EDICIÓN EUROPEA

THALES
Building a future we can all trust

RESUMEN EJECUTIVO

Estudio de Thales sobre seguridad en la nube de 2021

Desafíos a los que se enfrenta la protección de datos en la nube y la gestión de acceso en un ambiente híbrido y multinube

#SeguridadNube2021

cpl.thalesgroup.com

Acerca de este estudio

Aunque la pandemia provocó muchos cambios empresariales durante el año pasado, ya se observaba el aumento del uso de infraestructura en la nube. El aumento de la demanda de teletrabajo y la adopción digital en aumento solo lo incrementaron. El estudio de Thales sobre seguridad en la nube de 2021, basado en datos de una encuesta a más de 2600 encuestados en más de 10 países de todo el mundo, busca identificar la profundidad de ese cambio, así como el estado actual y los planes de las organizaciones en un una amplia gama de industrias a la hora de gestionar el acceso a las aplicaciones empresariales, los servicios en la nube y las redes. Este resumen ejecutivo analiza el segmento europeo de los resultados, comparándolo y contrastándolo con una perspectiva global. (El estudio incluye Reino Unido en los resultados europeos para la continuidad geográfica junto con Francia, Alemania, los Países Bajos y Suecia.) Las conclusiones recogidas en este informe se han obtenido de los datos de la encuesta y exploran el impacto en la estrategia y planificación de seguridad.

Los resultados del estudio muestran que no hay muchos controles de seguridad en uso en cuanto a un nuevo elemento en la infraestructura, incluso con el creciente aumento del éxodo a la nube. Las empresas encuestadas mostraron niveles significativos de brechas de datos, unos niveles bastante más altos en Europa en comparación con la media global. Estas empresas pueden aprovechar la oportunidad para acelerar la adopción de la nube mediante el refuerzo de su seguridad, con tácticas como el mayor cifrado y así permitir su uso con una mayor gama de cargas de trabajo.

451 Research

S&P Global
Market Intelligence

Fuente: encuesta personalizada de 2021 sobre seguridad en la nube de 451 Research, parte de S&P Global Market Intelligence, encargada por Thales

Nuestros patrocinadores son:

Introducción

"Las empresas deben ampliar y adaptar sus competencias para poder gestionar su seguridad con eficiencia y efectividad en los nuevos entornos dispersos".

Conclusiones principales

- Los requisitos de privacidad de datos y de gobernanza más robustos en Europa generan una mayor necesidad de una gestión de datos efectiva y eficiente, pero muchas empresas no disponen de esta capacidad.
- Las empresas europeas indicaron un mayor uso de consolas en la nube para sus gestiones principales, una práctica de mayor riesgo.
- Los encuestados un poco menos empáticos a la hora de reconocer la complejidad de la gestión en la nube en comparación con la media global.
- Existe un mayor enfoque en la importancia de la autenticación de múltiples factores (MFA) para la protección de datos en la nube.
- Aunque se constata un uso limitado del cifrado de datos sensibles en la nube, los encuestados europeos mostraron de un mayor uso del cifrado propio (BYO).
- Los europeos mostraron un nivel ligeramente mayor de brechas de datos relacionadas con la nube.

La adopción en masa de la multinube

A medida que las empresas se enfrentaron a los desafíos que provocó la pandemia durante el año pasado, estas se enfocaron en la infraestructura para darles escala y alcance. Las funciones que brinda la nube acercan las aplicaciones a los empleados y a su clientela más rápidamente que otras opciones. Sin embargo, este cambio puede comportar otros desafíos intrínsecos, ya que se trata de una nueva forma de operar, y las empresas podrían no entender totalmente sus características, desviando los procesos de los modelos en sus instalaciones. Estas empresas deben ampliar y adaptar sus competencias para poder gestionar su seguridad con eficiencia y efectividad en estos nuevos entornos dispersos, aunque los resultados del estudio muestran que puede ser complicado.

Pocas empresas colaboran con un único proveedor de servicios en la nube para contar con infraestructura como servicio (IaaS), plataforma como servicio (PaaS) o software como servicio (SaaS), y el uso de varios proveedores puede dificultar las operaciones, ya que cada uno cuenta con funciones y controles distintos. Aunque la media europea ronda en torno a la global, hay ciertos modelos atípicos que muestran la falta de homogeneidad general del club. En cuanto a proveedores de PaaS, un 73 % de encuestados europeos indicó que contaba con dos o más, en línea con las cifras mundiales. Sin embargo, esta cifra es mayor en proveedores de SaaS: aunque la mayoría (38 %) indica que cuenta con 26-50 de media, Países Bajos se encuentra por debajo (43 de media) y Suecia muy por encima (78). El número de aplicaciones de SaaS aumenta junto con la complejidad de la organización en cuanto a ingresos.

La complejidad de la nube como problema habitual

La diversidad de ambientes también podría contribuir a la complejidad operativa. Casi la mitad de encuestados europeos (un 45 %, casi la media global del 46 %) está de acuerdo o muy de acuerdo en que es más complicado gestionar la normativa en materia de privacidad y protección de datos en un entorno de nube que en las redes de la empresa. Cada país mostró individualmente un mayor nivel de preocupación, el Reino Unido con un 55 % y Países Bajos con un 56 %. Estos datos deben instar a las empresas a buscar métodos para simplificar sus operaciones con funciones de gestión de seguridad que abarquen todos sus entornos operacionales y unifiquen sus procesos generales.

FIGURA 1

Gestionar la seguridad en la nube es complejo

En qué medida está de acuerdo con la siguiente afirmación: es más complicado gestionar la normativa en materia de privacidad y protección de datos en un entorno de nube que en las redes de mi empresa.

- **19 %** Totalmente de acuerdo
- **26 %** De acuerdo
- **19 %** En desacuerdo
- **19 %** Totalmente en desacuerdo
- **16 %** No sabe

Fuente: encuesta personalizada sobre seguridad en la nube de 2021 de 451 Research

Definir las políticas de seguridad en la nube: un aspecto esencial para los equipos de seguridad

Las empresas deben contar con políticas que definan y pongan en marcha políticas de seguridad para acabar con la complejidad de los entornos que deben gestionar. El estudio observa los procesos de toma de decisiones, y un 84 % de los encuestados indica que sus equipos de seguridad estaban involucrados en las decisiones de seguridad en la nube. De estos, casi la mitad mostró que sus equipos de seguridad gestionaban la seguridad en la nube de manera independiente, y la otra mitad afirmó que su equipo colaboraba con equipos de ingeniería de la nube. Sin embargo, existe cierta discrepancia en la percepción de funciones: los altos cargos creen que los equipos de seguridad tienen una gran responsabilidad, y el personal general piensa que existe un mayor nivel de colaboración. Esta discrepancia también se observa en varios cargos jerárquicos en el proceso de compra.

84%

de los encuestados indicó que sus equipos de seguridad estaban implicados en las decisiones de seguridad en la nube

Migrar a la nube: esencialmente «Lift & Shift»

Existen muchos caminos que nos llevan a la nube. El estudio ha comprobado de qué manera las empresas esperan cambiar a entornos en la nube. Un poco más de la mitad (53 %) indicó que espera poder migrar sus cargas de trabajo existentes a la nube con cambios mínimos, lo que se conoce como «Lift & Shift». Este método generalmente es rápido con cargas de trabajo que pueden migrarse con facilidad, pero puede abrir brechas en la seguridad si no se planifica con cuidado y quizá no es la forma más eficiente de usar recursos en la nube. Tan solo el 22 % de los encuestados espera realizar algún tipo de reestructuración de sus aplicaciones. Este método puede hacer que las funciones nativas de la nube actúen más directamente, pero puede generar un mayor uso de recursos en su implementación. Para proteger las cargas de trabajo migradas a la nube, las empresas deben garantizar que disponen de los controles existentes en sus instalaciones en el nuevo entorno y que pueden realizar sus operaciones de manera efectiva y eficiente.

Tecnologías clave como método de protección de ambientes en la nube

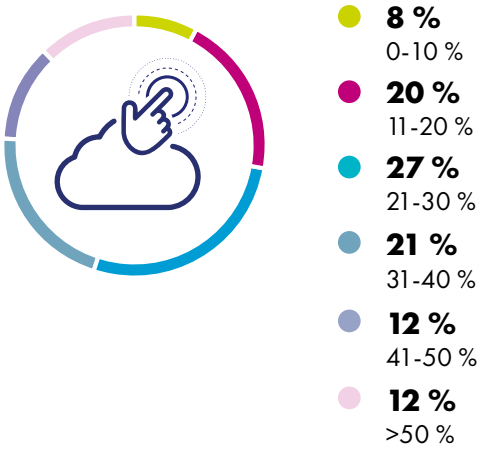
Proteger las aplicaciones y los datos en la nube exige disponer de una nueva gama de competencias y, seguramente, nuevas tecnologías. El estudio solicitó a los encuestados que enumerasen las tecnologías que utilizan para proteger sus datos en entornos en la nube: el 63 % de los encuestados europeos indicó que utilizaba cifrado, seguido de la gestión de claves en un 56 % y MFA en un 53%. Sin embargo, este porcentaje de uso de varias tecnologías fue diferente entre países. Suecia mostró que dispone del mayor nivel de uso de cifrado (67 %) y el menor uso de gestión de claves (45 %). Países Bajos mostró un uso elevado consistente de las tres tecnologías (cifrado en un 62 %, gestión de claves en un 65 % y MFA en un 57 %). Esta variación destaca la complejidad de la gestión de la seguridad en la nube, siendo necesario ejecutar estas tres tecnologías para poder salvaguardar la nube. Estas deben usarse para establecer una base segura para cualquier operación en la nube.

El estudio comprobó la gestión de acceso a las aplicaciones en la nube, y descubrió que las empresas utilizan tecnología moderna de autenticación, como la MFA, de una manera puntual y no consistente. Tan solo el 16 % de encuestados europeos (en consonancia con la media global) protege más del 50 % de sus operaciones en la nube con una tecnología moderna de autenticación, lo cual no protege del riesgo de ataques que han crecido de manera exponencial. Es un ámbito claro en el que invertir más recursos.

FIGURA 2

Aplicaciones en la nube protegidas por MFA

¿Qué porcentaje de la plantilla utiliza MFA en aplicaciones en la nube/SaaS?



Fuente: encuesta personalizada sobre seguridad en la nube de 2021 de 451 Research

Las reflexiones regionales sobre gestión de acceso parecen coincidir entre encuestados europeos y de otras partes del mundo. Tan solo un 16 % de encuestados indica utilizar MFA para proteger más de la mitad de sus aplicaciones en la nube, comparable al 16 % de europeos que responde de la misma manera. Ocurre lo mismo respecto el acceso con MFA a más de la mitad de aplicaciones en sus instalaciones: 11 % en el mundo, 12 % en Europa.

Respecto a la complejidad de proteger los servicios tanto en sus instalaciones como en la nube con sus capacidades de gestión de acceso, un 67 % de europeos (en comparación con el 66 % en el resto del mundo) indicó que era «complicado» o «muy complicado».

La necesidad de normalizar el cifrado en la nube

La protección de datos es otro ámbito en el que se invierte bastante menos. Los encuestados indicaron que el cifrado es importante para la protección de datos, pero sus respuestas denotan una ejecución limitada: tan solo el 17 % de los encuestados europeos indica que cifra más del 50 % de sus datos sensibles en entornos en la nube. Aunque está en consonancia con la media global, estas empresas se exponen a un riesgo considerable. No se trata de un uso limitado de la nube: casi un cuarto (24 %) de encuestados europeos indicó que opera más del 50 % de su carga de trabajo mediante un proveedor de nube externo, y que el 22 % de los datos en la nube es de carácter sensible.

El otro aspecto de la efectividad de la protección de datos en la nube es la gestión de claves. Como promedio, los encuestados europeos coincidieron bastante con la media mundial en cuanto al control de sus claves (un 36 % indicó que controla la mayoría o todas las claves), pero confía más en consolas de proveedores de nube para este control (un 57 % contra un 52 %). Las empresas que no controlan sus propias claves no solo se enfrentan al riesgo de que sus datos se vean expuestos, sino que añaden complejidad en la gestión de sus claves, ya que deben coordinar sus actividades en diversos entornos para los sistemas de gestión de claves tanto en sus instalaciones como fuera de ellas. Esta situación es tan intensiva en recursos como propensa a errores operativos. Invertir en un sistema de gestión de claves que abarque la infraestructura completa de una empresa puede reducir las cargas de trabajo del personal y mejorar el estado de su seguridad.

Solo el

17 %

de encuestados europeos indica que cifra más del 50 % de sus datos sensibles en entornos en la nube.

El **63 %**

de encuestados europeos indicó que el cifrado era la tecnología utilizada para proteger sus datos en la nube

> **"Las empresas que no controlan sus propias claves no solo se enfrentan al riesgo de que sus datos se vean expuestos, sino que también añaden complejidad en la gestión de sus claves, ya que deben coordinar sus actividades en diversos entornos para los sistemas de gestión de claves tanto en sus instalaciones como fuera de ellas".**

Un recorrido hacia el «Zero Trust»

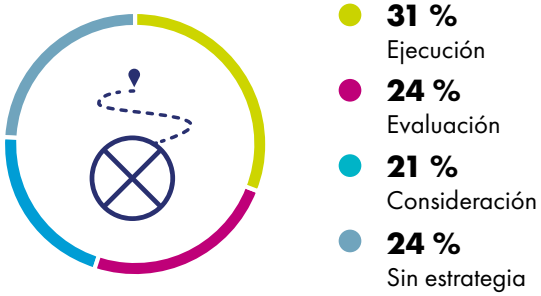
Una de las tendencias que observa el estudio es el mayor uso de principios operativos Zero Trust. Las empresas quieren mejorar su seguridad limitando el acceso y utilizando controles más granulares y basados en políticas, aspectos que ofrece la mentalidad operativa Zero Trust, un enfoque especialmente efectivo para proteger el modelo distribuido que conlleva utilizar la nube. Los encuestados informaron que acaban de empezar su recorrido hacia un plan Zero Trust, y menos de un tercio indica que lo han ejecutado.

La buena noticia es que el estudio afirma que una gran mayoría (76 %) cree que los principios del Zero Trust dan forma a su estrategia de seguridad en la nube. Es un buen indicio de que se reconoce la importancia de poder aplicar controles más granulares, y reitera la necesidad de invertir en las tecnologías necesarias para ejecutar el Zero Trust. Este exige una base de seguridad sólida que incluya una protección de datos y una gestión de acceso gestionadas con efectividad. El estudio muestra que las empresas deben invertir en métodos de autenticación modernos, como MFA y sistemas de gestión de claves, para disfrutar de la protección total del cifrado de datos.

FIGURA 3

Recorrido hacia el «Zero Trust»

¿En qué punto está en su proceso Zero Trust?

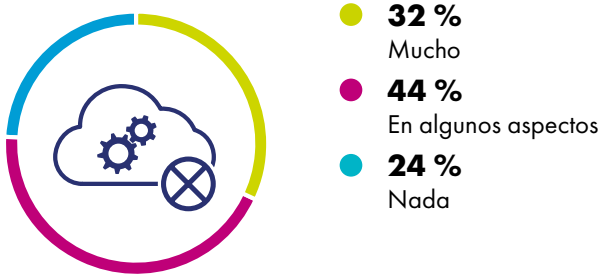


Fuente: encuesta personalizada sobre seguridad en la nube de 2021 de 451 Research

FIGURA 4

Zero Trust en la estrategia de la nube

¿En qué medida incide la seguridad que ofrece el Zero Trust en su estrategia de seguridad en la nube?



Fuente: encuesta personalizada sobre seguridad en la nube de 2021 de 451 Research

"Las empresas quieren mejorar su seguridad limitando el acceso y utilizando controles más granulares y basados en políticas, aspectos que ofrece la mentalidad operativa Zero Trust".

El **43 %**

de los encuestados europeos indica que su empresa ha tenido que lidiar con una brecha en su entorno en la nube

"Muchos altos cargos implicados en la toma de decisiones podrían ignorar la realidad de su entorno y no entender la urgencia de hacer cierta inversión".

Brechas y problemas de auditorías

La prueba definitiva de la efectividad en la seguridad es el número de ataques que una empresa no ha podido evitar. El estudio observó las brechas, y un 43 % de los encuestados europeos indica que su empresa ha tenido que lidiar con una brecha en sus entornos en la nube. Este número supera a la media mundial del 40 %. Los Países Bajos muestra una cifra aún mayor: el 52 % sus encuestados indicó que sufrió una brecha. Los encuestados suecos coinciden con el segundo mayor nivel en Europa: un 49 %. El estudio comparó los números con la actividad reciente, y un 46 % de encuestados europeos indicó que había sufrido una brecha o un problema en una auditoría en sus entornos en la nube durante los últimos 12 meses (un 52 % en Reino Unido y un 49 % en Suecia).

El estudio observó las diferencias que detectaban distintos cargos en las empresas en cuanto a brechas. Cuanto más alto el cargo en la gerencia, menor era el nivel de importancia que se le daba a las brechas. En otras palabras, había un número menor de altos cargos que informaba sobre si su empresa debía lidiar con una brecha que gerentes sénior, y sus números eran menores que los de la plantilla general. Esto significa que muchos altos cargos implicados en la toma de decisiones podrían ignorar la realidad de su entorno y no entender la urgencia con la que se debe invertir. Probablemente, esta situación dificulte las mejoras necesarias para fortalecer el estado de seguridad.

Avanzar

Las empresas trabajan duro para gestionar los cambios forzados por la pandemia, progresando con inversiones tecnológicas que les garantice un nivel de competitividad. Dominar la seguridad y las operaciones en una infraestructura en la nube es un aspecto indispensable de este recorrido. Los resultados del estudio mostraron que se observa un uso considerable de patrones híbridos y multinube a medida que las empresas se expanden para acercarse a sus clientes y socios, así como para dar soporte a una plantilla más distribuida. Los resultados también indicaron que aún queda mucho por hacer para proteger esta nueva infraestructura con efectividad y ejecutarla de manera eficiente. El creciente uso de recursos híbridos y distribuidos aumenta la complejidad operacional, y las empresas deben invertir en funciones que les permitan escalar sin que afecte críticamente a sus equipos de seguridad.

THALES

Building a future we can all trust

Contacto

Para consultar la dirección de las oficinas y nuestros datos de contacto, visite cpl.thalesgroup.com/es/contact-us

cpl.thalesgroup.com/cloud-security-research