Informe

¿Cielos Azules en el Horizonte?

El estado de la adopción de la nube

intel Security

Contenido

Damos las gracias a los 1.200 encuestados por su participación y a los altos ejecutivos por compartir sus conocimientos y 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, Director de Redes y Seguridad de la Información, de la Red Europea y Agencia de Seguridad de la Información (ENISA)
- Vanessa Pegueros, Directora de Seguridad de la Información de DocuSign, Inc.
- Jim Reavis, Director Ejecutivo de la Cloud Security Alliance
- Dave Shackleford, Analista de SANS y Director Ejecutivo de Voodoo Security
- Timothy Youngblood, Director de Seguridad de la Información de Kimberly-Clark

¿Una Nube para Cada Temporada? Es una Cuestión de Confianza.

Casi todos los consumidores que encienden un dispositivo electrónico están consumiendo computación en nube de alguna manera. Ya sea para la automatización del hogar o para aplicaciones de negocios que generen ingresos, todos nosotros dependemos de Amazon Web Services, Microsoft Azure, u otros proveedores de computación en nube que mantienen la disponibilidad de dichos servicios. Conforme consideramos la evolución y el futuro de la computación en nube, nuestro uso de esta plataforma de cómputo crecerá, y el impacto de nuestra dependencia en la nube tendrá enormes repercusiones para todos y cada uno de nosotros, consumidores y negocios. De acuerdo a nuestra encuesta, durante los próximos 12 a 18 meses, la mayoría del presupuesto de TI de las empresas será gastado en recursos de computación en nube. Algunas personas se refieren a esto como un punto de inflexión en TI.

Consideremos las implicaciones de esta transición. En primer lugar, las habilidades de los profesionales de tecnología que trabajan en estas compañías tendrán que evolucionar de forma significativa. En segundo lugar, el nivel de confianza en la nube tendrá que mejorar y, con ello, la visibilidad adicional que todos necesitamos para lograr este nivel de confianza.

Mientras que la nube es hoy una realidad, el futuro trae consigo una ampliación del alcance de sus capacidades, no será de extrañar ver aplicaciones y servicios de infraestructura crítica trasladarse hacia la nube. De hecho, cuando empezamos a especular sobre cómo será el centro de datos empresarial del futuro, podría ser que Primero la Nube será el despliegue predeterminado para las aplicaciones, con la excepción (sólo si tiene sentido) de hospedar en las instalaciones propias.

Con la seguridad apropiada implementada, el poder de la computación en nube puede ser aprovechado para dar soporte a nuevas aplicaciones y herramientas de negocios avanzadas para hacer crecer la productividad. Sin embargo, como usted podrá leer en nuestro estudio, las empresas siguen luchando con problemas de confianza y seguridad.

Conforme nuestra dependencia en dichas plataformas de computación crece, tenemos una oportunidad para elevar el nivel de confianza en la alineación con las expectativas de las empresas y los consumidores. La Cloud Security Alliance, una organización dirigida por voluntarios y líder en investigación técnica, extiende una invitación a las organizaciones y a sus integrantes a participar y liderar esta transformación.

- Raj Samani, Director de Tecnología de EMEA de Intel Security

- Jim Reavis, Director Ejecutivo de la Cloud Security Alliance

Introducción

Conforme los requisitos de negocios impulsan a las empresas rápidamente hacia el cómputo en nube y más allá de proyectos a pequeña escala y pilotos, ¿cuáles son las principales tendencias y problemas que tendrán que abordar? ¿Cómo pueden aprovechar los negocios las ventajas de la nube sin poner en riesgo la seguridad y el control?

En una encuesta en ocho países, preguntamos a 1.200 tomadores de decisiones de TI con responsabilidad de la seguridad en la nube en sus organizaciones, acerca de sus planes para la adopción de la nube, sus mayores desafíos, y sus prioridades de inversión durante el próximo año.

En este informe, observamos las tendencias de adopción de nube empresarial y cómo se diferencian según el software: como un servicio (SaaS), Infraestructura como un servicio (IaaS), Plataforma como un servicio (PaaS), Seguridad como un servicio, y también nube pública, privada o híbrida. También observamos cómo las organizaciones de diversos sectores industriales regulados están intentando superar los problemas de cumplimiento relativos a la adopción de computación en nube.

Exploraremos el mito y la realidad de los mayores problemas que enfrentan las empresas de seguridad en la nube, y observaremos la eficacia de las inversiones en tecnologías de la seguridad en la nube, incluyendo cifrado, prevención de pérdida de datos y más.

También examinaremos cómo están enfrentando las empresas el desafío de la nube adquirida de manera oculta, mientras se habilitan a los empleados y departamentos a acceder a los servicios que necesitan, cuando lo necesitan con la seguridad necesaria implementada para proteger la información corporativa. En este informe, también evaluaremos el conocimiento a nivel de consejo de administración de los riesgos de seguridad en la nube.

"Hemos ido mucho más allá de los primeros adoptantes, aquellos que prueban y realizan proyectos pilotos de la nube, hasta la adopción a gran escala de una variedad de diferentes tipos de nube. En los consejos de administración estamos observando un verdadero reconocimiento de que este es el futuro de la TI, trasladando la computación hacia servicios".

—Jim Reavis, Director Ejecutivo de la Cloud Security Alliance

La TI Empresarial Refuerza la Inversión en la Nube

Los consumidores ya viven su vida en la nube y la utilizan a diario para realizar tareas que van desde subir fotos, hasta acceder a correo electrónico y hacer copias de seguridad de sus datos. Nuestra encuesta muestra que estamos ahora en un punto de inflexión donde el cómputo en nube se convertirá en un enfoque tecnológico dominante para la TI de la empresa.

Aunque el aumento de la inversión en la nube y la adopción por parte de las empresas podría no ser una gran sorpresa, lo significativo es el rápido ritmo al que esto está ocurriendo. Nuestra encuesta revela un cambio importantísimo en la TI empresarial, donde la inmensa mayoría de los presupuestos de TI de las organizaciones se gastan en servicios de nube en menos de un año y medio, e incluso más rápido en algunos países (Figura 1). Los encuestados indicaron que esperan que el 80% del presupuesto de TI de su organización se dedique a los servicios de computación en nube en 16 meses. Las organizaciones en Brasil y Australia esperan llegar a esta marca del 80% dentro de un año.

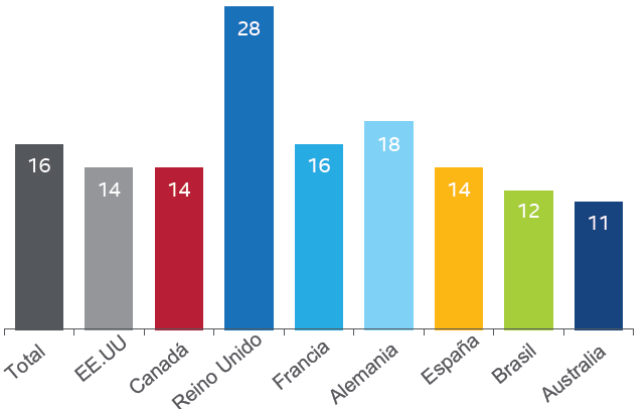

Figura 1. Número promedio de meses hasta que el 80% del presupuesto de TI de las organizaciones encuestadas estará compuesto de servicios de computación en nube, dividido por país.

"Nuestros partners de negocios están aprovechando la naturaleza dinámica de la nube, la velocidad mejorada, la mayor colaboración, la elasticidad de los servicios, cosas que hacen que la nube sea atractiva, y están tomando medidas para incrementar esto, porque es perjudicial para ellos no hacerlo. Como profesionales de seguridad, tenemos que estar comprometidos y mostrar cómo la seguridad puede ser la base".

—Timothy Youngblood, Director de Seguridad de la Información de Kimberly-Clark

La migración hacia los servicios de nube citados por nuestros encuestados será tanto para despliegues de nube pública como privada. Según nuestra encuesta, la nube privada es actualmente el modelo de nube más dominante en las empresas, con 51% de sus despliegues en nube compuestos por nube privada. La nube pública representa el 30%, y la nube híbrida representa el 19% de los despliegues de nube empresarial. Cuando observamos cuántos meses tomará hasta que el 80% del presupuesto de TI de la organización sea asignado a los servicios de cómputo en nube, el plazo para la nube privada se reduce a sólo 15 meses.

Podemos ver evidencia de que la adopción de servicios nube está en el punto de inflexión. Las organizaciones están utilizando un promedio de 43 servicios en la nube ahora, aunque vale la pena señalar algunas variaciones regionales significativas (Figura 2). El Reino Unido, por ejemplo, es el más lento en términos de adopción de nube (un promedio de sólo 29 servicios en la nube por organización), mientras que las empresas brasileñas están entre los mayores usuarios de servicios nube (55 servicios en la nube por organización).

"Tenemos una filosofía de 'nube primero' en DocuSign, y estamos observando que muchos de nuestros clientes a lo largo de las industrias siguen el mismo abordaje. Es una conversación más larga con compañías de sectores muy regulados, como los servicios financieros y el cuidado de la salud. Las organizaciones de TI de estas compañías están en una posición muy difícil, porque sus reguladores requieren que se demuestre que todas las medidas de seguridad necesarias estén habilitadas antes de la implementación. Sienten una increíble presión para tomarse el tiempo para demostrar esto a los reguladores, pero al mismo tiempo sus negocios están presionando para ser más eficientes y más ágiles, y hacerlo todo más rápido".

—Vanessa Pegueros
Directora de Seguridad de la Información de DocuSign, Inc.

"Esté consciente de cuál información es apropiada para almacenar en la nube y cuál no lo es. Si hay información que sea valiosa para la compañía, entonces probablemente debería permanecer dentro de los límites del dominio de la compañía y permanecer en la nube privada".

—Eric Knapp, Director Global de Ciberseguridad de Honeywell

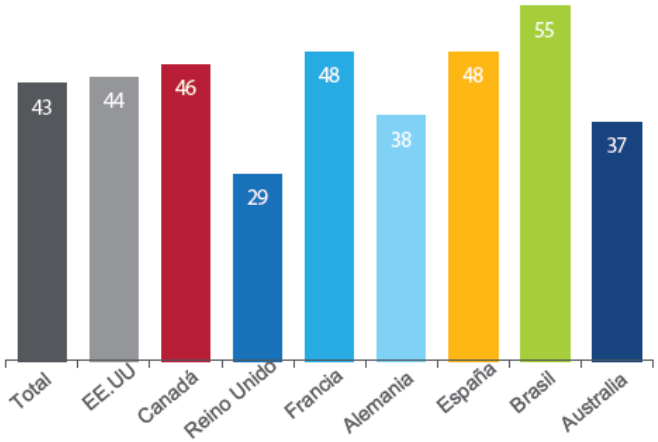

Figura 2. Número promedio de servicios de nube que las organizaciones están empleando actualmente, categorizados por país.

Por supuesto, también habrá diferencias en la tasa de adopción de diferentes tipos de plataformas de nube, pública, privada e híbrida o gestionada, así como SaaS, IaaS, PaaS. Anecdóticamente, también hay evidencia de que su adopción varía de un sector a otro. En sectores altamente regulados, como los servicios financieros, aún hay cautela acerca de trasladarse a la nube, y el gobierno y el sector público también van a la zaga.

Cuando observamos las tendencias de adopción de nube, es fácil caer en la trampa de hablar acerca de SaaS. De hecho, la encuesta revela que la mayoría de las organizaciones están planeando invertir en todos los modelos de servicio de nube, pero (tal vez sorprendentemente) el mayor porcentaje (81%) es en realidad para IaaS, en comparación con sólo el 60% de SaaS (Figura 3). Esto es seguido de cerca por la Seguridad como un Servicio (79%), e incluso las inversiones previstas en PaaS (69%) es mayor que en SaaS.

Eso está respaldado por el informe de SANS, que también muestra que IaaS será la mayor área de crecimiento para despliegues de nube empresarial durante el próximo año.

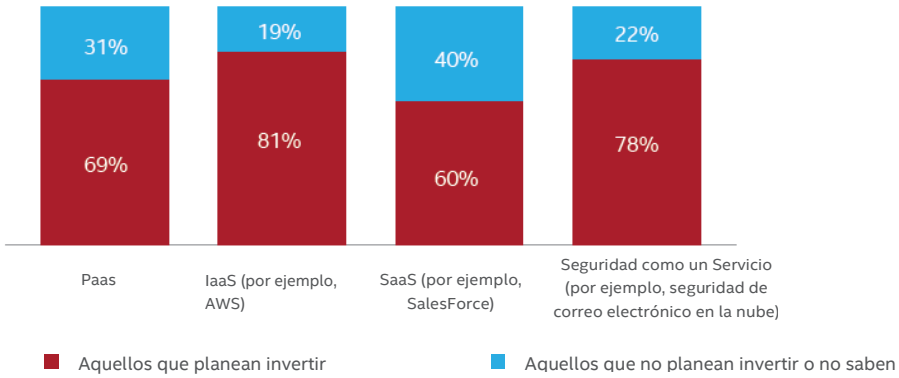

Figura 3. ¿En qué despliegue planea invertir su organización?

"La visibilidad hacia cómo opera el proveedor de servicios en nube y lo que realmente está sucediendo inhibe algunos de los análisis de riesgo y las decisiones de gestión de riesgo. Muchas regulaciones fueron hechas antes de la nube, suponiendo que una empresa tenía control total sobre la tecnología de cómputo, y con la nube eso ha cambiado".

—Jim Reavis, Director Ejecutivo de la Cloud Security Alliance

Seguridad y Conformidad: La Necesidad de una Mejor Visibilidad

¿Cuáles son las consecuencias de este aumento de la adopción de la nube para la seguridad empresarial? Podemos observar datos importantes y confidenciales adicionales alojados en la nube. Alrededor del 40% de los que respondieron a la encuesta de SANS, **Orquestando la Seguridad en la Nube**, dicen que procesan o almacenan datos confidenciales en la nube[1]. Los tipos más comunes de los datos almacenados en la nube son inteligencia de negocios (52%), contabilidad financiera (52%), registros de empleados (48%) e información personal de clientes (40%). De mayor preocupación son el 13% de las organizaciones que dijeron que no saben si tienen datos confidenciales en la nube. Muchos expertos de seguridad creen que esa cifra es mucho mayor, especialmente entre las empresas más grandes. Una razón para ello es que algunas organizaciones no quieren admitir que no saben, mientras que otras con operaciones y unidades de negocios que se extienden por todo el mundo, en realidad no saben si están expuestas de esta manera.

Mantener la conformidad en la nube es la mayor preocupación, en todos los tipos de despliegue de nube, de acuerdo al 72% de los encuestados en la encuesta SANS. El verdadero problema aquí tiene que ver con la visibilidad, siendo que más de la mitad (58%) de los encuestados de la encuesta SANS citaron la falta de visibilidad hacia las operaciones de proveedor de servicios nube como su mayor problema.

"Observamos preocupación con violaciones de datos. A menudo termina siendo un ataque a las credenciales del usuario quien tiene acceso legítimo al servicio en la nube, y la información se exfiltra de esa forma".

—Jim Reavis, Director Ejecutivo de la Cloud Security Alliance

¿Nubarrones en el Horizonte? Amenazas para el siglo XXI

Nuestro estudio sugiere que es tiempo de una re-evaluación de cuáles son las verdaderas amenazas para la nube, con la evidencia de una brecha entre la percepción y la realidad.

En la mayoría de los países, una de las tres preocupaciones principales del uso de SaaS son los incidentes contra la seguridad de los datos, según lo citado por más de uno de cada cinco encuestados (22%). Las violaciones de datos también son la principal preocupación para IaaS y las nubes privadas. Hay algunas diferencias regionales-más notablemente en Australia, donde el tiempo de inactividad es en realidad la principal preocupación.

Pero, ¿cuál es la realidad?

Cuando se les preguntó, más menos de una cuarta parte (23%) de los encuestados de las empresas en general, dijeron que en realidad sufrieron pérdida o violaciones de datos con sus proveedores de servicios de nube, y sólo uno de cada cinco sufrió acceso no autorizado a datos o servicios. La encuesta SANS muestra un nivel incluso inferior de violaciones de datos en la nube, siendo que sólo el 9% de los encuestados sufrieron un incidente en nubes públicas o en sus aplicaciones SaaS o de nube privada.

Los incidentes más comunes y los problemas que los encuestados tuvieron con los servicios de nube eran en realidad migración de servicios y datos, altos costos y valor deficiente o falta de visibilidad en las operaciones del proveedor de nube (Figura 4).

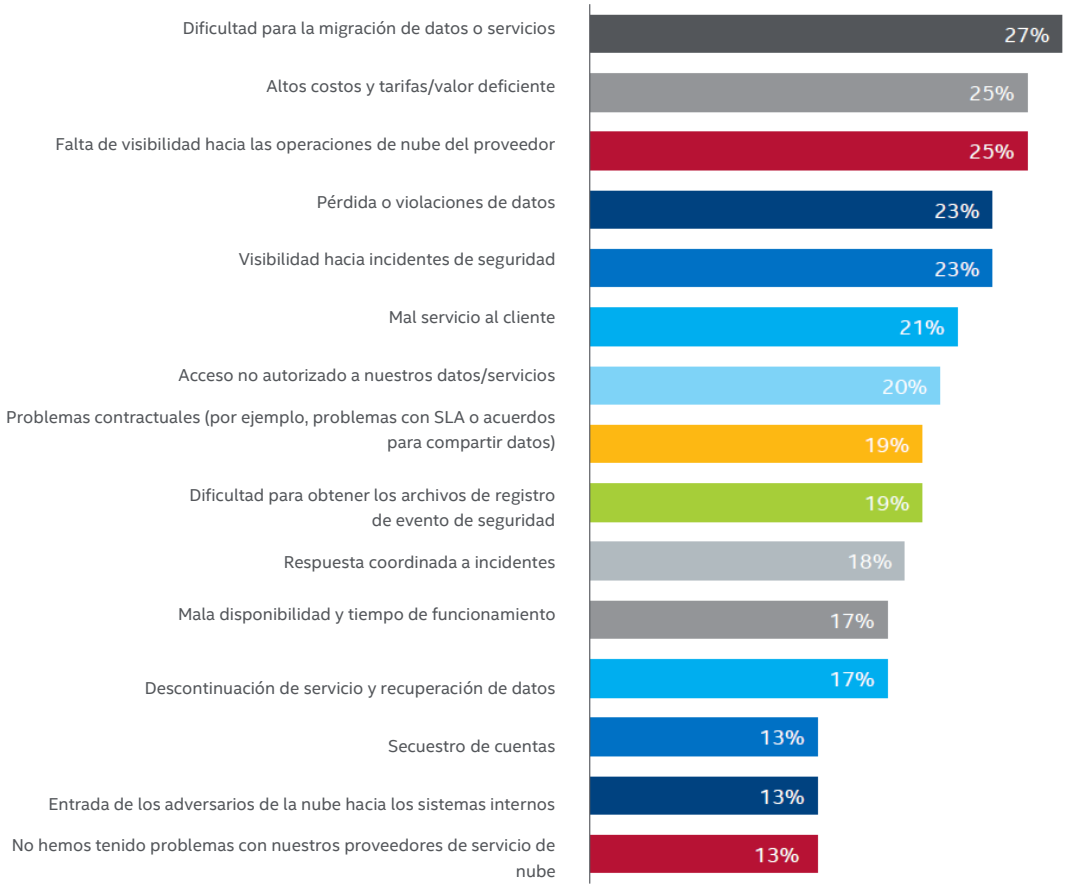

Figura 4. Con respecto a la seguridad de la nube, ¿qué problemas ha tenido su organización con los proveedores de servicios de computación en nube?

"Las empresas deben incorporar la seguridad en DevOps y los dos elementos más importantes son el monitoreo continuo y la detección de cambios".

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

Cuando observamos las amenazas de seguridad concretas para la nube identificadas por los encuestados, el malware y los botnets son el problema principal para despliegues de nube privada (33%), mientras que los ataques de denegación de servicio se perciben como la principal amenaza para las nubes públicas (36%).

Otros riesgos de seguridad para la nube surgen potencialmente a través de la rápida escalación hacia arriba o hacia abajo de los servicios, aunque se trata más de un problema de disponibilidad y continuidad de negocios para el que las empresas necesitan planificar. Otra característica clave de la adopción de la nube es el ascenso de DevOps, los ciclos cada vez más rápidos de desarrollo de aplicaciones, pruebas y despliegue. Incorporar una seguridad robusta en ese entorno de desarrollo continuo es vital para mantener un seguimiento de esos cambios rápidos y ser alertado de los posibles riesgos para la seguridad asociados con ellos.

Evidentemente, no debemos saltar a la conclusión con base en los resultados de la encuesta de que las violaciones de datos en la nube no son una grave amenaza para la seguridad o que nunca sucederán. Debemos considerar la posibilidad de que no se informen completamente las violaciones de datos a las agencias de seguridad pública o reguladores. Y por supuesto, cuando se producen violaciones de datos en la nube, las consecuencias son frecuentemente significativas. Mientras que la brecha entre la percepción de las amenazas para la seguridad en la nube y la realidad necesita ser cerrada en cierta medida, la encuesta sugiere que la inversión y la planificación en torno a la mitigación de los riesgos de violaciones de alto perfil debe estar equilibrada con algunas de las más comunes amenazas cotidianas para los sistemas y datos de la empresa en la nube. Estas incluyen problemas de migración, servicio al cliente deficiente y problemas contractuales, así como amenazas para la seguridad concretas tales como denegación de servicio, malware y hackeo de cuentas.

"Los Consejos Directivos y los ejecutivos C-suite están reconociendo ampliamente que la seguridad en la nube es un elemento fundamental de cualquier negocio y debe ser tomada en serio".

—Vanessa Pegueros Directora de Seguridad de la Información de DocuSign, Inc.

Seguridad de Nube y Riesgo: Punto Ciego de C-Suite

Nuestro estudio muestra un alto nivel de participación en la toma de decisiones de seguridad en la nube de altos ejecutivos, no solo del Director de TI, del CIO y del CISO, sino también con frecuencia del CEO y del CFO.
Sin embargo, ¿los directivos comprenden plenamente los riesgos de seguridad?

Cuando se trata de nubes públicas, parece existir una brecha perturbadora en la conciencia de las implicaciones de seguridad de almacenar datos confidenciales en la nube pública por parte de los consejos de administración. (Ver Figura 5). Sólo el 34% de los encuestados opinaron que sus altos directivos entienden plenamente las implicaciones, mientras que uno de cada cinco dice que los ejecutivos de nivel C no tienen ni idea ni comprenden en parte esos riesgos. Existe una brecha aún más pronunciada en el Reino Unido, donde sólo el 15% cree que la alta gerencia en su organización comprende totalmente los riesgos de almacenar datos en la nube pública. Compárese eso con Brasil (49%) y Australia (47%), donde el conocimiento es mucho más alto entre los miembros del consejo de dirección.

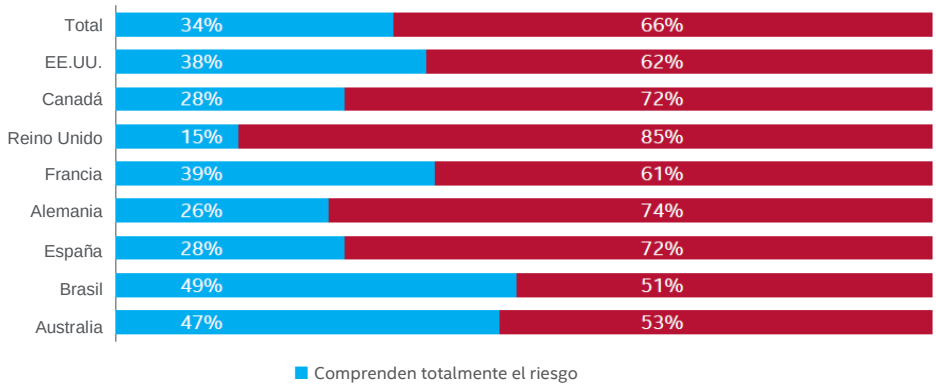

Figura 5. ¿Cree que sus altos directivos y ejecutivos comprenden las implicaciones de seguridad al almacenar datos confidenciales en la nube pública?

"La educación es poder. Contamos con un intenso programa de generación de conciencia en relación a la seguridad, que se enfoca en capacitar a todos nuestros empleados sobre el valor de la información. Es lo que llamo un 'firewall humano'".

—Timothy Youngblood, Director de Seguridad de la Información de Kimberly-Clark

Mientras que las violaciones de datos de alto perfil y las consecuencias financieras y de reputación han hecho que la seguridad de los datos sea una preocupación primordial para muchos Directores Ejecutivos y ejecutivos C-suite, nuestro estudio sugiere que todavía hay la necesidad de una mayor educación para aumentar la conciencia y comprensión de los riesgos asociados con el almacenamiento de datos confidenciales en la nube.

TI Oculta: ¿Riesgo u Oportunidad?

La mayoría de los encuestados que respondieron nuestra encuesta dicen que la TI oculta tiene un impacto negativo sobre la capacidad de su organización para mantener los servicios de nube seguros, y un 11% de las compañías de servicios financieros indicaron que deja a sus organizaciones expuestas a riesgos significativos.

Brindar seguridad a la TI oculta sigue siendo un desafío importante: El 52% de las líneas de negocio aún esperan que TI brinde seguridad a sus servicios de nube no autorizados obtenidos por su departamento. Además, casi un cuarto de los encuestados (23%) dicen que estos departamentos obtienen su propia seguridad sin la ayuda de TI.
La visibilidad sobre la TI oculta de los departamentos es generalmente mayor para SaaS que para IaaS. Sin embargo, al menos una quinta parte de los encuestados no saben si la TI oculta se presenta en todos los departamentos a lo largo de sus organizaciones. Los niveles de TI oculta son más altos en el departamento de ventas, R&D, y marketing. La mayor interrogante se cierne sobre el departamento legal, Aproximadamente 37% de los encuestados no puede decir si el departamento está adquiriendo nube sin el conocimiento del departamento de TI.

.

"La TI oculta es la nueva TI. El viejo modelo ha desaparecido. Cuanto más luchamos contra ella, más desviamos nuestro enfoque en trabajar para brindarle seguridad. Nosotros necesitamos aceptar que la TI oculta es hoy una realidad y debemos enfocar nuestra energía en gestionarla de forma segura".

—Vanessa Pegueros
Directora de Seguridad de la Información de DocuSign, Inc.

¿Cómo están lidiando las organizaciones con la TI oculta? Los métodos más comunes son

- Monitoreo de actividad de base de datos (49%).
- Firewalls de próxima generación (41%).
- Gateways da Web (37%).

Existe una notable brecha en cómo tratar con la TI oculta cuando es descubierta. Casi la mitad de los encuestados (46%) bloquean el acceso, mientras que el 37% migran la TI oculta hacia un servicio autorizado.

¿Crece la Confianza en la Nube?

A primera vista, las cifras principales de nuestra encuesta muestran un nivel relativamente bajo de confianza en la computación en nube frente a TI en las instalaciones o alojada internamente. No es de extrañar que la nube pública es la menos confiable del modelo (Figura 6).

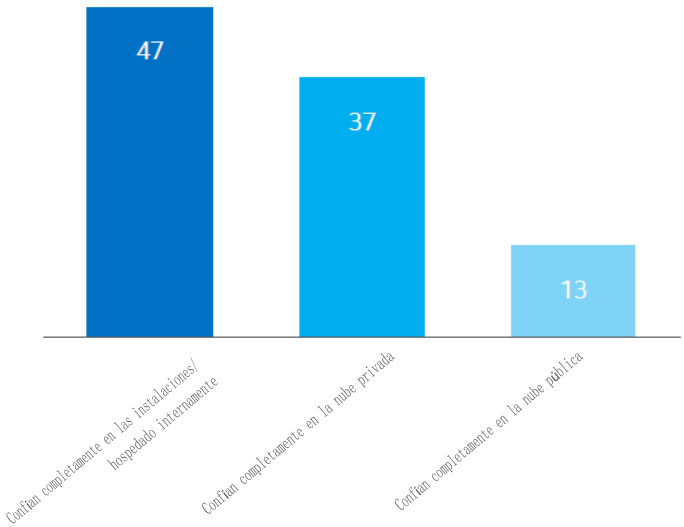

Figura 6. "¿Hasta qué punto se puede confiar en los siguiente para mantener la información confidencial de su organización segura?"

"La gente simplemente está tratando de hacer su trabajo Si no podemos proporcionarlo, lo obtendrán en otra parte. La TI y el Director de Informática deben ser los intermediarios y adoptar la nube y los servicios SaaS".

—Brent Conran,
Vicepresidente y Director de Seguridad de la Información de Intel

Más significativamente, el panorama general muestra un nivel de crecimiento general de la confianza en la computación en nube durante el pasado año, el 77% de las empresas dicen que su organización confía en el cómputo en nube más ahora, que hace un año (Figura 7).

"Viene una nueva era para los proveedores de nube. Estamos en un período de transición, pero creo que estas nuevas disposiciones normativas ayudarán a la inversión y a la confianza, así que deberíamos sentirnos más cómodos con los servicios en la nube".

—Dimitra Liveri, Director de Redes y Seguridad de la Información de la Red Europea y Agencia de Seguridad de la Información (ENISA)

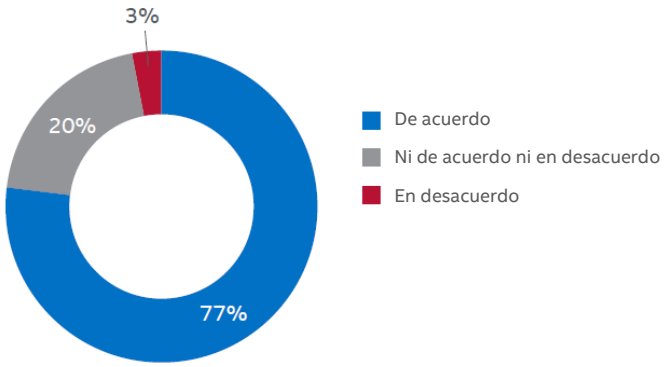

Figura 7. Quienes están de acuerdo con la afirmación "Mi empresa confía en la computación en nube más ahora que hace 12 meses".

Con dos regulaciones significativas en espera de una votación por la Comisión Europea, 2016 promete ser un gran año para los proveedores y usuarios de la nube de Europa. Las regulaciones son el Reglamento de Protección de Datos General de la Unión Europea y la Directiva de Seguridad de Información de las Redes. ¿Eso ayuda a reforzar la confianza en la seguridad de la nube? Los expertos creen que sí.

Prioridades de Inversiones en Seguridad de Nube

Las prioridades de inversión en seguridad varían entre los diferentes tipos de despliegues de nube. Las compañías están utilizando un promedio de tres soluciones de seguridad para proteger sus aplicaciones SaaS. La más común es el cifrado de archivos (60%), seguida por seguridad de correo electrónico (55%).

Para IaaS, las organizaciones están utilizando un promedio de cuatro soluciones de seguridad. Las más comunes son: firewalls (70%) y el cifrado (62%). La nube privada también tiene un promedio de cuatro soluciones de seguridad, con el firewall siendo la más común (67%).

Las cuatro principales áreas de Seguridad como un Servicio en que las organizaciones planean invertir son las mismas en las que ya están invirtiendo: protección de correo electrónico, protección Web, anti-malware, y firewall de aplicaciones (Figura 8). Esta tendencia indica que las empresas están planeando mejorar y ampliar los servicios de seguridad basados en nube que ya tienen implementados.

La encuesta de SANS también destaca algunas áreas clave para la inversión en seguridad de nube durante los próximos 18 meses. Estas incluyen análisis de vulnerabilidad, autenticación multifactor, prevención de pérdida de datos, gestión de registros, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), seguridad de la información y gestión de eventos (SIEM) y servicios de intermediación de acceso a la nube (CASBs).

"El primer punto de partida para la seguridad de la empresa en la nube pública es preguntar: ¿cuáles son los límites de responsabilidad? ¿Qué, como empresa, es capaz de controlar plenamente frente a lo que el proveedor de nube está obligado a gestionar? Y usted necesita evaluar los controles en todo el espectro de seguridad incluyendo seguridad de datos, gestión de identidad y aplicación de políticas. Habrá cosas que simplemente ya no podrá controlar, especialmente a nivel de red".

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

Según el informe de Gartner, *Market Guide for Cloud Access Security Brokers*, los CASBs en particular son una zona de alto crecimiento. Gartner predice que, "para 2020, el 85% de las grandes empresas utilizará un producto intermediador de seguridad de acceso a la nube para sus servicios en la nube, que es de menos del 5% en la actualidad[2]". Nuestra encuesta respalda esta afirmación. A pesar del hecho de que los CASBs son un servicio relativamente nuevo, el 36% de las empresas utilizan estos servicios para proteger sus aplicaciones SaaS y el 32% utilizan estos servicios para monitorear las implementaciones de nube adquiridas mediante TI oculta. Casi una cuarta parte (24%) de las empresas también planean invertir en un CASB como un Servicio en el futuro.

"Comprender lo que está sucediendo en su entorno en nube, por ejemplo entre el usuario base y Salesforce - es realmente crítico, y las herramientas que nos permiten gestionar de forma más segura que son algo que buscaré mucho más. También necesitamos herramientas que ayuden a automatizar procesos como respuesta a incidentes y nos permitan hacer más con lo que tenemos actualmente".

—Vanessa Pegueros
Directora de Seguridad de la Información de DocuSign, Inc.

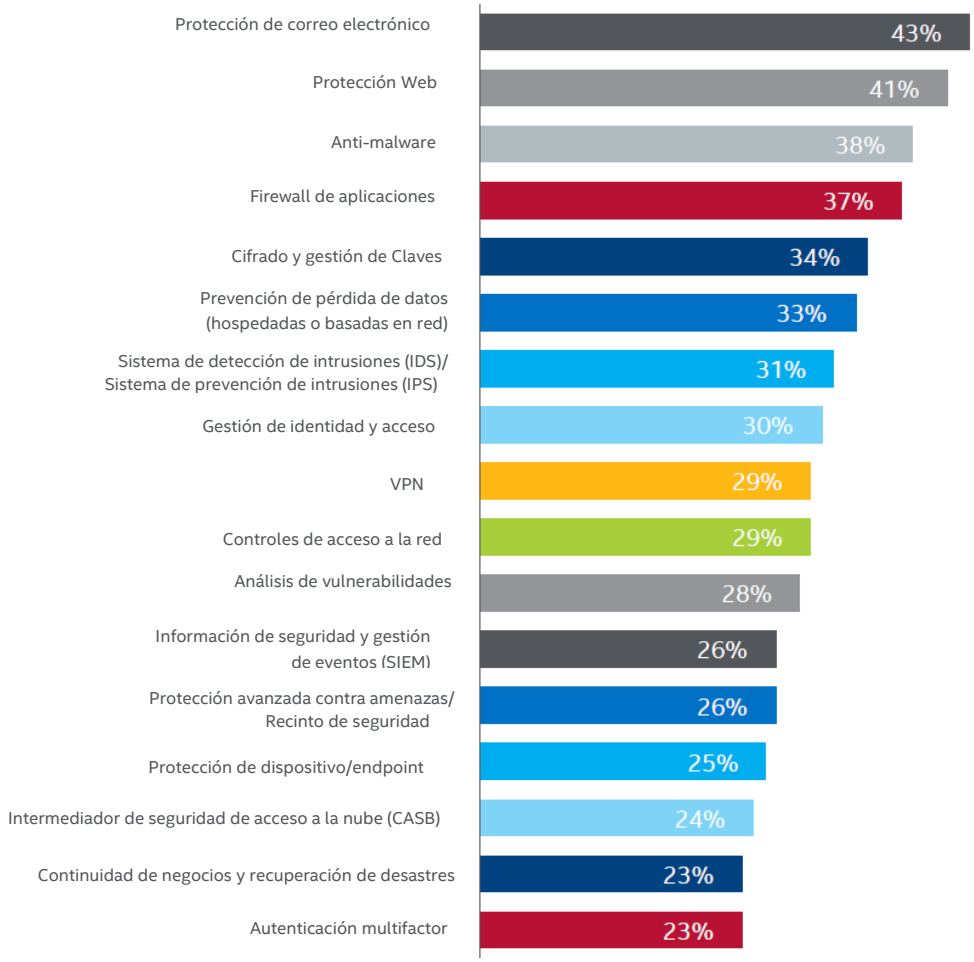

Figura 8. ¿En qué áreas de seguridad como servicio planea invertir su organización?

De esas organizaciones que utilizan un servicio de nube pública, poco más de una tercera parte (34%) dicen tener una solución unificada con integración completa y gestión central a lo largo de su nube híbrida y sistemas en sus instalaciones. Así que hay margen de mejora aquí.

Resumen

La adopción de la nube en la empresa se aproxima rápidamente a un punto de inflexión, siendo que las organizaciones indican que el 80% de su presupuesto de TI será consumido por la nube en 16 meses o menos.

Existen muchos incentivos persuasivos que impulsan a los negocios hacia la nube, incluyendo una mayor agilidad, innovación más rápida y eficiencia de costos. Sin embargo, con esa gran variedad de opciones de despliegue de nube, existen desafíos de seguridad inherentes. Debido a que la nube es o será el repositorio de tantos datos corporativos vitales, las organizaciones deben considerar lo siguiente:

- Los controles de seguridad y la conformidad son responsabilidades compartidas entre las empresas y proveedores de servicios de nube. Pregunte a su proveedor de servicios acerca de sus controles de seguridad y asegúrese de que los informes estén incluidos en su acuerdo de nivel de servicio (SLA). Sin embargo, es esencial para la empresa dar seguridad a lo que está bajo su control en la nube, ya sea datos, aplicaciones o cargas de trabajo, y construir esto en sus planes de arquitectura de nube.

"Aunque haya externalizado y esté utilizando la nube, usted no ha externalizado su responsabilidad. Usted no puede decir "Hey, esa fue la culpa de Amazon'".

—Brent Conran, Vicepresidente y Director de Seguridad de la Información de Intel

- Las áreas claves para la inversión en seguridad nube incluyen cifrado de datos, gestión de identidad y acceso, prevención de pérdida de datos, y protección de correo electrónico. Cada vez más, las organizaciones también están invirtiendo en Seguridad como un Servicio y otras herramientas que pueden ayudar a organizar la seguridad a lo largo de múltiples proveedores y entornos, más notoriamente CASBs.
- Aunque los despliegues de nube de TI oculta siguen siendo un desafío, ya que potencialmente puede exponer los datos de la compañía a un mayor riesgo, las organizaciones de TI deben trabajar con las unidades de negocios para encontrar una forma más segura para permitir a los usuarios a implementar sus propios despliegues de nube. TI puede recuperar el control y la visibilidad al ser el intermediario y redirigir a los usuarios de negocios hacia alternativas de servicio de nube más seguras.
- Aunque muchos consejos de administración están involucrados en la toma de decisiones de seguridad en la nube, siempre hay espacio para mejorar el conocimiento y la comprensión de los riesgos implicados. Se necesita más educación, así como una mayor participación de los CIO y CISO en las discusiones con otros ejecutivos de alta dirección. Las consecuencias económicas y daños a la reputación sufrido por las organizaciones en algunas violaciones de datos ampliamente divulgadas, deben ser un incentivo para que ejecutivos de alto nivel primaren por la seguridad de datos, internamente o en la nube.

Metodología

La encuesta aplicada a 1.200 responsables de la toma de decisiones de TI con la responsabilidad de la seguridad en la nube en sus organizaciones, fue realizada por Vanson Bourne en junio de 2015. Los encuestados procedían de Australia, Brasil, Canadá, Francia, Alemania, España, el Reino Unido y los Estados Unidos, y pertenecían a diversas organizaciones, desde aquellas con 251 a 500 empleados a aquellas con más de 5.000 empleados.

Acerca de Intel Security

McAfee ahora forma parte de Intel Security. Con su estrategia de Seguridad Conectada, abordaje innovador hacia la seguridad del hardware mejorada, y su Global Threat Intelligence único, Intel Security se enfoca intensamente en desarrollar soluciones y servicios de seguridad proactivos y comprobados que protegen sistemas, redes, y dispositivos móviles de uso de negocios y personal en todo el mundo. Intel Security combina la experiencia y pericias de McAfee con la innovación y desempeño comprobado de Intel para hacer de la seguridad un ingrediente esencial en cada arquitectura y en cada plataforma de cómputo. La misión de Intel Security es la de brindar a todos la confianza de vivir y trabajar con seguridad en el mundo digital. **www.intelsecurity.com**

1. *SANS: Orchestrating Security in the cloud* por Dave Shackleford, septiembre de 2015 (patrocinado por Intel Security)
2. Gartner Report, *Market Guide for Cloud Access Security Brokers*, por Craig Lawson, Neil MacDonald y Brian Lowans, 22 de octubre de 2015

McAfee. Parte de Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766.
www .intelsecurity .com