thalesgroup.com

THALES

Protegemos los datos en la nube
Estudio de Thales sobre seguridad en la nube de 2019

Resumen

#CloudSecurity

Ponemon INSTITUTE

Acerca de Ponemon Institute

En Ponemon Institute nos dedicamos a llevar a cabo estudios independientes y una labor educativa para promover prácticas responsables de gestión de la información y la privacidad en empresas y administraciones estatales. Nuestra misión consiste en realizar estudios empíricos de gran calidad sobre asuntos críticos que afectan a la gestión y la seguridad de aquella información sobre personas y organizaciones que tiene una naturaleza delicada.

Implantamos normas en materia de confidencialidad, privacidad y ética en el estudio de datos. No recogemos ninguna información que permita identificar a particulares (ni a empresas, en el caso de nuestros estudios empresariales). Además, cumplimos estrictas normas de calidad para no plantear a los interesados preguntas impertinentes, irrelevantes o inadecuadas.

Acerca de Thales

Las personas a las que confía la protección de su privacidad confían en Thales para proteger sus datos. Las empresas se enfrentan a una cantidad cada vez mayor de momentos decisivos relacionados con la seguridad de los datos. Tanto si se trata de elaborar una estrategia de cifrado, como de facilitar un acceso de confianza a la nube o cumplir los requisitos normativos, puede confiar en Thales para proteger su proceso de transformación digital.

Tecnología decisiva para momentos decisivos.

Introducción

Redactada por el Dr. Larry Ponemon, presidente y fundador de Ponemon Institute

Ponemon Institute se complace en presentar las conclusiones del Estudio global sobre seguridad en la nube de 2019 patrocinado por Thales. La finalidad de este estudio es comprender la evolución de las tendencias en materia de gobernanza en la nube y prácticas de seguridad desde su primera edición, publicada en 2015.

La edición de este año revela un aumento del riesgo de no cumplimiento de los nuevos reglamentos globales en materia de privacidad y protección de datos. Otra tendencia importante durante los últimos tres años ha sido el aumento del uso de aplicaciones y plataformas en la nube sin las necesarias salvaguardas de seguridad.

Hemos encuestado a un total de 3346 personas, entre profesionales de TI y de seguridad en TI, en Estados Unidos, el Reino Unido, Australia, Alemania, Francia, Japón, la India y Brasil. Se trata de personas que están al corriente del uso que hacen sus empresas de los recursos de nube pública y privada y participan en dicho uso. El 76% de los encuestados afirma que su organización es usuaria intensiva (34%) o moderada (42%) de recursos en la nube.

Cada vez hay un mayor compromiso con la seguridad en la nube, pero las salvaguardas de seguridad se van quedando rezagadas respecto al aumento del uso de las diversas plataformas en la nube. Como ilustra la figura 1, el compromiso de proteger la información confidencial o delicada ha aumentado considerablemente, desde el 62% de los encuestados que lo asumían en 2015 hasta el 72% de la edición de este año. No obstante, solo la mitad de los encuestados (50%) afirma que su organización ha establecido funciones y mecanismos de rendición de cuentas claramente definidos para la protección de información confidencial o delicada almacenada en la nube.

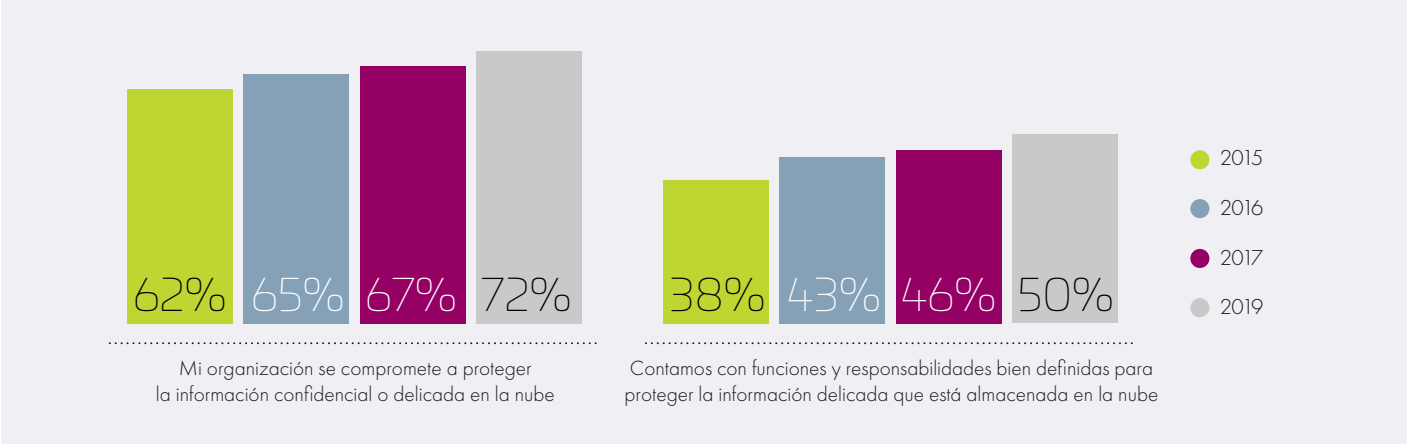


Figura 1
Compromiso con la protección de datos en la nube
Combinación de las respuestas "Totalmente de acuerdo" y "De acuerdo"

Principales conclusiones

Las organizaciones no logran proteger los datos de naturaleza delicada, a pesar de que su almacenamiento en la nube está cada vez más extendido

Las nuevas investigaciones de Thales y Ponemon Institute han sacado a la luz un contraste entre el rápido auge del almacenamiento de datos en la nube y la estrategia de protección de información delicada que aplican las organizaciones.

- Indudablemente, las empresas están aprovechando el aumento de opciones disponibles en la nube, pero al mismo tiempo no se dejan guiar por sus propias inquietudes en cuanto al riesgo que estas entrañan y no están aplicando las medidas de seguridad adecuadas.
- Tras haber endosado claramente la responsabilidad de proteger sus datos a los proveedores de servicios en la nube, resulta extremadamente preocupante comprobar que la seguridad no constituye un factor de peso a la hora de escoger entre ellos.
- Independientemente del modelo o proveedor de servicios en la nube que escoja, el responsable de la seguridad de los datos de su organización en la nube es usted.
- Cuando se produce una violación de la seguridad de los datos, la reputación de las empresas se ve perjudicada, así que estas deberían asumir un mayor control de la seguridad y también la propiedad de sus claves de cifrado.

A la luz del estudio, a las organizaciones les cuesta asumir una postura de seguridad más firme en la nube debido a su incapacidad de hacer lo siguiente:

- Aplicar prácticas de seguridad tradicionales en el entorno de la nube
- Evaluar directamente el cumplimiento y las prácticas de seguridad de los proveedores de servicios en la nube
- Contar con suficientes recursos que les permitan evaluar las prácticas de seguridad de los proveedores de servicios en la nube
- Controlar o limitar el acceso de los usuarios finales
- Conocer todas las aplicaciones y servicios de plataforma o infraestructura informática en la nube que se utilizan
- Reducir la complejidad de gestión de los reglamentos de privacidad y protección de datos en el entorno de la nube

Las empresas están aprovechando la nube, pero sin aplicar las medidas de seguridad adecuadas

el **48%**

del total de los datos corporativos se almacena en la nube, en comparación con el 35 % de hace tres años

el **49%**

de las organizaciones cifra los datos delicados en la nube

Las empresas conservan la responsabilidad sobre la seguridad de sus datos en la nube independientemente del proveedor

el **53%** de las empresas ostentan el control de las claves cuando los datos están cifrados en la nube,

a pesar de que

el **78%** afirma que es importante conservar la propiedad de las claves de cifrado

Algunas empresas endosan la responsabilidad de mantener la seguridad de los datos a los proveedores de servicios en la nube, pero no consideran que la seguridad constituya un factor de peso a la hora de escoger entre ellos

el **30%**

de las organizaciones cuentan con un sistema unificado de acceso seguro a aplicaciones en la nube e in situ

el **32%**

no emplea un enfoque de primacía de la seguridad a la hora de almacenar datos en la nube

Las empresas utilizan de media 29 cloud aplicaciones en la nube, en comparación con las 27 que utilizaban hace dos años

terminada **10%** cuenta con más de 50 y la más del empresa media en EE. UU. cuenta con 41

A las empresas les cuesta reducir la complejidad de gestión de los reglamentos de privacidad y protección de datos en el entorno de la nube

el **46%**

ha revelado que almacenar datos de los clientes en la nube entraña un mayor riesgo para la seguridad, así como de incumplimiento normativo (56 %)

el **44%**

de las organizaciones tienen cuidado a la hora de compartir información delicada con terceros

Información sobre clientes 60%, correos electrónicos 48% y datos sobre consumidores 46% representan la mayor cantidad de datos almacenados en la nube

La nube es un valioso componente de la estrategia de TI de las organizaciones

La nube reduce los costes y el tiempo de implantación, y aumenta la eficiencia de las organizaciones.

El principal incentivo para utilizar la nube es la reducción de costes. No obstante, como muestra la edición del estudio de este año, la mejora de la eficiencia y de la seguridad ha aumentado su importancia durante los últimos tres años como motivo para trasladar recursos a la nube.

Prácticamente todas las organizaciones representadas en este estudio utilizarán servicios en la nube durante los próximos dos años.

Según el 80% de los encuestados, las aplicaciones y soluciones de plataforma informática en la nube se consideran esenciales para las operaciones de una organización en la actualidad, mientras que un 90% de los mismos afirma que la importancia de la nube aumentará durante los próximos dos años.

Las organizaciones no están avanzando en el conocimiento de todos los servicios de cloud computing que utilizan.

Más de la mitad (54%) de los encuestados están muy seguros (24%) o seguros (30%) de que su departamento de TI conoce todas las aplicaciones, servicios o infraestructura de cloud computing que se utilizan en la actualidad.

El software como servicio (SaaS) ya se utiliza en casi todas las organizaciones.

Desde 2016, el porcentaje de los encuestados que indica que su organización no utiliza SaaS[1] ha disminuido del 54% al 9% de la edición de este año.

De media, las organizaciones participantes en este estudio utilizan 29 aplicaciones en la nube. Las aplicaciones empresariales, incluidas aplicaciones de infraestructura en la nube como copias de seguridad en línea, escritorio virtual, mensajes de texto a correo electrónico y otras herramientas de comunicación, han aumentado considerablemente desde 2016. El valor del uso del correo electrónico, los mensajes de texto y otras herramientas de comunicación también ha aumentado para las organizaciones.

el 91%

de las organizaciones encuestadas utilizan SaaS

29

número de aplicaciones en la nube que utilizan de media las organizaciones

[1] SaaS es un sistema de software por el que un proveedor concede a sus clientes licencias de uso de una aplicación a modo de servicio a la carta. Los proveedores de SaaS pueden alojar la aplicación en sus propios servidores web o instalarla en el dispositivo del consumidor para luego desactivarla después del uso o cuando expira el contrato de uso a la carta.

Aumenta el uso de la plataforma como servicio (PaaS).

Desde 2016, el porcentaje de los encuestados que utiliza PaaS[2] ha aumentado. El porcentaje de los encuestados que indica que su organización no utiliza PaaS ha disminuido del 54% al 44%. El uso de servicios como los de gestión de identidad, pagos y búsquedas ha aumentado del 24% al 32% durante los últimos tres años.

el 56%

de los encuestados afirman que sus organizaciones utilizan PaaS

Hay más empresas que utilizan la infraestructura como servicio (IaaS).

Las organizaciones representadas en este estudio utilizan de media 13 servicios de proveedor/infraestructura de cloud computing. El porcentaje de los encuestados que afirma no utilizar IaaS[3] ha caído del 41% en 2016 al 28% en 2019. El uso de servicios de almacenamiento e informática viene aumentando constantemente desde 2016.

el 28%

de los encuestados afirman que sus organizaciones no utilizan PaaS

Casi la mitad (48%) de las organizaciones representadas en este estudio utiliza una arquitectura o estrategia multi-cloud[4] , que se traduce en un promedio de uso de 3 nubes distintas. Dentro del 50% de los encuestados que no utiliza múltiples nubes, un 60% afirma que va a implantar una arquitectura multi-cloud durante los próximos 6 meses (37%) o 12 meses (23%).

el 48%

de las organizaciones utilizan una arquitectura o estrategia multi-cloud

13

número de servicios de proveedor/ infraestructura de cloud computing utilizados de media

[2] PaaS consiste en proporcionar una plataforma informática y paquete de soluciones a modo de servicio. Suele ampliarse mediante el suministro de una plataforma de desarrollo de software diseñada para el entorno de informática en la nube.

[3] IaaS consiste en proporcionar una infraestructura informática a modo de servicio. En lugar de comprar servidores, software, espacio en centros de datos o equipos de redes, los clientes obtienen los mismos recursos a través de un servicio totalmente subcontratado. Este servicio se suele facturar según un modelo de consumo informático, y la cantidad de recursos consumidos (y, por ende, el coste) normalmente refleja el nivel de actividad.

[4] Multi-cloud se refiere al uso de múltiples servicios de informática y almacenamiento en la nube dentro de una sola arquitectura heterogénea. También se refiere a la distribución de recursos, software, aplicaciones, etc., entre varios entornos de alojamiento en la nube. Al hacer uso de dos o más nubes públicas, así como varias nubes privadas, la arquitectura multi-cloud típica ofrece un entorno con el que se busca eliminar la dependencia de un solo proveedor de servicios en la nube. Se diferencia de la nube híbrida en cuanto a que hace referencia a múltiples servicios en la nube, en lugar de múltiples modos de implantación (pública, privada, heredada).

Disminuye el control del gasto en seguridad de TI por parte de los departamentos de TI.

El porcentaje medio del gasto corporativo total en TI controlado por el departamento de TI ha disminuido al 36% desde el 40% registrado en la edición del estudio del año pasado, como ilustra la figura 2.

Según se puede comprobar en la figura 3, el porcentaje de los servicios en la nube implantado por departamentos ajenos al de TI corporativa es inferior al promedio del 58% registrado en la edición del estudio del año pasado.

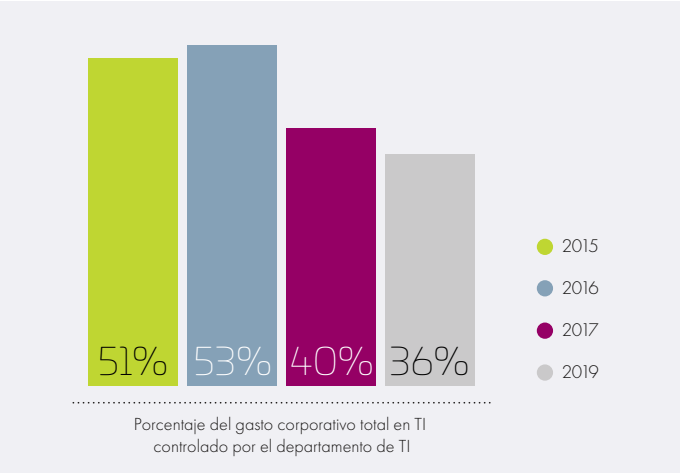


Figura 2
Porcentaje del gasto corporativo total en TI controlado por el departamento de TI
Valores extrapolados

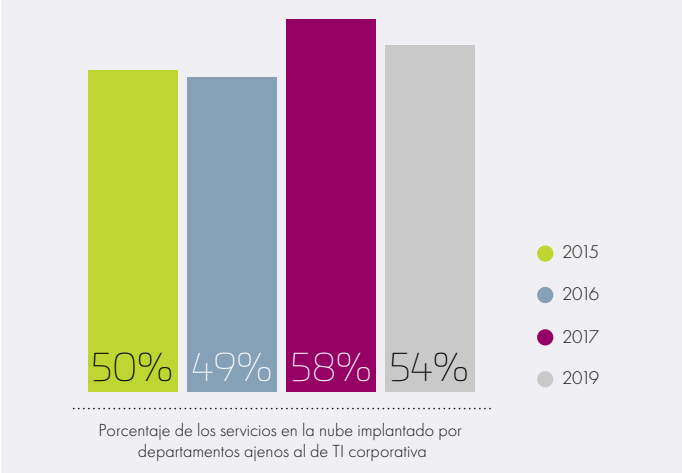


Figura 3
Porcentaje de los servicios en la nube implantado por departamentos ajenos al de TI corporativa
Valores extrapolados

Se están almacenando más datos corporativos en la nube.

Como ilustra la figura 4, el porcentaje de los datos corporativos que se almacena en el entorno de nube ha aumentado desde un promedio del 30% en 2015 hasta el promedio actual del 48%.

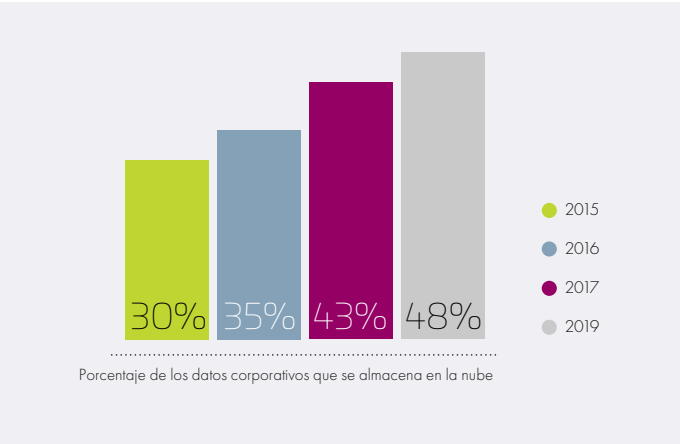


Figura 4
Porcentaje de los datos corporativos que se almacena en la nube
Valores extrapolados

Las prácticas de seguridad en la nube siguen siendo conflictivas e irregulares

Se están almacenando más datos corporativos en la nube y el uso de plataformas y aplicaciones en la nube se ha generalizado en las organizaciones.

Sin embargo, la figura 5 ilustra los obstáculos a los que se enfrenta la protección de datos confidenciales y delicados en el entorno de la nube. Concretamente, al 70% de los encuestados les resulta más complicado gestionar los reglamentos en materia de privacidad y protección de datos en un entorno de nube que in situ. Aún más, solo el 44% de los encuestados afirma que su organización tiene cuidado a la hora de compartir información delicada con terceros, y solo el 46% afirma que su organización es proactiva en cuanto a la gestión del cumplimiento de los reglamentos de privacidad y protección de datos en la nube.

Figura 5
Percepciones sobre prácticas de gobernanza en la nube
Combinación de las respuestas "Totalmente de acuerdo" y "De acuerdo"

En la mayoría de las organizaciones se sigue creyendo que el uso de recursos en la nube influye en los riesgos relacionados con el cumplimiento normativo.

Más de la mitad (56%) de los encuestados afirma que el uso de recursos en la nube aumenta el riesgo de incumplimiento normativo. Como ya se ha mencionado en la página anterior, resulta difícil gestionar los reglamentos en materia de privacidad y protección de datos en la nube.

el 56%

de los encuestados afirma que el uso de recursos en la nube aumenta el riesgo de incumplimiento normativo

Las organizaciones almacenan en la nube datos corporativos que consideran sometidos a riesgo.

Información sobre clientes, correos electrónicos y datos sobre consumidores son los tres principales tipos de datos que se almacenan en la nube. La propensión a almacenar en la nube es menor en el caso de datos confidenciales, como información sobre pagos, expedientes de empleados, propiedad intelectual e información de tipo sanitario.

La mayoría de las organizaciones adoptan un enfoque de primacía de la seguridad para la nube.

Aunque el 32% de los encuestados no ha adoptado un enfoque de primacía de la seguridad, el 68% restante sí lo ha hecho en alguna medida. Según se puede comprobar en la figura 6, el 39% delega la responsabilidad sobre el cifrado y los mecanismos de gestión de claves a su proveedor de servicios en la nube (21%) o a su proveedor de servicios de gestión de seguridad (18%).

el **32%**

de los encuestados no han adoptado un enfoque de primacía de la seguridad

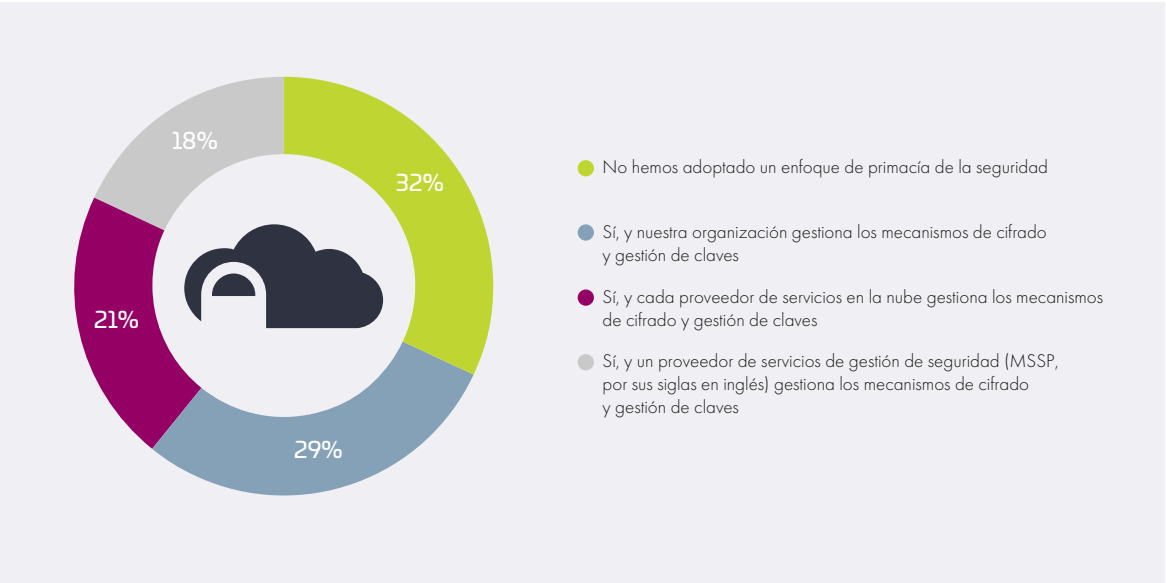


Figura 6
¿Ha adoptado su organización un enfoque de primacía de la seguridad para la nube?

Aumenta el uso del cifrado, la tokenización y otras herramientas criptológicas.

Durante los últimos tres años, ha aumentado el uso del cifrado, la tokenización u otras herramientas criptológicas para proteger los datos en la nube. Estos datos también se protegen mediante redes de datos privadas y los sistemas de seguridad de alta gama que ofrecen los proveedores de servicios en la nube. También hay un mayor conocimiento de las medidas que se toman para proteger información delicada o confidencial en la nube. En 2016 y 2017, el 35% de los encuestados afirmaba que no las conocía. Este valor ha caído hasta el 4% en la edición de este año del estudio.

el **96%**

de las organizaciones saben que están protegiendo información confidencial o delicada en la nube

Hay más organizaciones para las que resulta difícil proteger la información confidencial o delicada cuando utilizan servicios en la nube.

el 56%

considera que los servicios en la nube dificultan la protección de información delicada y confidencial

Este año, el 56% de los encuestados considera que los servicios en la nube dificultan la protección de información delicada y confidencial, lo que supone un aumento respecto al 49% que lo consideraba en la edición del estudio del año pasado.

Los motivos aducidos para el aumento de la dificultad de proteger datos en la nube son: la dificultad de aplicar medidas tradicionales de seguridad de la información en el entorno de cloud computing (67%) y la incapacidad de someter a inspección directa el cumplimiento normativo en materia de seguridad de los proveedores de servicios en la nube (64%). El 50% de los encuestados considera más difícil controlar o limitar el acceso de los usuarios finales.

El talón de Aquiles de la seguridad en la nube: la inadecuada inspección de los proveedores de servicios

Las organizaciones no están asumiendo la responsabilidad de garantizar la seguridad en la nube.

Más de un tercio (35%) de los encuestados considera que se debería responsabilizar de la protección de la información delicada o confidencial al proveedor del servicio, o bien que la responsabilidad debería ser compartida (33% de los encuestados). Solo el 31% de los encuestados afirma que su organización debería asumir la plena responsabilidad.

Las organizaciones siguen seleccionando proveedores de servicios en la nube según consideraciones de eficiencia y coste, pero no de seguridad.

Como ya se ha mencionado, muchas organizaciones esperan que el proveedor del servicio se haga responsable de la seguridad o que la responsabilidad sea compartida. No obstante, solo el 23% afirma que la seguridad es un factor que se baraja a la hora de seleccionar a un proveedor.

Aumenta el uso y la importancia de las soluciones de criptoagilidad, cifrado y tokenización

La mayoría de las organizaciones afirman que las aplicaciones en la nube aumentan su criptoagilidad o no influyen en ella en absoluto[5].

Más de la mitad (57%) de los encuestados afirma que la implantación de aplicaciones en la nube aumenta considerablemente (11%), aumenta (20%) o no influye (26%) en el nivel de criptoagilidad de su organización.

En la nube, es más probable que se protejan los datos estáticos que los datos dentro de las aplicaciones.

Desde 2015, ha habido un aumento de los encuestados que afirman que su organización utiliza el cifrado, la tokenización y otras soluciones criptológicas. No obstante, el cifrado de datos confidenciales en aplicaciones en la nube ha disminuido hasta el 29% del total de encuestados. Según estos encuestados, el cifrado es necesario de media para 10 aplicaciones.

La mayoría de los datos delicados que se encuentran en la nube no están cifrados.

El 80% de los encuestados afirma que la capacidad de cifrado o tokenización de datos delicados o confidenciales es muy importante o importante para la decisión de su organización en cuanto al uso de recursos en la nube. No obstante, como ilustran los promedios de la figura 7, menos de un 46% de esos datos se cifra cuando se traslada al entorno de nube, y solo un 43% se protege mediante cifrado y gestión de claves.

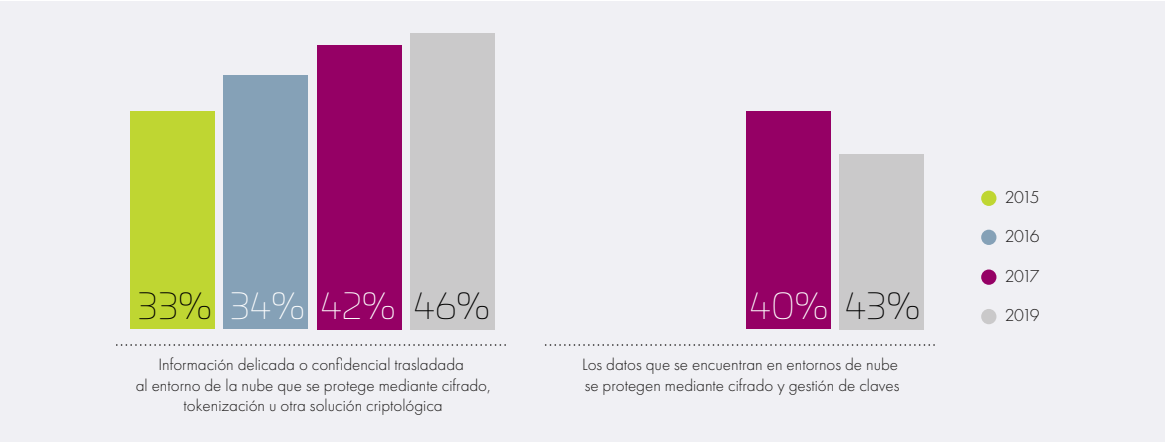


Figura 7
Porcentaje de toda la información delicada que está cifrada en la nube
Se presentan valores extrapolados

Cuando los datos están cifrados en la nube, solo la mitad de las organizaciones ostentan el control de las claves.

Poco más de la mitad de las organizaciones ostentan el control de las claves cuando los datos están cifrados en la nube, aunque el 53% de los encuestados afirma que su organización sí lo ostenta. Solo el 20% de los encuestados afirma que el proveedor de servicios en la nube ostenta el control, mientras que el 16% afirma que lo ostenta un tercero.

Casi la mitad (48% de los encuestados) afirma que es esencial o muy importante que su organización custodie las claves de seguridad y cifrado.

[5] La criptoagilidad, o agilidad criptográfica, es la capacidad que tiene un sistema de seguridad de la información para adoptar alternativas al método de cifrado original, o primitiva criptográfica, sin que se apliquen cambios significativos a la infraestructura de dicho sistema. Las pautas NIST declaran que "conservar la criptoagilidad es imperativo" para prepararse para la era de la informática cuántica. Se puede conseguir criptoagilidad adoptando nuevos marcos de respuesta ante incidencias y desarrollo de aplicaciones, así como adquiriendo una capa de software de servicios que facilite dicha criptoagilidad en aplicaciones heredadas y de la nube.

Tendencias en las prácticas de gestión de identidad y acceso en la nube

La mayoría de las organizaciones varían en su enfoque a la hora de controlar el acceso a datos delicados y confidenciales en la nube.

La mitad (50%) de los encuestados afirma que su organización cuenta con interfaces de gestión de identidad separadas para el entorno de la nube y el entorno in situ. Solo un 30% de los encuestados afirma contar con una interfaz de gestión de identidad unificada para ambos entornos.

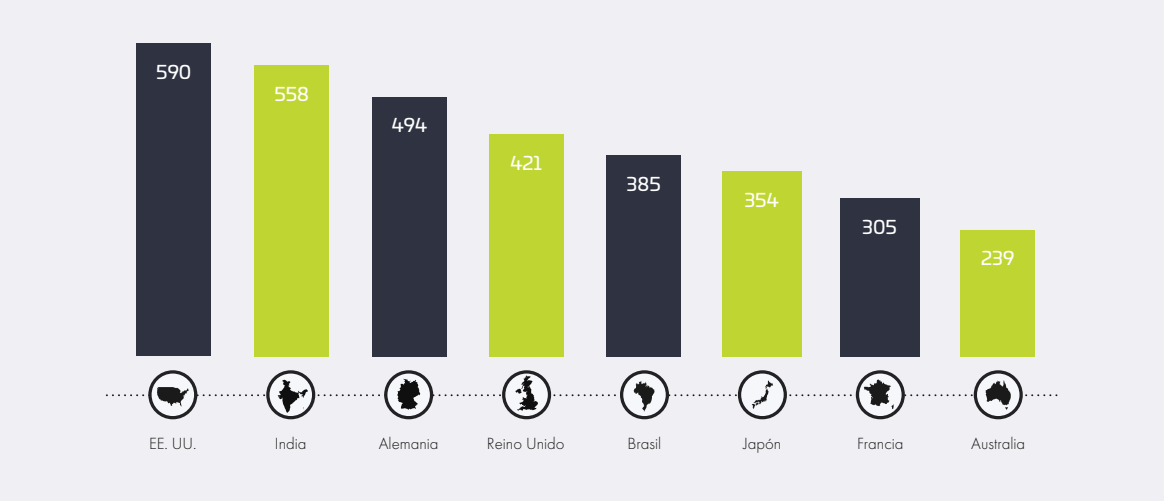
La importancia de la compatibilidad con múltiples normas de federación de identidad ha aumentado durante los últimos cuatro años.

Aun así, la característica más importante es la capacidad de controlar la autenticación fuerte antes de acceder a datos y aplicaciones en la nube (el porcentaje de los entrevistados que opina esto ha aumentado desde el 73% hasta el 82%). El estándar SAML se ha extendido considerablemente durante los últimos cuatro años (del 56% al 72%). Las características más importantes a la hora de controlar y proteger el acceso a los recursos en la nube se muestran en la figura 8.

Figura 8
Las características de gestión de identidad y acceso más importantes
Combinación de las respuestas "Esencial" y "Muy importante"

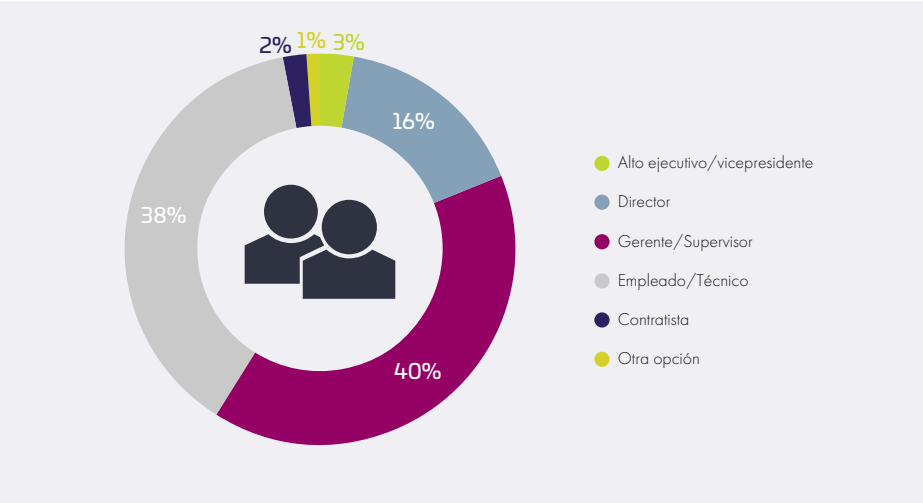
Información demográfica

Para participar en este estudio, se seleccionó una muestra de 95 242 expertos profesionales de TI y de seguridad en TI ubicados en Estados Unidos, el Reino Unido, Australia, Alemania, Francia, Japón, la India y Brasil, los cuales están al corriente del uso que hacen sus empresas de los recursos de nube pública y privada. La gráfica 1 muestra un total de 3667 encuestas cumplimentadas. Las verificaciones de selección y fiabilidad exigieron la eliminación de 321 de ellas. Nuestra muestra definitiva consistía en 3346 encuestas cumplimentadas, lo que equivale a una tasa de respuesta del 3,5%.



Gráfica 1
Número de encuestados

La gráfica 2 indica el nivel jerárquico del encuestado dentro de la organización participante. Por diseño, el 59% de los encuestados pertenece al nivel de supervisor o superior, y el 38% pertenece al nivel de empleado/técnico.

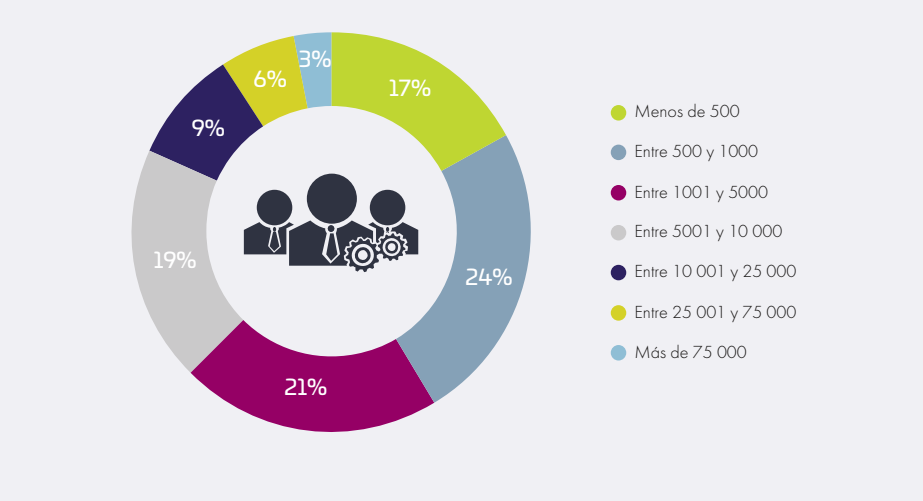


Gráfica 2
Puesto actual dentro de la organización

Como ilustra la gráfica 3, el 59% de los encuestados pertenece a organizaciones con más de 1000 empleados a nivel mundial.

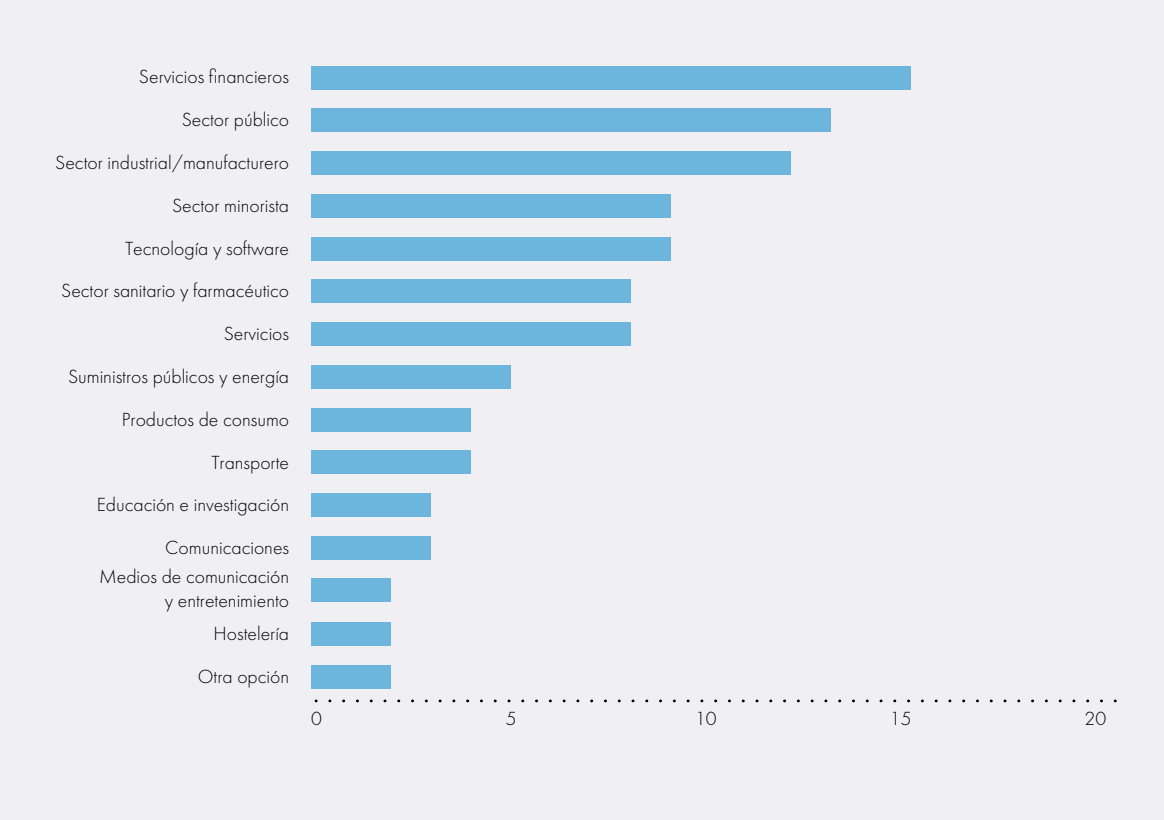
el 59%

de las organizaciones encuestadas tienen más de 1000 empleados a nivel mundial



Gráfica 3
Número de empleados a nivel mundial

Los porcentajes que figuran a continuación representan la clasificación industrial de las organizaciones de los encuestados. La gráfica 4 identifica los servicios financieros (15% de los encuestados) como el mayor segmento, seguido del sector público (13% de los encuestados) y el sector industrial/manufacturero (12% de los encuestados).



Gráfica 4
Clasificación industrial de las organizaciones de los encuestados

THALES

América
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100 | Austin, TX 78759 EE. UU.
Tel.:+1 888 343 5773 o +1 512 257 3900
Fax:+1 954 888 6211 | Correo electrónico: sales@thalesesec.com

Asia-Pacífico - Thales Transport & Security (HK), Ltd.
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel.:+852 2815 8633
Fax:+852 2815 8141 | Correo electrónico: asia.sales@thales-esecurity.com

Europa, Oriente Medio y África
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ, Reino Unido
Tel.:+44 (0)1844 201800 | Fax:+44 (0)1844 208550
Correo electrónico: emea.sales@thales-esecurity.com

> thalesgroup.com <

#CloudSecurity