentro de los proveedores de servicios cloud (CSPs) o mediante servicios de terceros para hacer cumplir las políticas, en alineación con los requisitos regulatorios y los estándares aplicables a nivel empresa.

Utilizar el monitoreo y las respuestas de seguridad

Monitorear de manera efectiva y a escala el costo de los activos en la nube usando herramientas de seguridad nativas y una biblioteca de casos de uso que se actualicen continuamente para abordar las amenazas en constante evolución y los requisitos regulatorios complejos.

Contactos

Daniel W. Mellen
Managing Director,
Accenture Security Cloud

Rex Thexton
Senior Managing Director,
Applied Cybersecurity Services

Harpreet Sidhu
Managing Director,
Managed Security Services

Andrew Winkelmann
Managing Director,
Accenture Security

Referencias

1 Navigating the barriers to maximizing cloud value, Accenture, 2020; https://www.accenture.com/us-en/insights/technology/maximize-cloud-value

2 Perspectives on cloud outcomes: Expectation vs reality, Accenture, 2020; https://www.accenture.com/us-en/insights/cloud/cloud-outcomes-perspective

3 Mitigating Cloud Vulnerabilities, National Security Agency, January 2020; https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

4 Innovate for Cyber Resilience, Accenture, 2020; https://www.accenture.com/gb-en/insights/security/invest-cyber-resilience

5 Accenture Cloud First Launches with $3 Billion Investment to Accelerate Clients' Move to Cloud and Digital Transformation, Accenture, 2020; https://newsroom.accenture.com/news/accenture-cloud-first-launches-with-3-billion-investment-to-accelerate-clients-move-to-cloud-and-digital-transformation.htm

Acerca de Accenture

Accenture es una compañía global de servicios profesionales que proporciona capacidades líderes en soluciones digitales, de seguridad y cloud. Combinando nuestra experiencia inigualable y conocimientos especializados en más de 40 industrias, ofrecemos servicios de Estrategia y Consultoría, Interactive, Tecnología y Operaciones, impulsados por la red de centros de Advanced Technology e Intelligent Operations más grande el mundo. Nuestros 506.000 empleados cumplen la promesa de desarrollar la tecnología y el ingenio humano cada día, ofreciendo servicios a clientes en más de 120 países. Adoptamos el poder del cambio para crear valor y éxito compartido para nuestros clientes, personas, accionistas, socios y comunidades. Visitanos en **www.accenture.com**

Acerca de Accenture Security

Accenture Security es proveedor líder de servicios completos de ciberseguridad que incluyen ciber defensa avanzada, soluciones de ciberseguridad aplicada y operaciones gestionadas de seguridad. Aportamos innovación en seguridad, con escala global y una capacidad de servicios a nivel mundial a través de nuestra red de centros de Advanced Technology e Intelligent Operations. Con el respaldo de nuestro equipo de profesionales altamente calificados, ayudamos a los clientes a innovar en forma segura, desarrollar ciber resiliencia y crecer con confianza. Seguinos como **@AccentureSecure** en Twitter o visitanos en **www.accenture.com/security**

Copyright © 2021 Accenture.
Todos los derechos reservados.

Accenture y su logo son marcas registradas de Accenture.

El propósito de este documento es servir como información general solamente, no tomando en cuenta las circunstancias específicas del lector y pudiendo no reflejar los acontecimientos más actuales. Accenture no asume responsabilidad alguna, con el mayor alcance permitido por la legislación aplicable, por la precisión e integridad de la información vertida en el presente ni por ningún acto u omisión basado en dicha información. Accenture no proporciona asesoramiento legal, regulatorio, de auditoria o impositivo. Los lectores son responsables de obtener dicho asesoramiento de parte de sus propios asesores legales u otros profesionales autorizados.