Informe

¿Cielos despejados?

El nivel de adopción de la nube

intel Security

Índice

Agradecemos a los 1200 encuestados su participación y a los altos ejecutivos que indicamos a continuación haber compartido su experiencia y sus puntos de vista para este informe:

- Brent Conran, Vicepresidente y Director de seguridad de la información de Intel
- Brian Dye, Vicepresidente corporativo de Intel Security
- Dimitra Liveri, Directora de seguridad de la información y de redes de ENISA (Agencia Europea de Seguridad de las Redes y de la Información)
- Vanessa Pegueros, Directora de seguridad de la información de DocuSign, Inc.
- Jim Reavis, Director general de Cloud Security Alliance
- Dave Shackleford, Analista de SANS y Director general de Voodoo Security
- Timothy Youngblood, Director de seguridad de la información de Kimberly-Clark

¿Una nube para cada temporada? Es cuestión de confianza

Prácticamente toda persona que enciende un dispositivo electrónico consume computación en la nube de alguna manera. Ya sea para aplicaciones de automatización doméstica o para aplicaciones empresariales destinadas a generar ingresos, todos confiamos en Amazon Web Services, Microsoft Azure y otros proveedores de servicios en la nube que ofrecen dichos servicios. Según nuestra visión sobre la evolución y el futuro de la computación en la nube, el uso que hacemos de esta plataforma informática se expandirá y las consecuencias de nuestra dependencia de la nube tendrán enormes ramificaciones para cada uno de nosotros —consumidores y empresas—. De acuerdo con nuestra encuesta, en los próximos 12 - 18 meses, la mayor parte del presupuesto para la infraestructura de TI de las empresas se dedicará a recursos de nube pública. Algunas personas consideran esto un punto de inflexión en las tecnologías de la información.

Analicemos las implicaciones de esta transición. En primer lugar, los profesionales técnicos que trabajan en estas empresas deberán desarrollar convenientemente sus competencias. En segundo lugar, el nivel de confianza depositado en la nube tendrá que mejorar —y, con ello, la visibilidad adicional que todos exigimos para alcanzar ese nivel de confianza—.

Aunque la nube es una realidad hoy en día, el futuro augura una expansión de sus capacidades, así que no es de extrañar que los servicios y las aplicaciones más importantes se trasladen a la nube. De hecho, ahora que empezamos a especular sobre cómo será el centro de datos empresarial del futuro, es posible que se dé prioridad a la nube para el despliegue por defecto para las aplicaciones, y el alojamiento en las instalaciones sea la excepción (únicamente si hay una razón para ello).

Con las medidas de seguridad adecuadas en vigor, las posibilidades que ofrece la computación en la nube permiten integrar nuevas aplicaciones y herramientas empresariales avanzadas destinadas a aumentar la productividad. No obstante, como podrá leer en nuestro estudio, las empresas siguen enfrentándose a problemas de confianza y seguridad.

A medida que dependemos más de estas plataformas informáticas, tenemos la oportunidad de aumentar el nivel de confianza en sintonía con las expectativas de las empresas y los consumidores. Cloud Security Alliance, una organización dirigida por voluntarios y líder en investigación técnica, invita a otras organizaciones y sus miembros a participar y dirigir esta transformación.

—Raj Samani, Director de tecnología de Europa, Oriente Medio y África de Intel Security
—Jim Reavis, Director general de Cloud Security Alliance

Introducción

Conforme los requisitos empresariales conduzcan a las empresas rápidamente a la computación en la nube y más allá de proyectos piloto y a pequeña escala, ¿cuáles son las tendencias y los problemas clave a los que tendrán que hacer frente? ¿Cómo pueden las empresas aprovechar las ventajas que ofrece la nube sin poner en riesgo la seguridad y el control?

En una encuesta basada en ocho países, preguntamos a 1200 responsables de la toma de decisiones en entornos de TI encargados de la seguridad de la nube de sus organizaciones sobre sus planes en cuanto a la adopción de la nube, y cuáles eran sus mayores desafíos y sus prioridades en términos de inversión para el año siguiente.

En este informe, analizamos las tendencias de la adopción de la nube en empresas y cómo varían en función de si se trata de software como servicio (SaaS), infraestructura como servicio (IaaS), plataforma como servicio (PaaS), seguridad como servicio, y también nube pública, privada o híbrida. También analizamos cómo las empresas de sectores más regulados intentan superar los problemas relacionados con el cumplimiento normativo al adoptar la computación en la nube.

Exploraremos los mitos y la realidad en relación a los mayores problemas de seguridad de la nube a los que se enfrentan las empresas y analizaremos la efectividad de las inversiones en tecnologías de seguridad en la nube, incluidos el cifrado y la prevención de la pérdida de datos, entre otros.

Asimismo, veremos cómo afrontan las empresas el desafío que supone la nube suministrada por la TI en la sombra, al tiempo que se permite a los empleados y los departamentos acceder a los servicios que requieren con la seguridad necesaria para proteger la información corporativa. En este informe, evaluaremos también el conocimiento a nivel de administración de los riesgos de la seguridad en la nube.

"Hemos ido bastante más allá que las primeras empresas que probaron la nube, adoptando a escala completa diversos tipos de nube. En el consejo de administración, estamos observando un reconocimiento real de que este es el futuro de la TI: trasladar la computación a un servicio general".

—Jim Reavis, CEO de Cloud Security Alliance

La tecnología de la información empresarial incrementa la inversión en la nube

Los consumidores ya utilizan la nube en su vida diaria para realizar todo tipo de tareas, desde cargar fotos hasta acceder al correo electrónico o realizar copias de seguridad de los datos. Nuestra encuesta pone de manifiesto que actualmente nos encontramos en un punto de inflexión que da paso a la computación en la nube como tecnología dominante para la infraestructura de TI de las empresas.

Si bien es posible que el incremento de la inversión y el aumento de adopción de la nube por parte de las empresas no sean tan sorprendentes, lo que sí es significativo es el ritmo tan rápido al que está ocurriendo. Nuestra encuesta revela un cambio en el panorama de las infraestructuras de TI a nivel empresarial, en el que la gran mayoría de los presupuestos de TI de las organizaciones se va a dedicar a servicios en la nube en menos de un año y medio —e incluso con mayor celeridad en el caso de algunos países (Figura 1)—. Los encuestados respondieron que esperaban que el 80 % del presupuesto de TI de su empresa se invirtiese en servicios de computación en la nube en un plazo de 16 meses. Las empresas de Brasil y Australia esperan alcanzar esta cifra del 80 % en el plazo de un año.

"Nuestros socios empresariales están aprovechado la naturaleza dinámica de la nube, la velocidad mejorada, la mayor colaboración y la flexibilidad de los servicios —que, en su conjunto, hacen de la nube una opción atractiva— y están dando pasos en esa dirección porque, de no hacerlo, sufrirían las consecuencias. Como profesionales de la seguridad, tenemos que involucrarnos y demostrar cómo la seguridad puede ser la base".

—Timothy Youngblood, CISO de Kimberly-Clark

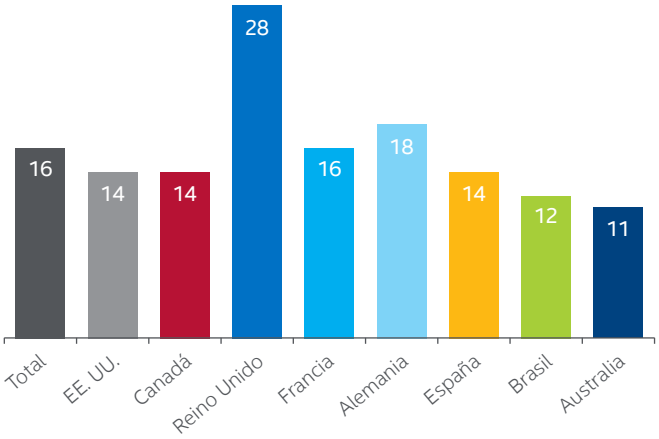

Figura 1. Promedio de meses hasta que los servicios de computación en la nube constituyan el 80 % del presupuesto de TI de la empresa del encuestado (por países).

La migración a los servicios en la nube mencionada por los encuestados de nuestro estudio se refiere a implementaciones tanto de carácter privado como público. Según nuestra encuesta, la nube privada es actualmente el modelo imperante entre las empresas, con el 51 % de la implementación total en la nube. La nube pública representa el 30 %, y la nube híbrida asciende al 19 % de las implementaciones en la nube de las empresas. Cuando analizamos cuántos meses transcurrirán hasta que el 80 % del presupuesto de TI de una empresa se asigne a los servicios de computación en la nube, el plazo correspondiente a la nube privada se reduce a solo 15 meses.

"En DocuSign, nuestra filosofía es dar prioridad a la nube, y estamos observando que muchos de nuestros clientes en todos los sectores están aplicando el mismo enfoque. En el caso de las compañías de los sectores muy regulados, como los servicios financieros y la atención sanitaria, resulta más complejo. Las organizaciones de TI de estas compañías se encuentran en una posición muy complicada porque las entidades reguladoras relevantes exigen que demuestren que se han aplicado todas las medidas de seguridad necesarias antes de la implementación. Por una parte, reciben una enorme presión para dedicar el tiempo suficiente a confirmar esto a las entidades reguladoras y, al mismo tiempo, sus empresas les presionan para que sean más eficientes y hábiles, además de para que hagan todo con mayor rapidez."

—Vanessa Pegueros,
CISO de DocuSign, Inc.

"Somos conscientes de qué información es adecuado almacenar en la nube y cuál no. Si se trata de información valiosa para la empresa, probablemente debería permanecer dentro de los dominios de la compañía y mantenerse en una nube privada".

—Eric Knapp, Director global de ciberseguridad de Honeywell

Se observan evidencias de que la adopción de los servicios en la nube se encuentra en un punto de inflexión. Las empresas están empleado una media de 43 servicios en la nube actualmente, aunque cabe destacar que existen algunas variaciones significativas a nivel regional (Figura 2). El Reino Unido, por ejemplo, es el más lento en términos de adopción de la nube (una media de solo 29 servicios en la nube por organización), mientras que las empresas de Brasil se encuentran entre las que más adoptan los servicios en la nube (55 servicios en la nube por organización).

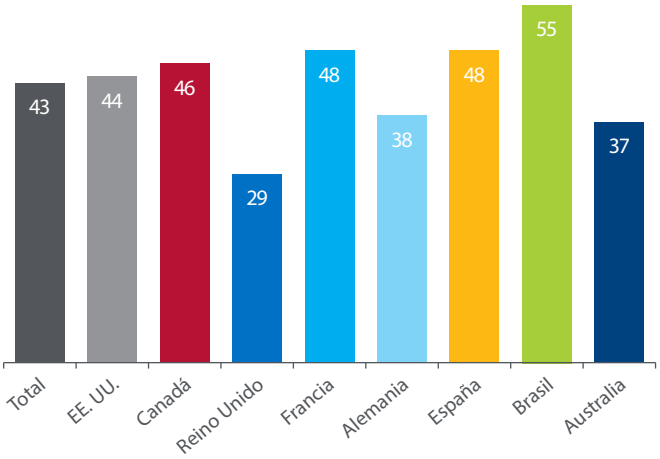

Figura 2. Promedio de servicios en la nube que utilizan actualmente las empresas (por países).

Por supuesto, también habrá diferencias en la adopción de los diferentes tipos de plataformas de nube —públicas, privadas, e híbridas o gestionadas, así como SaaS, IaaS y PaaS. Además, también hay evidencias de que la adopción varía de un sector a otro. En sectores muy regulados, como los servicios financieros, sigue habiendo ciertas reticencias a migrar a la nube, y el sector público y el gobierno también se quedan atrás.

Si analizamos la tendencia de la adopción de la nube, es fácil caer en la trampa de limitarse a hablar sobre SaaS. De hecho, nuestra encuesta revela que la mayoría de las empresas tienen pensado invertir en todos los modelos de servicios en la nube, pero —y esto puede parecer sorprendente— el mayor porcentaje (81 %) lo representa la IaaS, en comparación con solo el 60 % del SaaS (Figura 3). A esta le sigue de cerca la seguridad como servicio (79 %), e incluso la inversión programada en la PaaS (69 %) es superior a la del SaaS.

Esto está respaldado por el informe de SANS, que también demuestra que la IaaS será la mayor área de crecimiento de las implementaciones en la nube a nivel empresarial durante el próximo año.

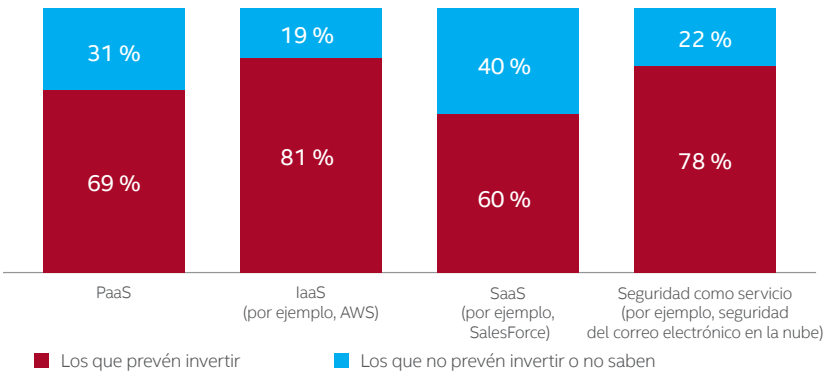

Figura 3. ¿En qué implementaciones en la nube tiene pensado invertir su empresa?

"La visibilidad de cómo opera el proveedor de servicios en la nube y de qué ocurre realmente obstaculiza parte del análisis de riesgos y de las decisiones en torno a la gestión de los mismos. Muchas de las normativas se elaboraron antes de la era de la nube, cuando se asumía que una empresa tenía el control total sobre las tecnologías informáticas y ahora, con la nube, ya no es así".

—Jim Reavis,
CEO de Cloud Security Alliance

"Sí hay aspectos preocupantes sobre las fugas de datos. A menudo, se traducen en ataques a las credenciales del usuario que tiene derecho de acceso al servicio en la nube, de modo que la información se filtra de esa forma".

—Jim Reavis,
CEO de Cloud Security Alliance

Seguridad y cumplimiento normativo: necesidad de una mejor visibilidad

¿Cuáles son las implicaciones de esta mayor adopción de los servicios en la nube para la seguridad de las empresas? Es posible que se alojen en la nube otros datos importantes y confidenciales. Un 40 % de los encuestados en el estudio de SANS —**Orchestrating Security in the Cloud** (Organización de la seguridad en la nube)—, mantiene que procesa o almacena datos confidenciales en la nube[1]. Los tipos más comunes de datos que se almacenan en la nube son inteligencia empresarial (52 %), contabilidad financiera (52 %), registros de empleados (48 %) e información personal de los clientes (40 %). Lo más preocupante es el 13 % de las empresas que afirma que no sabe si tiene datos confidenciales en la nube. Muchos expertos en seguridad creen que esta cifra es mucho más elevada, especialmente entre las grandes empresas. Esto se debe, en parte, a que algunas empresas no quieren admitir que no lo saben, mientras que otras que mantienen operaciones y unidades de negocio repartidas por todo el mundo no saben realmente si están expuestas de este modo.

Garantizar el cumplimiento normativo en la nube es la mayor preocupación, en todos los tipos de implementación en la nube, según el 72 % de los encuestados en el estudio de SANS. La mayor dificultad en este caso gira en torno a la visibilidad: más de la mitad (58 %) de los encuestados del estudio de SANS menciona la falta de visibilidad de las operaciones del proveedor de los servicios en la nube como su mayor problema.

¿Nubes oscuras en el horizonte? Amenazas de cara al siglo XXI

Nuestra encuesta pone de relieve que ha llegado el momento de volver a evaluar cuáles son las verdaderas amenazas de la nube, dado que existe una brecha entre lo que se percibe y la realidad.

En la mayoría de los países, la principal preocupación sobre el uso del SaaS gira en torno a los incidentes de seguridad de los datos —según más de uno de cada cinco encuestados (22 %)—. Las fugas de datos también son una de las principales preocupaciones en torno a las nubes privadas y la IaaS. Existen algunas diferencias a nivel regional, en especial, en Australia, donde el tiempo de inactividad es lo que más preocupa.

Pero, ¿cuál es la realidad?

Al indagar sobre el tema, menos de la cuarta parte (23 %) de las empresas mantiene que ha experimentado pérdidas o fugas de datos con sus proveedores de servicios en la nube, y solo una de cada cinco había observado accesos no autorizados a los datos o servicios. La encuesta de SANS revela un nivel de fugas de datos en la nube incluso más bajo, y solo el 9 % de los encuestados afirma haber experimentado algún incidente en nubes públicas o con sus aplicaciones en la nube privada o SaaS.

Los incidentes y problemas más comunes a los que se enfrentaron los encuestados con los servicios en la nube fueron precisamente la migración de los servicios y los datos, los altos costes, y la visibilidad insuficiente o inexistente de las operaciones del proveedor de la nube (Figura 4).

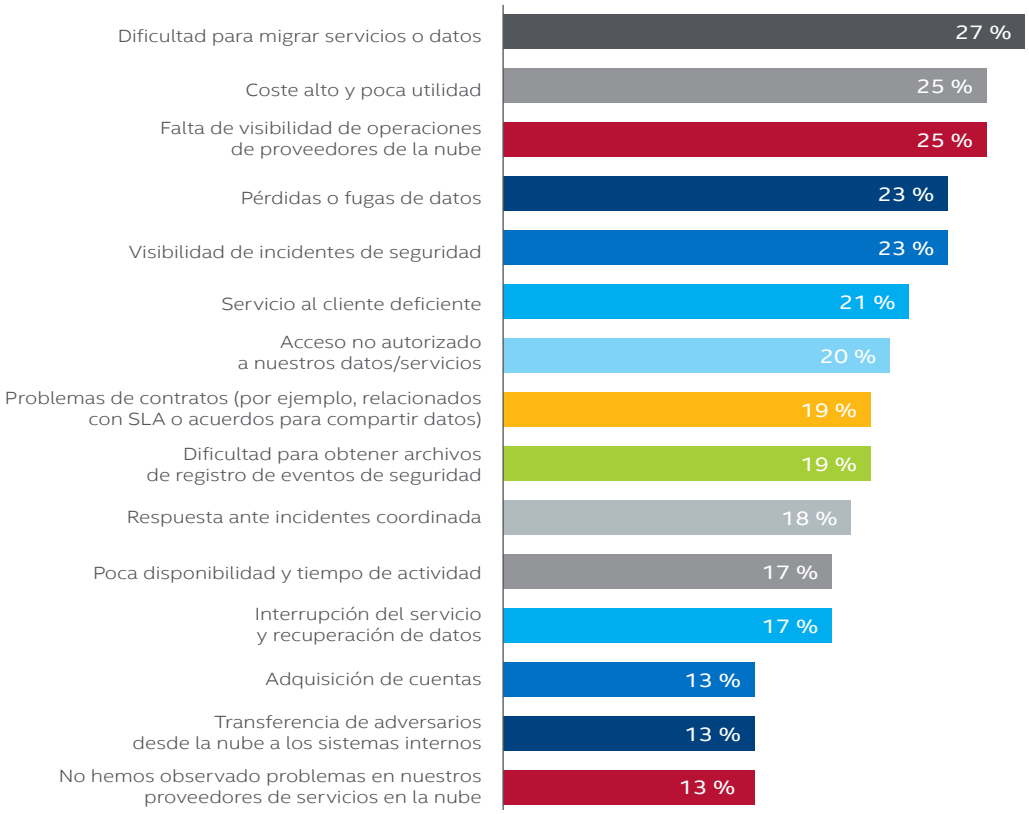

Figura 4. En cuanto a la seguridad de la nube, ¿qué problemas ha tenido su empresa con los proveedores de servicios en la nube?

"Las empresas requieren incorporar la seguridad en DevOps y los dos elementos más críticos son una supervisión continua y la detección de cambios".

—Dave Shackleford, Analista de SANS y Director general de Voodoo Security

Al analizar las amenazas de seguridad específicas de la nube identificadas por los encuestados, el malware y las redes de bots constituyen el principal problema de las implementaciones en nubes privadas (33 %), mientras que los ataques de denegación de servicio se consideran la principal amenaza en las nubes públicas (36 %).

Pueden surgir otros riesgos de seguridad en la nube al ampliar o reducir los servicios de forma rápida, aunque esto responde más a un problema de disponibilidad y continuidad de la actividad empresarial que las empresas deben prever. Otra característica clave de la adopción de la nube es el aumento de DevOps —los ciclos cada vez más rápidos de desarrollo, prueba e implementación de las aplicaciones—. Incorporar una seguridad sólida en este entorno de desarrollo continuo es esencial para mantener un seguimiento de esos rápidos cambios y permanecer alerta ante cualquier posible riesgo de seguridad relacionado.

Está claro que no debemos sacar conclusiones de forma precipitada basándonos en los resultados de la encuesta que sugieren que las fugas de datos en la nube no constituyen una amenaza de seguridad grave o no han ocurrido nunca. Debemos considerar la posibilidad de que las fugas de datos no se hayan comunicado, ya que no siempre se informa a las entidades reguladoras y organismos de las fuerzas de seguridad. Además, cuando se producen fugas de datos en la nube, las consecuencias suelen ser significativas. Aunque hasta cierto punto es preciso cerrar la brecha entre cómo se perciben las amenazas de seguridad de la nube y la realidad, la encuesta sugiere que la inversión y la planificación sobre cómo mitigar los riesgos de fuga más destacados se debe equilibrar con algunas de las amenazas cotidianas más habituales en sistemas empresariales y los datos en la nube. Entre ellas, se incluyen los problemas de la migración, un servicio de atención al cliente deficiente y problemas contractuales, así como amenazas de seguridad específicas, como la denegación de servicio, el malware y el pirateo de cuentas.

Seguridad y riesgos en la nube: el ángulo muerto de la alta dirección

Nuestra encuesta muestra un alto grado de implicación en la toma de decisiones sobre la seguridad de la nube por parte de la alta dirección —no solo el director de TI, el CIO y el CISO, sino también con frecuencia el CEO y el CFO—. No obstante, ¿comprenden los altos directivos los riesgos de seguridad?

"Los consejos de administración y los altos ejecutivos reconocen cada vez más que la seguridad de la nube es un aspecto clave de cualquier empresa y se debe tomar en serio".

—Vanessa Pegueros, CISO de DocuSign, Inc.

En lo que se refiere a las nubes públicas, parece haber una falta de concienciación entre los directivos en cuanto a las implicaciones de almacenar datos confidenciales en la nube pública (véase la Figura 5). Solo el 34 % de los encuestados opina que los altos directivos de su empresa conocen perfectamente las implicaciones, mientras que uno de cada cinco mantiene que los ejecutivos de alto nivel desconocen completamente dichos riesgos o los conocen solo por encima. En el Reino Unido el problema es aún más acusado, ya que solo el 15 % considera que la alta dirección de su empresa entiende plenamente el riesgo de almacenar datos en la nube pública. Esta cifra contrasta con Brasil (49 %) y Australia (47 %), donde la concienciación al respecto es mucho mayor entre los miembros del consejo de administración.

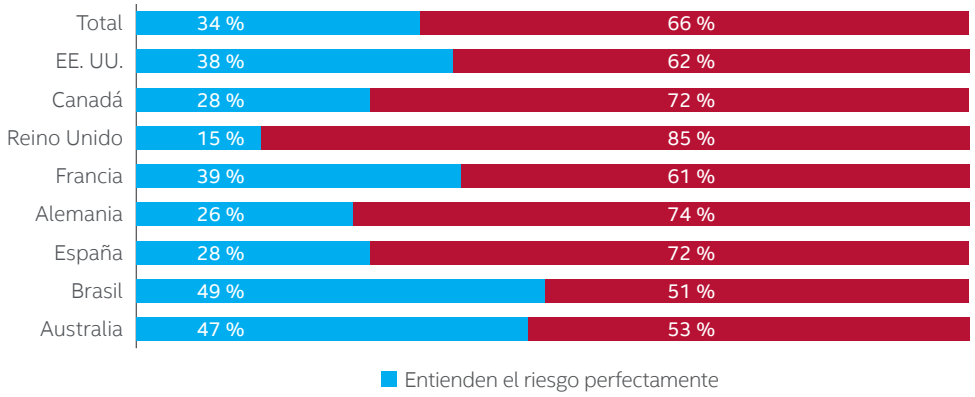

Figura 5. ¿Cree que los altos directivos comprenden las implicaciones en materia de seguridad de almacenar información confidencial en la nube pública?

"La educación es poder. Contamos con un programa de concienciación de seguridad muy intensivo que se centra en formar a todos nuestros empleados en el valor de la información. Es lo que denominamos nuestro 'firewall humano'".

—Timothy Youngblood, Director de seguridad de la información de Kimberly-Clark

Si bien las fugas de datos más destacadas, y sus consecuencias financieras y para la reputación, han hecho que la seguridad de los datos sea fundamental para muchos CEO y altos directivos, nuestra encuesta sugiere que falta trabajo de educación para mejorar la concienciación y el conocimiento de los riesgos asociados al almacenamiento de información confidencial en la nube.

Tecnologías de la información en la sombra: ¿un riesgo o una oportunidad?

La mayor parte de nuestros encuestados mantiene que la "TI en la sombra" (o tecnologías utilizadas sin la aprobación de la empresa) influye de manera negativa en la capacidad de su empresa para garantizar la seguridad de los servicios en la nube, y el 10 % de ellos afirma que deja a sus empresas expuestas a un nivel de riesgo importante.

La protección de la TI en la sombra sigue suponiendo un gran reto: el 52 % de los departamentos sigue esperando que el equipo de TI proteja sus servicios en la nube que no cuentan con autorización. Además, casi una cuarta parte de los encuestados (23 %) afirma que estos departamentos se ocupan de su propia seguridad sin la ayuda del equipo de TI.

"La TI en la sombra es la nueva tecnología de la información. El modelo antiguo ha salido de escena. Cuanto más nos resistimos, más lejos estamos de trabajar para protegerla. Debemos aceptar que la TI en la sombra es la nueva realidad y dedicar nuestras energías a gestionarla de forma segura".

—Vanessa Pegueros, CISO de DocuSign, Inc.

"Los profesionales básicamente intentan hacer su trabajo. Si nosotros no les ofrecemos los medios necesarios, recurrirán a otros. El departamento de TI y el CIO deben actuar como el agente de seguridad y adoptar los servicios de la nube y de SaaS."

—Brent Conran, Vicepresidente y CISO de Intel

La visibilidad de la TI en la sombra departamental es normalmente superior para el SaaS que para la IaaS. Sin embargo, en todos los casos, al menos un 20 % de los encuestados desconoce si hay TI en la sombra en todos los departamentos de sus empresas. Los niveles de TI en la sombra son mayores en los departamentos de ventas, I+D y marketing. La mayor incógnita es el departamento jurídico. El 37 % de los encuestados no es capaz de decir si dicho departamento emplea servicios en la nube sin el conocimiento del departamento de TI.

¿Cómo gestionan las empresas la TI en la sombra? Los métodos más comunes son los siguientes:

- Supervisión de la actividad de las bases de datos (49 %).
- Firewalls de última generación (41 %).
- Gateways web (37 %).

Otra táctica consiste en colaborar con el departamento financiero para que les avisen sobre informes de gastos enviados para los servicios en la nube.

Hay una notable diferencia en cómo se reacciona ante la TI en la sombra cuando se detecta. Casi la mitad de los encuestados (46 %) bloquea el acceso, mientras que el 37 % migra la TI en la sombra a un servicio aprobado.

¿Está afianzándose la confianza en la nube?

A primera vista, las cifras de nuestra encuesta muestran un nivel relativamente bajo de confianza en la computación en la nube en comparación con la tecnología in situ o alojada de forma interna. No sorprende que la nube pública sea el modelo que menos confianza inspira (Figura 6).

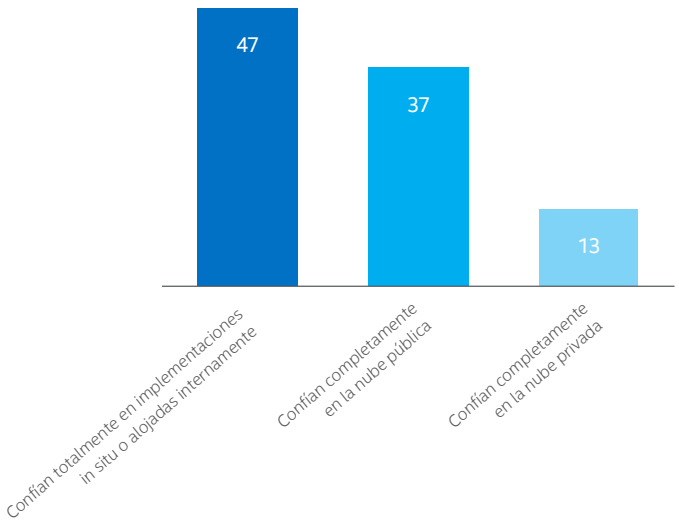

Figura 6. "¿Hasta qué punto confiaría en los siguientes métodos para mantener segura la información confidencial de su empresa?"

Lo que es más significativo es que, si nos basamos en una visión más amplia, hay un mayor grado de confianza en general en la computación en la nube con respecto al año anterior: el 77 % de las empresas mantiene que su empresa confía más ahora en la computación en la nube que hace un año (Figura 7).

"Se acerca una nueva era para los proveedores de servicios en la nube. Nos encontramos en un periodo de transición, pero creo que estas nuevas disposiciones regulatorias contribuirán a que aumente la inversión y la confianza, para que nos sintamos más cómodos con los servicios en la nube".

—Dimitra Liveri, Directora de seguridad de la información y de redes de ENISA (Agencia Europea de Seguridad de las Redes y de la Información)

"El primer punto de partida para la seguridad de las empresas en la nube pública es preguntarse cuáles son los límites de responsabilidad, y qué puede, como empresa, controlar a la perfección y qué está obligado a gestionar el proveedor de servicios en la nube. Además, es necesario evaluar los controles de todo el espectro de seguridad, incluidas la seguridad de los datos, la administración de identidades y la aplicación de directivas. Habrá cosas que ya no podrá controlar, especialmente a nivel de la red".

—Dave Shackleford, Analista de SANS y director general de Voodoo Security

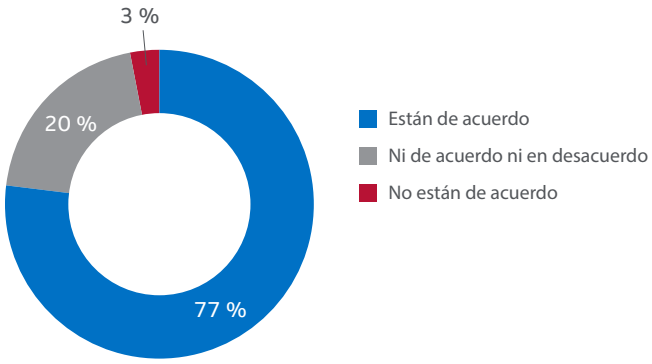

Figura 7. Encuestados que están de acuerdo con la afirmación "Mi empresa confía más ahora en la computación en la nube que hace 12 meses".

Con dos normativas importantes pendientes de votación en la Comisión Europea, el 2016 promete ser un gran año para los usuarios y los proveedores de los servicios en la nube de Europa. Se trata de la normativa europea sobre protección de datos y la directiva sobre seguridad de la información y las redes. ¿Contribuirá esta legislación a mejorar la confianza en la seguridad de la nube? Los expertos creen que así será.

Prioridades de la inversión en seguridad de la nube

Las prioridades de la inversión en seguridad varían en función de los distintos tipos de implementaciones basadas en la nube. Las empresas hacen uso de una media de tres soluciones de seguridad para proteger sus aplicaciones de SaaS. La más común es el cifrado de archivos (60 %), seguida de la seguridad del correo electrónico (55 %).

En el caso de la IaaS, las empresas recurren a una media de cuatro soluciones de seguridad. Las más comunes son los firewalls (70 %) y el cifrado (62 %). En el caso de la nube privada, también se contempla una media de cuatro soluciones de seguridad, de las que los firewalls constituyen la más común (67 %).

Las cuatro áreas principales de la seguridad como servicio en las que las empresas tienen planificado invertir son las mismas en las que ya están invirtiendo: protección del correo electrónico, protección web, protección antimalware y firewalls para aplicaciones (Figura 8). Esta tendencia indica que las empresas tienen intención de mejorar y ampliar los servicios de seguridad basados en la nube que ya tienen implementados.

La encuesta de SANS también destaca algunas áreas clave de la inversión en seguridad de la nube para los próximos 18 meses. Entre ellas, se incluyen el análisis de vulnerabilidades, la autenticación multifactor, la prevención de la pérdida de datos, la gestión de registros, los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS), la administración de información y eventos de seguridad (SIEM) y los servicios de los agentes de seguridad de acceso a la nube (conocidos como CASB).

Según el informe de Gartner *Market Guide for Cloud Access Security Brokers* (Guía de mercado para agentes de seguridad de acceso a la nube), los CASB, en concreto, constituyen un área de alto crecimiento. Gartner predice que, "para 2020, el 85 % de las grandes empresas utilizará un producto basado en agentes de seguridad de acceso a la nube para sus servicios en la nube, que es más del escaso casi 5 % de hoy en día"[2]. Nuestra encuesta respalda esta cifra. A pesar del hecho de que los CASB constituyen un servicio relativamente nuevo, el 36 % de las empresas utiliza estos servicios para proteger sus aplicaciones de SaaS, y el 32 % los utiliza para supervisar las implementaciones basadas en la nube por servicios de TI en la sombra. Casi una cuarta parte (24 %) de las empresas tiene pensado también invertir en CASB como servicio de cara al futuro.

"Comprender qué está ocurriendo en su entorno basado en la nube —por ejemplo, entre la base de usuarios y Salesforce— es absolutamente esencial. Además, estudiaré más de cerca las herramientas que nos permiten gestionarlo de forma más segura. Necesitamos también herramientas que contribuyan a automatizar los procesos, como la respuesta a los incidentes, y que nos permitan hacer más con lo que ya tenemos".

—Vanessa Pegueros,
CISO de DocuSign, Inc.

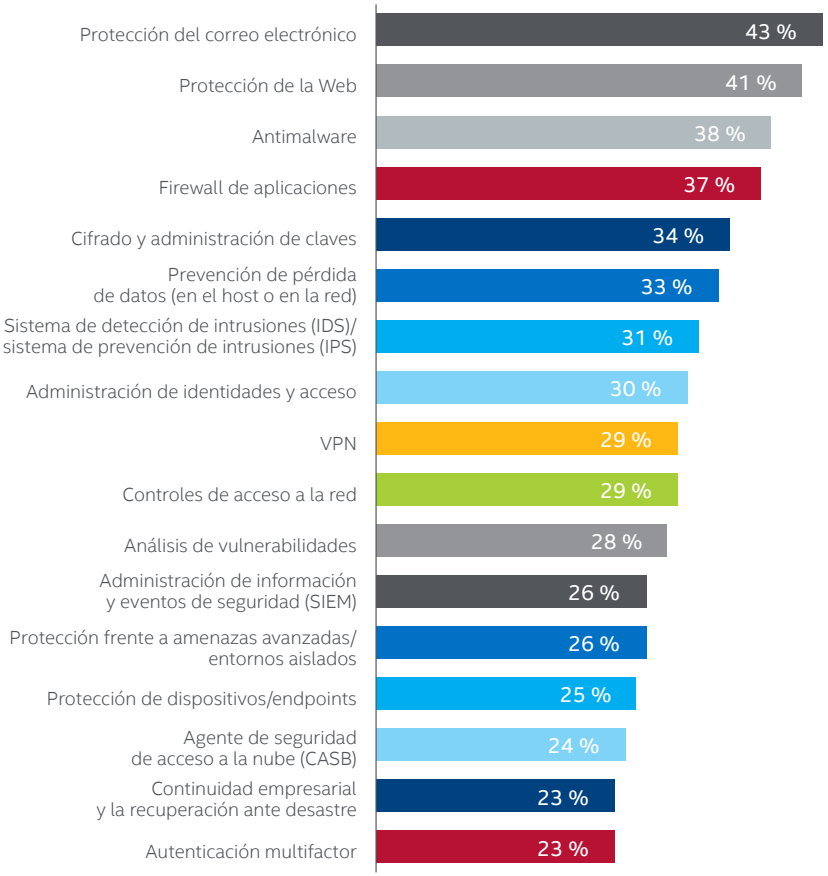

Figura 8. ¿En qué áreas de la seguridad como servicio tiene previsto invertir su empresa?

De las empresas que utilizan un servicio basado en la nube pública, poco más de la tercera parte (34 %) declara que disponen de una solución unificada con una integración completa y una administración centralizada en sus sistemas in situ y basados en la nube híbridos. Por lo tanto, aún se puede mejorar.

Resumen

La adopción de la nube en las empresas se acerca a pasos agigantados a un punto de inflexión, ya que las organizaciones afirman que el 80 % de su presupuesto en TI se dedicará a los servicios en la nube en un plazo de 16 meses como máximo.

Hay muchos motivos para que las empresas opten por los servicios en la nube, como una mayor agilidad, una innovación más rápida y una rentabilidad superior. Sin embargo, una variedad tan enorme de opciones de implementación comporta dificultades en materia de seguridad. Dado que la nube es o será el repositorio de tantos datos corporativos importantes, las empresas deben tener en cuenta lo siguiente:

- Los controles de seguridad y el cumplimiento normativo son responsabilidades que comparten las empresas y los proveedores de servicios en la nube. Pregunte a su proveedor de servicios acerca de los controles de seguridad y asegúrese de que la elaboración de informes esté incluida en su acuerdo de nivel de servicio (SLA). No obstante, es esencial que la empresa proteja lo que está bajo su control en la nube —ya sean datos, aplicaciones o cargas de trabajo— e incorpore esta seguridad en los planes de arquitectura de la nube.

"Aunque haya externalizado la nube, sus responsabilidades siguen recayendo sobre usted. No se puede decir 'Ah, es responsabilidad de Amazon'".

—Brent Conran, Vicepresidente y CISO de Intel

- Entre las áreas clave de la inversión en seguridad de la nube, se incluyen el cifrado de datos, la administración de identidades y de acceso, la prevención de pérdida de datos y la protección del correo electrónico. Las empresas invierten cada vez más también en la seguridad como servicio y en otros servicios que contribuyen a organizar la seguridad entre diversos proveedores y entornos, en especial, los CASB.
- Mientras que las implementaciones en la nube basadas en la TI en la sombra sigan planteando dificultades, dado que pueden exponer los datos de la empresa a un mayor riesgo, las empresas de TI deben trabajar con las unidades de negocio para encontrar un modo más seguro que permita a los usuarios desplegar sus propias implementaciones en la nube. El equipo de TI puede recuperar el control y la visibilidad al desempeñar el papel de agente de seguridad y ofrecer a los usuarios empresariales unas alternativas de servicios en la nube más seguras.
- Aunque muchos consejos de administración se están involucrando en mayor medida en la toma de decisiones relacionadas con la seguridad de los servicios en la nube, hay una clara y preocupante falta de concienciación y conocimiento de los riesgos. Es necesaria más formación, así como una mayor implicación de los CIO y los CISO en las discusiones de las juntas directivas con otros cargos de la alta dirección. Las repercusiones financieras y los daños a la reputación que han experimentado recientemente las empresas debido a algunas fugas de datos de gran calado deberían motivar a los altos ejecutivos a considerar la seguridad de los datos como una prioridad —ya estén alojados de forma interna o en la nube—.

Metodología

La encuesta a 1200 responsables de la toma de decisiones en entornos de TI, encargados de la seguridad de la nube de sus organizaciones ha sido realizada por Vanson Bourne en junio de 2015. Los encuestados se seleccionaron en Australia, Brasil, Canadá, Francia, Alemania, España, el Reino Unido y Estados Unidos, a partir de una amplia diversidad de empresas, desde aquellas con entre 251 y 500 empleados, hasta las que tenían más de 5000 empleados.

Acerca de Intel Security

McAfee forma ahora parte de Intel Security. Con su estrategia Security Connected, su innovador enfoque de seguridad reforzada por hardware y su exclusiva red Global Threat Intelligence, Intel Security trabaja sin descanso para desarrollar soluciones y servicios de seguridad proactivos que protejan los sistemas, las redes y los dispositivos móviles de uso personal y empresarial en todo el mundo. Intel Security combina la experiencia y los conocimientos de McAfee con la innovación y el rendimiento demostrados de Intel para hacer de la seguridad un ingrediente fundamental en todas las arquitecturas y plataformas informáticas. La misión de Intel Security es brindar a todos la tranquilidad para vivir y trabajar de forma segura en el mundo digital. **www.intelsecurity.com**

1. *SANS: Orchestrating Security in the Cloud* (Organización de la seguridad en la nube), por Dave Shackleford, septiembre de 2015 (patrocinado por Intel Security).
2. Informe de Gartner *Market Guide for Cloud Access Security Brokers* (Guía de mercado para agentes de seguridad de acceso a la nube), por Craig Lawson, Neil MacDonald y Brian Lowans, 22 de octubre de 2015.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com