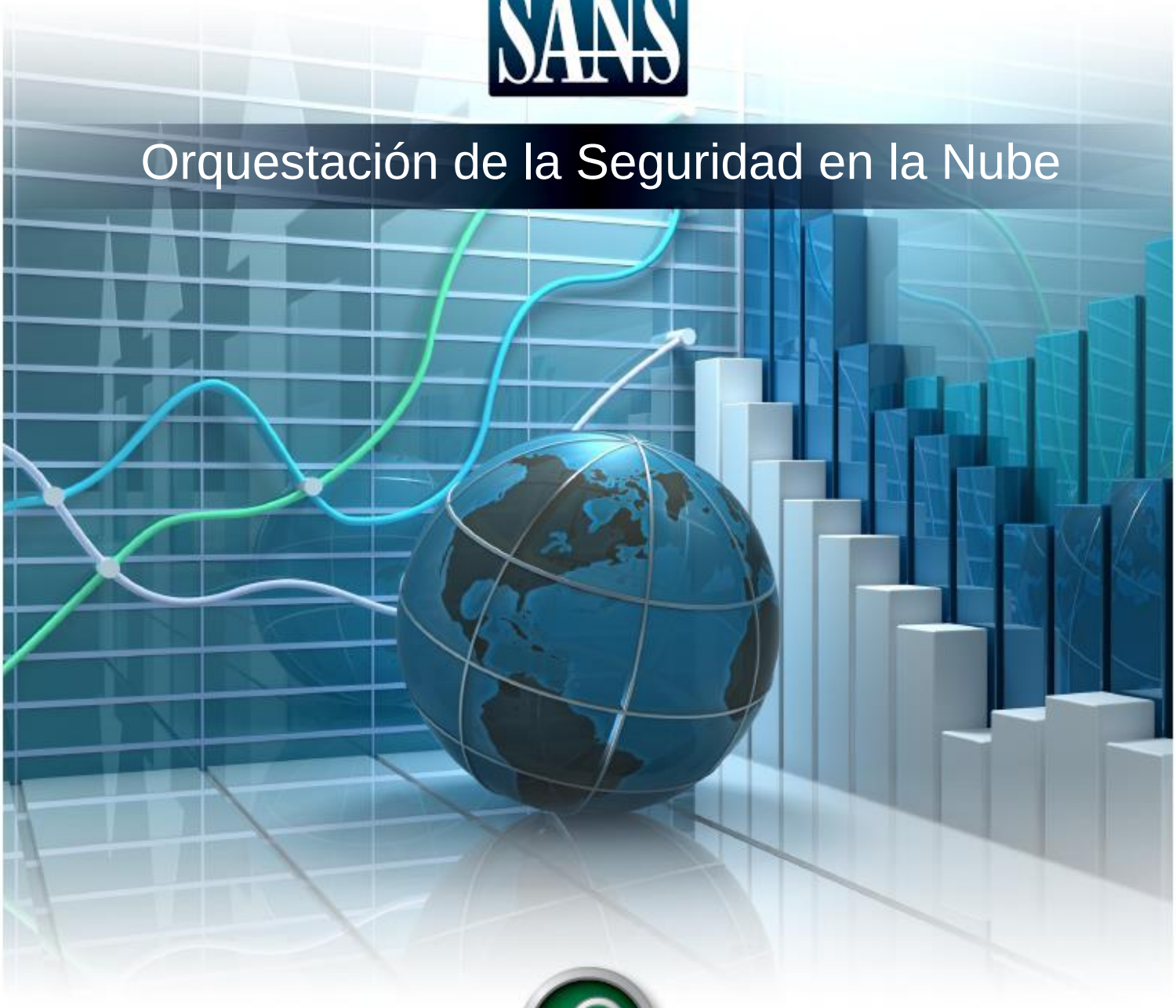
Orquestación de la Seguridad en la Nube



Una encuesta de SANS

Escrita por Dave Shackleford

Septiembre de 2015

Patrocinada por Intel Security

Resumen Ejecutivo

Los servicios de colaboración, correo electrónico, servicios gestionados, copias de seguridad y recuperación de desastres, representan los casos de uso actuales más comunes de los servicios en la nube, según los resultados de una nueva encuesta de SANS sobre seguridad en la nube. Los 485 profesionales de TI que participaron en la encuesta afirmaron utilizar diversos proveedores de nube y modelos de servicio, incluyendo ofertas de nube de software como servicio (SaaS), junto con una mezcla bastante homogénea de implementaciones en infraestructura como servicio (IaaS) y plataforma como servicio (PaaS). La mayoría de los encuestados dijeron que están invirtiendo tanto en nubes públicas como en privadas según las necesidades.

Descubrimientos Claves

de los encuestados almacenan o procesan datos confidenciales en la nube

citaron el acceso no autorizado a los datos confidenciales de otros inquilinos como la preocupación más apremiante con despliegues de nube pública

no tienen suficiente visibilidad actualmente de las operaciones de nube pública de sus proveedores

de la organizaciones que han sufrido brechas en la nube citaron el malware como el principal vector de ataque en la nube privada, mientras que 36% dijeron que DoS es el principal vector de ataque en la nube pública

Sin embargo, aunque los servicios en nube proporcionan la funcionalidad que los negocios necesitan, también vienen con un aumento de los riesgos de seguridad, particularmente dado que 40% de los encuestados dijeron que procesan datos confidenciales en la nube. Las preocupaciones incluyen la falta de control sobre el acceso a los datos, ubicación geográfica de datos confidenciales, conformidad, y visibilidad de controles de seguridad incorporados en los entornos de nube pública e híbrida de la organización.

Junto con estos problemas, más del 27% de los encuestados dijeron que tienen poco o ningún soporte de respuesta a incidentes dentro de sus implementaciones de nube pública, citando una letanía de problemas, incluyendo la incapacidad para determinar quién es el responsable de la seguridad y la conformidad en la nube y cómo implementar y evaluar controles de seguridad.

En general, los resultados de la encuesta indican una fuerte necesidad de mantener una estrecha seguridad de los datos a medida que atraviesan los sistemas de nube, no sólo a través de sistemas de cifrado, sino también mediante el control de permisos y accesos. Los resultados también indican la necesidad de las organizaciones para integrar capacidades de monitoreo a lo largo de sus entornos híbridos y asociaciones con proveedores de nube pública, para obtener plena visibilidad del espectro completo y respuesta.

Estos y otros puntos destacados de la encuesta se cubren en el siguiente informe.

Estado de la Computación en Nube

NUBE HÍBRIDA
Una infraestructura que vincula implementaciones de nube privada (ejecutada por la empresa) y pública para obtener ventajas comerciales, pero los segmentos siguen siendo entidades separadas

Nube Pública
Una infraestructura que normalmente se gestiona por un tercero en donde el espacio está disponible para varios inquilinos que comparten recursos

NUBE PRIVADA
Una aplicación, disponible en las instalaciones o como un segmento de nube pública, que proporciona recursos y entornos de cómputo separados para diferentes inquilinos

Debido a su flexibilidad y ahorro de costos, cada vez más organizaciones están trasladando las cargas de trabajo hacia la nube más que nunca. Según Forrester Research, "En 2015 la adopción de la nube se acelerará y los grupos de gestión de tecnología deben adaptarse a esta realidad aprendiendo cómo añadir valor al uso por parte de su compañías de estos servicios a través de facilitación, adaptación y promoción"[1]

Arquitecturas

Las nubes están siendo desarrolladas para dar soporte a muchos tipos de servicios de negocios utilizando una amplia gama de arquitecturas. Las arquitecturas de nube híbrida son los más comúnmente utilizadas entre los encuestados, siendo que 40% de ellos las han desplegando actualmente y 43% planean avanzar en esa dirección durante los próximos 12 meses. Las implementaciones de nube privada están cerca, con 38%, mientras que 12% utilizan implementaciones de nube pública. Ver Figura 1.

¿Clasificaría el modelo de computación en nube actual de su organización como fundamentalmente público, privado o híbrido? ¿Prevé que este sea el caso para los próximos 12 meses?
Seleccione la respuesta más apropiada

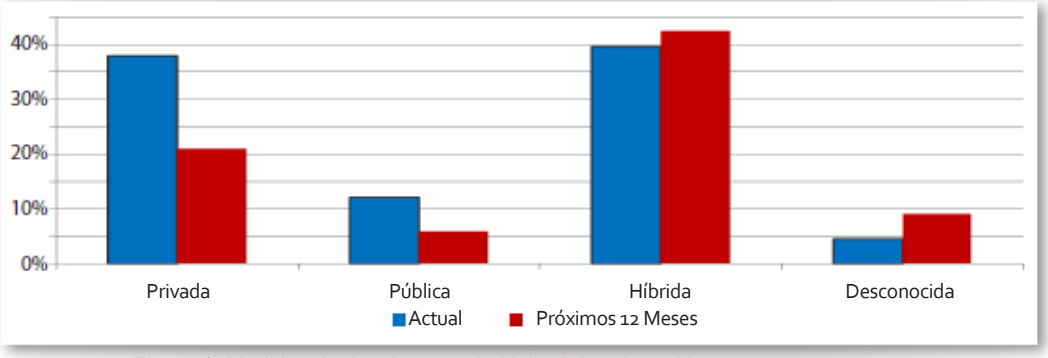


Figura 1. Modelos de Arquitectura de Nube Primaria en Uso

Algunas estrategias de nubes privadas y públicas están planificadas para los próximos 12 meses, pero la gran mayoría de los encuestados parecen equilibrar los recursos internos y de nube pública.

[1] http://whatsthebigdata.com/2014/12/02/top-2015-it-predictions-from-forrester-research

Cargas de Trabajo de Negocios en la Nube

Los encuestados están pasando una gran variedad de cargas de trabajo hacia los entornos de proveedor de servicios de nube: 47% utilizan actualmente servicios de colaboración como compartir archivos y calendarios, 45% utilizan servicios de mensajería y correo electrónico, y 29% utilizan servicios gestionados basados en la nube. Durante los próximos 12 meses, 24% planean utilizar servicios de colaboración en la nube, 23% usarán servicios de copia de seguridad y recuperación de desastres basados en la nube, y 22% están buscando implementar servicios de mensajería y correo electrónico. El desglose completo de los despliegues de cargas de trabajo actual y previsto se ilustra en la Figura 2.

Porcentaje de los encuestados que esperan tener servicios de colaboración en la nube dentro de los próximos 12 meses

Porcentaje de encuestados que planean tener herramientas de correo electrónico y mensajería en la nube durante los próximos 12 meses

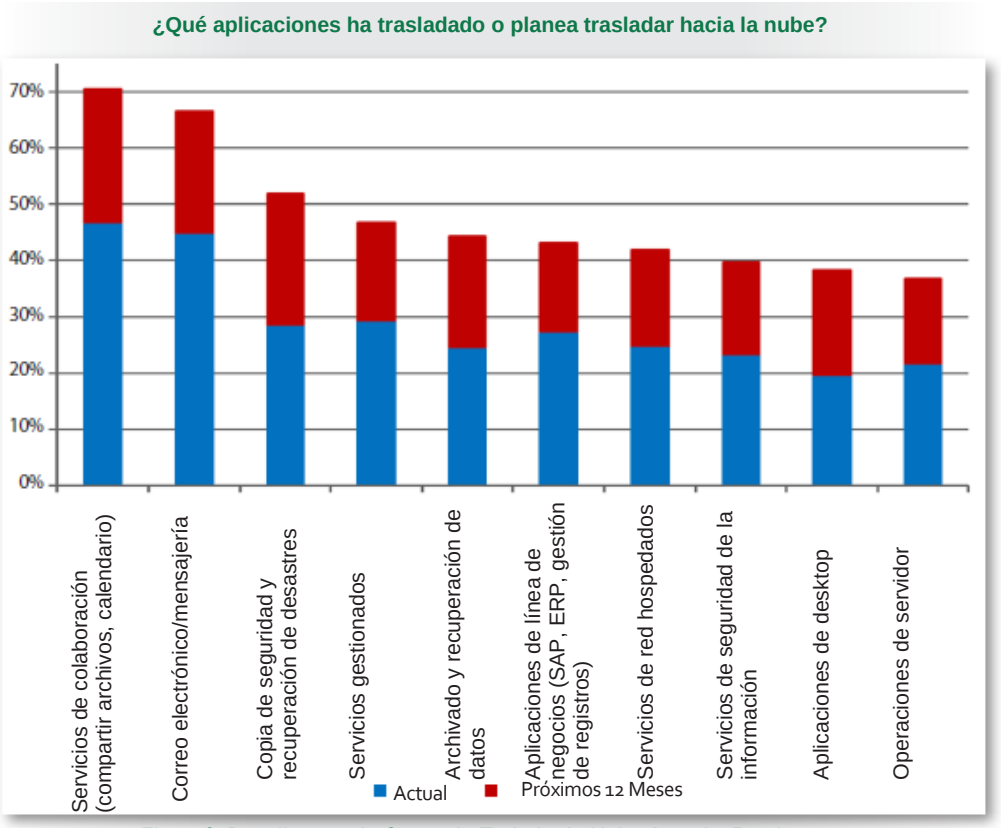


Figura 2. Despliegues de Carga de Trabajo de Nube Actual y Prevista

Los resultados muestran, cómo los encuestados del estudio de SANS están utilizando una increíblemente amplia mezcla de servicios, en particular herramientas de mensajería y colaboración, siendo que más del 60% indican que ellos tienen o tendrán estos servicios en la nube durante los próximos 12 meses. Las cargas de trabajo de nube previstas para implementación en los próximos 12 meses se distribuyen de manera más uniforme pero aún varían ampliamente. Otras aplicaciones clave que los encuestados piensan trasladar hacia la nube incluyen aplicaciones de archivado y recuperación de datos, citadas por 20%, seguidas por las aplicaciones de desktop, servicios gestionados, servicios de red hospedados y servicios de seguridad de la información, con 19%, 18%, 17% y 16%, respectivamente.

Cada una de estas aplicaciones implica el procesamiento o el almacenamiento de información confidencial dentro del entorno de la nube del proveedor, incluyendo datos de seguridad y red que se pueden utilizar para irrumpir en la red física. La prevención de la explotación a lo largo de estas aplicaciones y sus correspondientes superficies de ataque, es ahora una meta clave de soporte para los grupos de seguridad con cualquier tipo de operación dinámica basada en nube.

Impulsores de Negocios

Existen diversos impulsores de negocios para la adopción de los servicios de nube hoy, pero estos varían dependiendo de la organización. La investigación de KPMG descubrió que los ejecutivos se enfocan fundamentalmente en la transformación y el desempeño del negocio, seguidos por la agilidad y los ahorros[2].

Los encuestados en el estudio de SANS hicieron eco de esas prioridades, siendo que 61% citaron un menor tiempo de despliegue como su principal impulsor y 54% dijeron que utilizan servicios en la nube porque ellos no pueden escalar sus propias soluciones. Además, 48% dijeron que necesitan una manera central de gestionar la conformidad. Ver Figura 3.

¿Cuáles son sus tres principales motivadores para trasladar cargas de trabajo y aplicaciones hacia la nube?

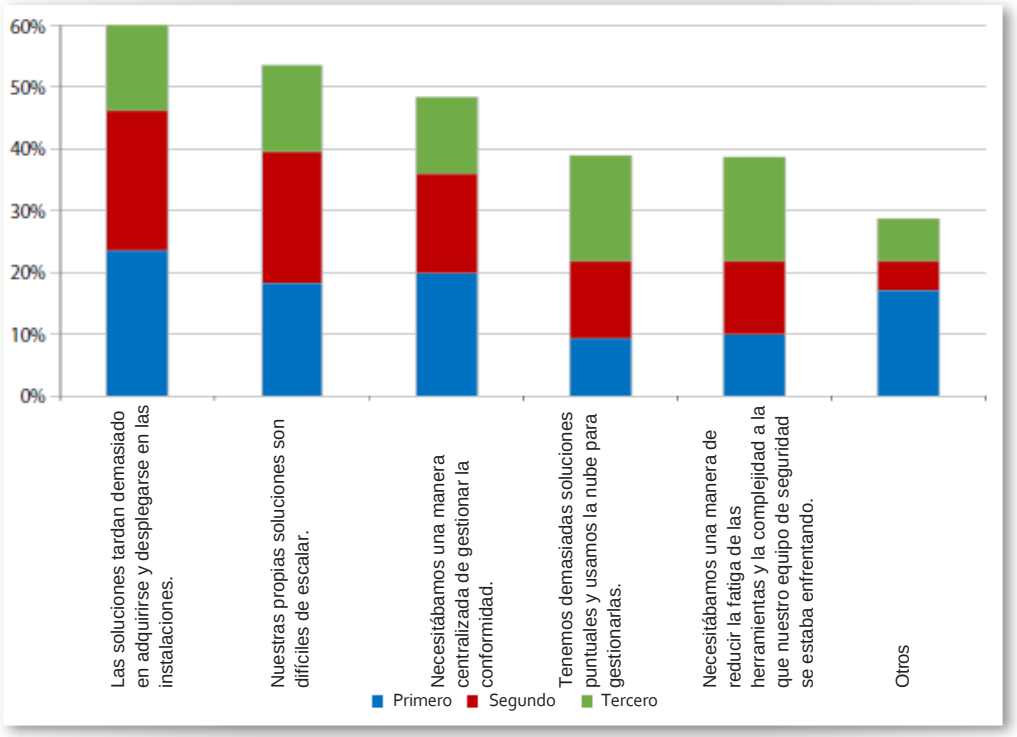


Figura 3. Motivos para el Despliegue de Nube

[2] www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014 KPMG Cloud Survey Report - Final 12-10-14.pdf

Las adiciones a la lista de motivadores para despliegues de nube incluyen ahorros, disponibilidad y facilidad de uso. Tomados en conjunto, los resultados indican que el modelo de nube híbrida, impulsado por las exigencias de los negocios, está aquí para quedarse. Esta tendencia marca un fuerte crecimiento para los profesionales de seguridad de TI que deseen especializarse en la nube y los proveedores que desarrollan herramientas para integrar acceso, protección de datos, monitoreo y visibilidad, así como inteligencia de protección a lo largo de estos sistemas, plataformas y proveedores.

Modelos de Uso

Porcentaje de los encuestados que esperan desplegar un entorno SaaS dentro de los próximos 12 meses

Actualmente, el 59% de las empresas están utilizando ofertas de software como servicio (SaaS), muy probablemente por las herramientas de mensajería y colaboración, como se destacó anteriormente. Los sistemas de máquina virtual (VM) y las cargas de trabajo de aplicaciones también se están desplegando hoy en entornos de infraestructura como servicio (IaaS) y plataforma como servicio (PaaS). Ver Figura 4.

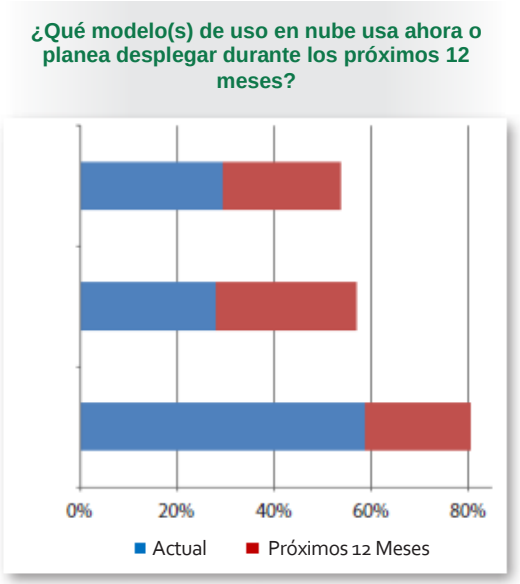


Figura 4. Modelos de Nube Actual y Previsto

Durante los próximos 12 meses, 29% de los encuestados dijeron que planean desplegar un entorno IaaS, haciendo de esta la mayor área de crecimiento pronosticado. Las razones para trasladarse hacia PaaS y IaaS no son diferentes de las razones para los despliegues SaaS: la velocidad y la escalabilidad, junto con los servicios adicionales que los proveedores de nube puede ofrecer. Muchas organizaciones están buscando reducir el tamaño total y la presencia de sus centros de datos internos, por lo tanto, migrar instancias de sistema hacia la nube tiene sentido.

En la encuesta de KPMG citada anteriormente[3], los CIOs y los ejecutivos de negocios indicaron por igual que están muy enfocados en la seguridad y privacidad de los datos, así como en los riesgos del robo de propiedad intelectual a la hora de evaluar a los proveedores de nube hoy en día, y por una buena razón. 40% de los encuestados por SANS indicaron que almacenan o procesan datos confidenciales en sus entornos de nube pública hoy, mientras que 13% dijeron que no saben si tienen datos confidenciales en la nube.

[3] www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014 KPMG Cloud Survey Report - Final 12-10-14.pdf

Estado de la Computación en Nube (CONTINUACIÓN)

TEMA IMPORTANTE:

Siempre que sea posible, adoptar medidas para proteger los datos que se envían en el entorno nube- en tránsito, en reposo y en uso

La inteligencia de negocios y la información financiera y contable son los tipos más comunes de datos que los encuestados están almacenando o procesando en la nube, cada uno reportado por 52% de los encuestados, Otros 48% almacenan o procesan registros de empleados, y el 40% almacenan información personal de los clientes. Ver Figura 5.

¿Qué tipo de información confidencial está almacenando o procesando en la nube pública?

Seleccione todo lo que aplique.

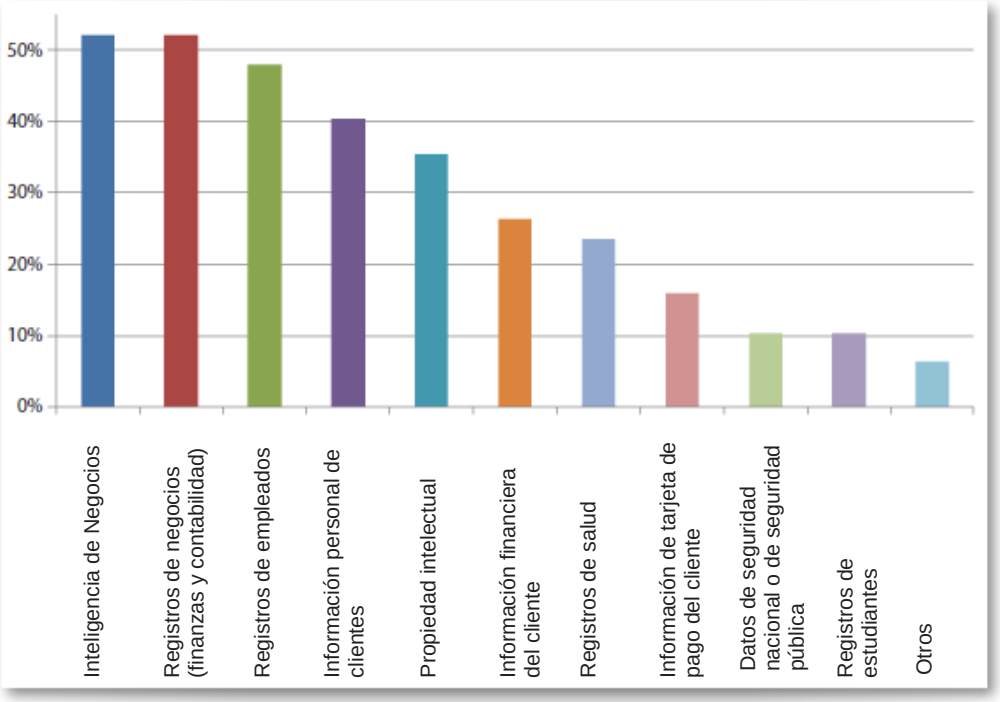


Figura 5. Datos Confidenciales Almacenados o Procesados en la Nube

Estado de la Computación en Nube (CONTINUACIÓN)

Al menos el 20% de los encuestados dijeron que también están usando la nube para almacenar o procesar propiedad intelectual, información financiera de clientes y registros de salud. Con todos estos diferentes tipos de datos sensibles representados hoy en los entornos de nube, las organizaciones deben cumplir con diversos mandatos de conformidad regulatoria y de la industria: El 49% de los encuestados dijeron que deben cumplir con los requisitos de los Estándares de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), 39% mencionaron la conformidad con Sarbanes-Oxley (SOX), y 37% deben cumplir con los mandatos de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA). El desglose completo de los mandatos de conformidad a los que se deben adherir los encuestados se muestra en la Figura 6.

TEMA IMPORTANTE:

Las organizaciones deben evaluar cuidadosamente los tipos de datos confidenciales que almacenan en la nube y si pueden satisfacer los requisitos de conformidad relacionados en los entornos de los proveedores de SaaS, PaaS e IaaS.

¿Cuáles son las normas o estándares aplicables que debe cumplir?
Seleccione todo lo que aplique

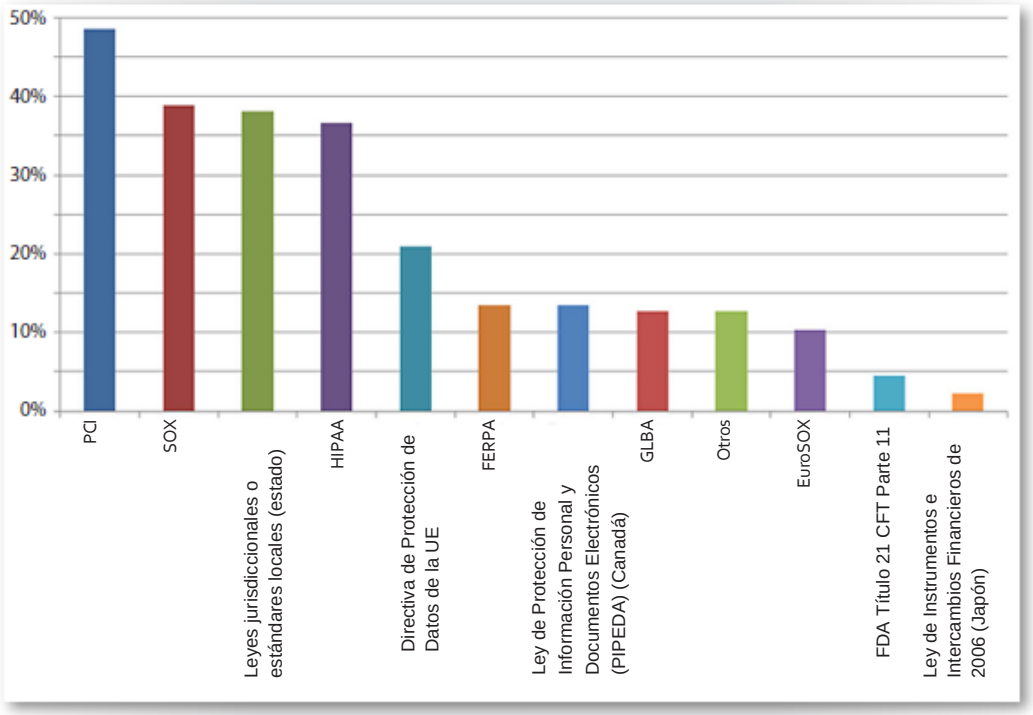


Figura 6. Requisitos de Conformidad Empresarial

Estar en conformidad con diversas normas de protección de datos en la nube es muy diferente del uso de la nube para lograr conformidad de estos mandatos. Sería razonable que las organizaciones encuestadas utilizaran la nube para hacer ambas cosas, como se mostró anteriormente en la Figura 2 (página 3), siendo que casi 30% usan servicios gestionados basados en nube y un poco menos del 25% utilizan servicios de seguridad de la información basados en la nube. Dado que los CIOs y sus negocios lidian cada vez más con requisitos de conformidad, el tratar de aliviar parte de este trabajo pasándolo a los proveedores de nube, de hecho comienza a tener sentido.

Quién Está Utilizando la Nube

Los requisitos de protección de datos en la Unión Europea se aplican también a poco más del 21% de los encuestados. Dada la adherencia a las normas, en particular a las leyes de privacidad que en Europa fueron citadas por una quinta parte de los encuestados, no es de sorprender que aproximadamente 36% de los encuestados dijeron tener algún tipo de operaciones en esa región. Vea la Tabla 1 para ver un desglose completo de las operaciones de las empresas de los encuestados.

Tabla 1. Regiones/Países Representados

Región/País	% de Encuestados
Estados Unidos	77,3%
Europa	36,1%
Asia-Pacífico	27,4%
Canadá	22,9%
Centroamérica y Sudamérica	18,1%
Australia y Nueva Zelanda	17,5%
Oriente Medio	16,5%
África	12,0%

Los encuestados representan una gran variedad de industrias, siendo las principales tres: tecnología de la información (17%), gobierno (14% del total), banca y finanzas (11%). Ver Figura 7.

¿Cuál es la industria principal de su organización?

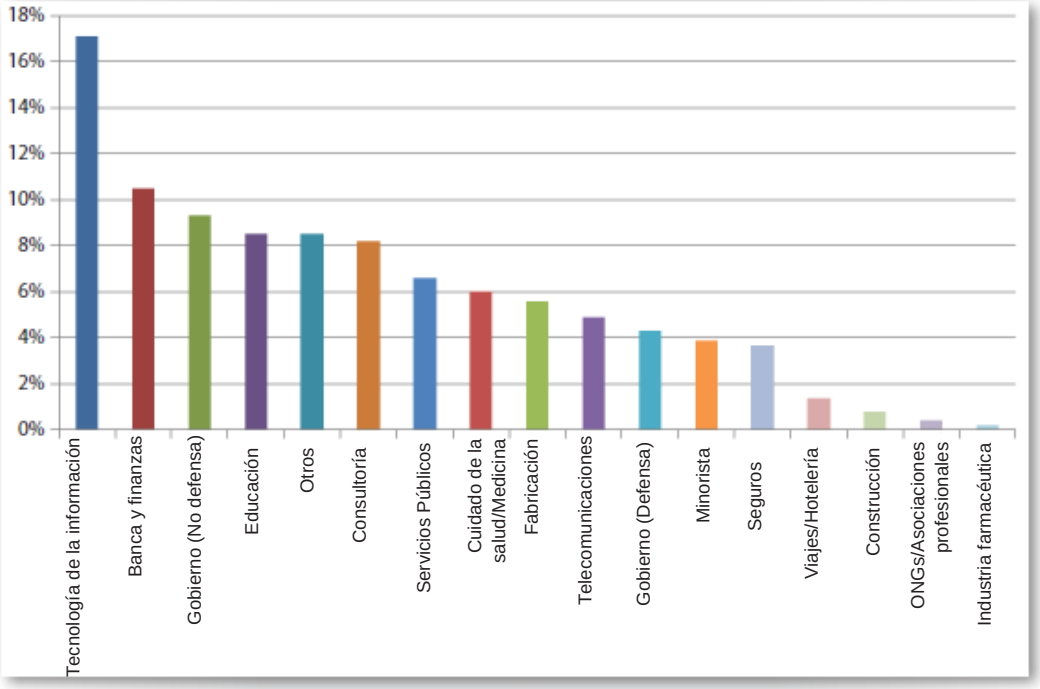


Figura 7. Industrias Representadas

Los encuestados también representaron una mezcla de pequeñas y grandes organizaciones, siendo que 38% tienen 1.000 o menos empleados, 24% más de 15.000 empleados, y el resto entre 1.000 y 10.000 empleados.

La mayoría de las respuestas provinieron de operaciones de seguridad (administradores y analistas), seguidas por operaciones de red, administración de sistemas y gestión de TI. Una buena mezcla de respuestas provino de otros roles de TI, así como de auditoría interna, desarrollo de aplicaciones y de altos ejecutivos, como se muestra en la Figura 8.

Figure 8. Funciones de los Encuestados

En general, la mayoría de los encuestados representan a las organizaciones más grandes que son globales u operan en varias regiones, y tienen posiciones diferentes y superpuestas de seguridad, negocios, conformidad y TI dentro de sus respectivas industrias y organizaciones.

Preocupaciones de Seguridad de la Nube

Con tantas aplicaciones y entornos tan diversos, la principal preocupación con el procesamiento de datos en las nubes es mantener la conformidad. De hecho, cuando se calculó el promedio de todos los modelos (pública, privada e híbrida), fue citada por el 72% de los encuestados. Ver Figura 9.

¿Cuáles son los principales problemas o preocupaciones que se relacionan con su(s) modelo(s) de computación en nube?

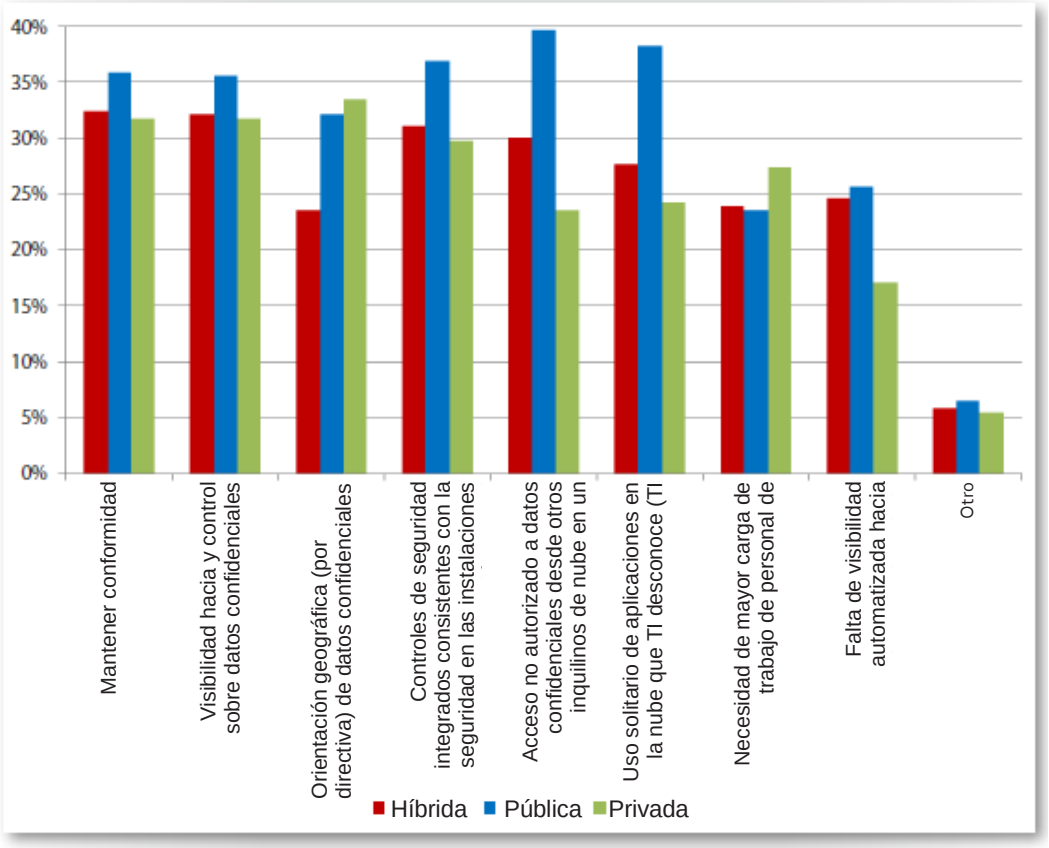


Figura 9. Principales Preocupaciones de Seguridad en Despliegues de Nube

La principal preocupación con la computación de nube pública es el riesgo de exponer datos confidenciales, siendo que 40% dicen que están preocupados principalmente por el acceso no autorizado a los datos por parte de otros inquilinos, mientras 38% están preocupados por el posible uso indebido de los recursos de la nube (TI oculta en la nube). Otros 37% dijeron que una de las principales preocupaciones generales de tener sus datos en la nube pública, es la falta de consistencia de los controles de seguridad que se integran con las herramientas en las instalaciones y la gestión de seguridad.

Para las organizaciones que utilizan servicios de nube privada, 33% calificaron a la ubicación geográfica de sus datos como una preocupación clave, que probablemente coincide con la multitud de regiones en las que operan y las normas con las que deben cumplir. Mantener la conformidad y asegurar la visibilidad de los controles implementados, mencionadas por 32% de los encuestados, son fundamentales para los usuarios tanto de la nube privada como de la híbrida.

Falta de Control

Otros problemas con proveedores de nube pública incluyen la dependencia en proveedores y servicios de intermediarios, vulnerabilidades de bibliotecas de terceros y una falta general de visibilidad hacia las prácticas de los proveedores de nube en general.
Los distintos modelos de nube permiten diferentes niveles de control:

- **SaaS:** Los usuarios tienen control sobre sus propios datos, pero no sobre las aplicaciones, tampoco tienen controles de protección de datos dentro del entorno del proveedor.
- **PaaS**: Servicios de plataforma que permiten a los usuarios gestionar las aplicaciones, y los proveedores pueden proporcionar algunos controles sencillos de infraestructura, pero la mayoría de los controles gestionados por el usuario están relacionados a la protección de datos, tales como cifrado y monitoreo.
- **IaaS:** Los usuarios pueden crear controles basados en la red y tener visibilidad completa de la seguridad y gestión de los sistemas que se ejecutan en las plataformas IaaS.

Falta de Visibilidad

Independientemente del modelo utilizado, los problemas son los mismos: La falta de visibilidad, las cuotas excesivas para la seguridad proporcionada por el proveedor y la falta de soporte para la conformidad, son las 'tres preocupaciones principales de los encuestados con relación a sus servicios de nube pública. Ver Figura 10.

¿Su organización ha tenido alguno de los siguientes problemas con su(s) proveedor(es) de nube para dar soporte a su nube privada, pública y/o híbrida? *Seleccione todo lo que aplique*

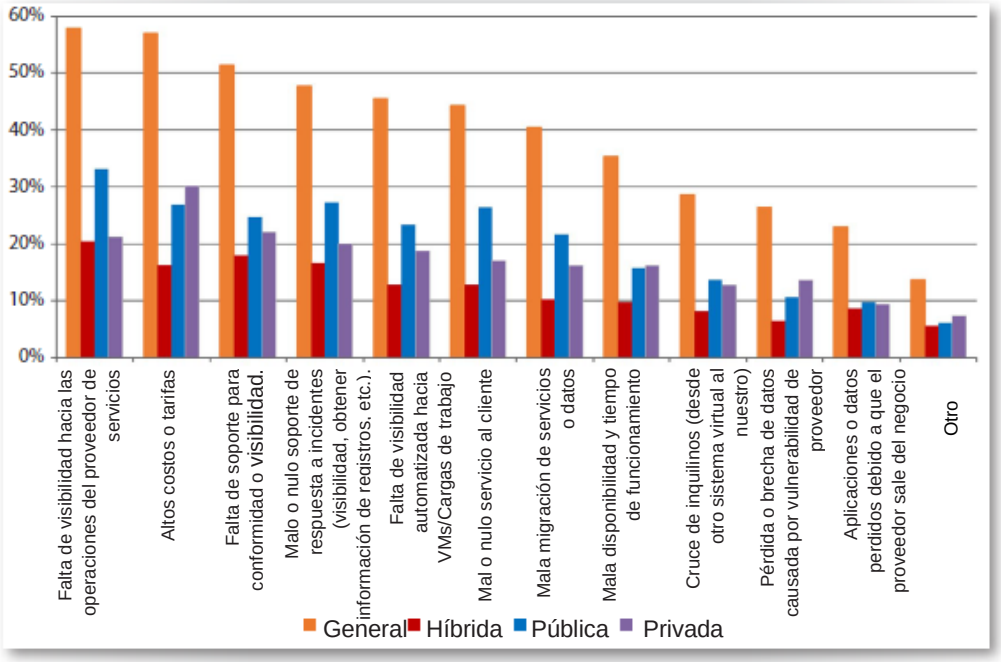


Figura 10. Problemas con Proveedores de Nube

TEMA IMPORTANTE:
Independientemente del modelo de nube que usted implemente, los problemas de responsabilidad y gestión de riesgos con su proveedor de nube son inevitables. Determine de antemano qué problemas pueden y no pueden ser abordados y cómo manejarlos.

En general, la falta de visibilidad hacia las operaciones del proveedor de nube y controles, citada por 58%, se erige como el mayor problema que tienen los encuestados con sus proveedores. De hecho, entre todos los problemas relacionados con la nube, los encuestados dijeron que la falta de visibilidad y control desempeñan un papel fundamental en otros problemas, tales como:

- Falta de soporte de respuesta a incidentes, citando falta de visibilidad (48%).
- Falta de visibilidad de VM y cargas de trabajo (46%)
- Vulnerabilidades introducidas por el proveedor que provocan una brecha o incidente (26%)

Sorprendentemente, 57% de los encuestados dijeron que los altos costos y tarifas del proveedor son un gran problema, que parece contradecir la percepción generalizada de que un gran impulsor del traslado hacia la nube son los ahorros.

Como tales, los descubrimientos de la encuesta indican que probablemente existen costos ocultos asociados con la auditoría y descubrimiento de los controles de seguridad y conformidad del proveedor de nube.

Incapacidad para Probar

Otro gran problema que enfrentan muchos proyectos en la nube de las organizaciones, es la falta de soporte para pruebas de penetración. Sólo el 24% de los encuestados afirmaron que son capaces de realizar pruebas de penetración de sus activos en nube sin restricciones, como se muestra en la Figura 11.

¿Es capaz de realizar periódicamente pruebas de penetración de sus activos y datos de nube pública de acuerdo a su contrato con su proveedor de nube?

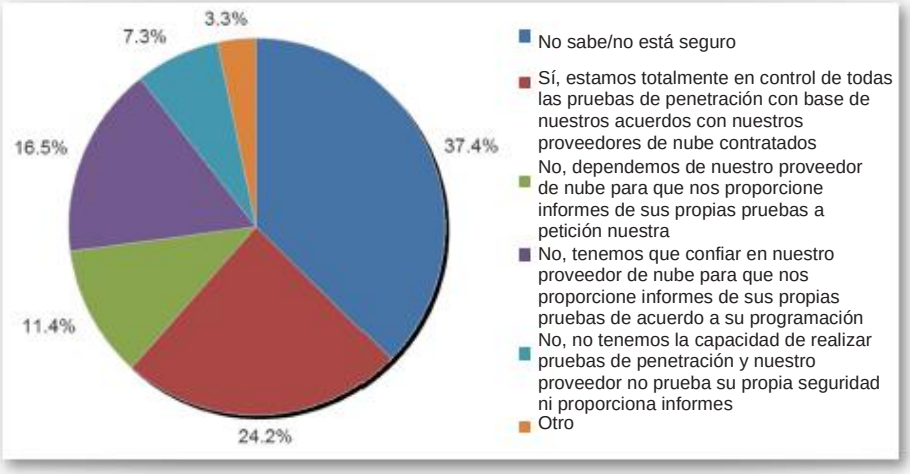


Figura 11. Desafíos de Pruebas de Penetración con Proveedores de Nube

El resto de los encuestados deben ya sea solicitar que sus proveedores de nube realicen pruebas de penetración de redes y aplicaciones o confiar en el programa del proveedor, o no recibir informes. Bajo la respuesta "otro", un encuestado dijo que las pruebas dependen de qué proveedor está utilizando la organización (utiliza más de uno), uno indicó que las pruebas de penetración eran programadas tras aprobación, y otro dijo que la organización puede probar, pero no al nivel que desea.

Sin embargo, las organizaciones no deberían verse forzadas a creer en la palabra a sus proveedores cuando se trata de pruebas de penetración. Deberían contar con una manera viable para probar la seguridad de sus aplicaciones y datos hospedados y procesados para garantizar:

- Que las zonas seguras entre inquilinos no puedan ser violadas
- Que no se puedan explotar las fallas de sistema operativo y aplicaciones
- Que los datos confidenciales no estén expuestos al personal del proveedor de nube o a atacantes externos

Porcentaje de encuestados que dijeron que su organización sufrió una brecha de nube pública o privada

Maduros para Brechas

Por lo que sabemos actualmente, los sistemas de cómputo basados en nube no han sufrido brechas masivas de una manera que impacten los datos confidenciales de los encuestados. En esta encuesta, sólo 9% de los encuestados ha sufrido una brecha real en la nube pública o en sus aplicaciones SaaS o de nube privada. No obstante, 25% no estaban seguros, lo que remite a la falta de visibilidad y control que los encuestados dijeron que están sufriendo.

Eso no significa que no estén sucediendo brechas en nubes públicas y privadas. En 2014, el entorno de Amazon Web Services de la compañía privada Code Spaces estuvo en riesgo, y eso terminó con la destrucción de los datos confidenciales y, en última instancia, el cierre de la compañía[4]. Google Drive, Dropbox, Box e iCloud llegaron la lista de los principales hacks de nube en 2014.[5]

[4] http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan
[5] http://psg.hitachi-solutions.com/credeon/blog/google-drive-dropbox-box-and-icloud-reach-the-top-5-cloud-storage-security-breaches-list

Para el 9% de los encuestados que sufrieron brechas o ataques, 55% fueron causados por una infección de malware o botnet y 54% sufrió un ataque de denegación de servicio (DoS). Desglosados entre brechas de nube pública y privada, los vectores de ataque son así:

- En sus nubes privadas, 33% de los encuestados identificaron al malware o a los botnets como la naturaleza del ataque, y sólo 23% citaron DoS.
- En la nube pública, 36% dijeron que su principal experiencia de brecha fue de DoS, siendo que 29% identificaron al malware y 28% el rapto de cuenta de usuario con la naturaleza de las brechas.
- En nubes públicas y privadas, las respuestas tienen que ver con la exfiltración de datos confidenciales: El 20% de los usuarios de nube pública y el 21% de los usuarios de nube privada, sufrieron exfiltración de datos confidenciales en las brechas que experimentaron.

Consulte la Figura 12 para ver el desglose completo de las experiencias de brechas de los encuestados.

¿Cuál fue la naturaleza de las brechas reales sufridas por su organización en sus aplicaciones ya sea en la nube pública o SaaS, o nube privada? *Seleccione todo lo que aplique.*

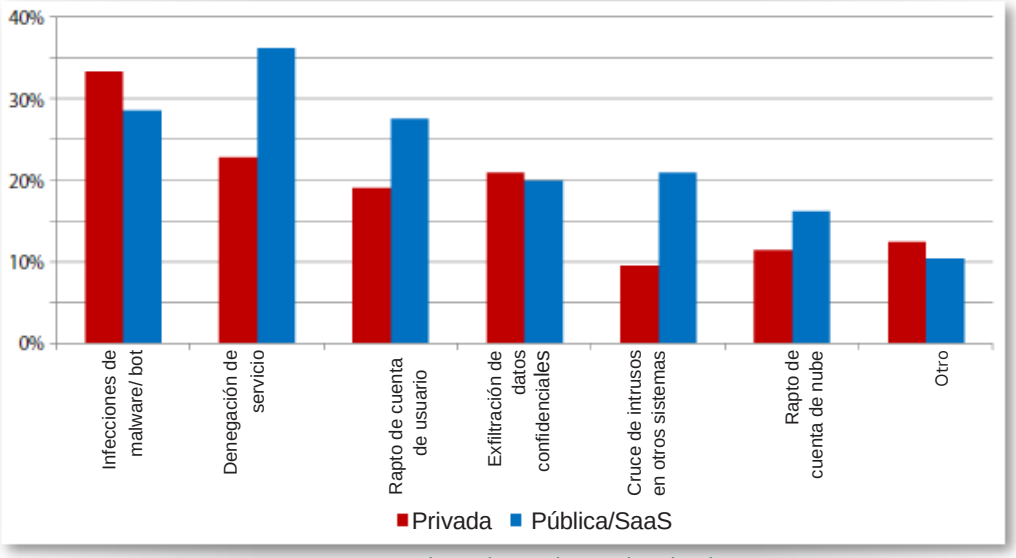


Figure 12. Attacks and Breaches in the Cloud

El informe "Principales Amenazas en la Nube" de la Cloud Security Alliance indica que los ataques DoS pueden producirse en cualquier entorno de hosting, independientemente del modelo de arquitectura de la nube, así que es lógico que los ataques DoS sean comunes tanto para los proveedores de nubes públicas como privadas6. En 2014, Kelly Jackson Higgins de Dark Reading predijo un aumento en los ataques DDoS en servicios basados en la nube como resultado de un DoS sostenido en el sitio de noticias y agregación de información Feedly. La motivación a menudo es el pago de un rescate para restablecer el servicio, según el artículo7.

[6] https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf
[7] www.darkreading.com/attacks-breaches/wave-of-ddos-attacks-down-cloud-based-services/d/d-id/1269614

Preparación para Respuesta

A pesar de que los incidentes en nube aún no parecen totalmente comunes, las organizaciones todavía necesitan adaptar sus procesos de respuesta a incidentes para adaptar mejor los bienes y servicios en la nube. Por desgracia, sólo 13% de los encuestados dijeron que han actualizado completamente sus procesos y herramientas de respuesta a incidentes para que se adecúen a sus modelos de nube, mientras que 15% han actualizado parcialmente los procesos y herramientas y 22% están en proceso de transición en este momento. Ver Figura 13.

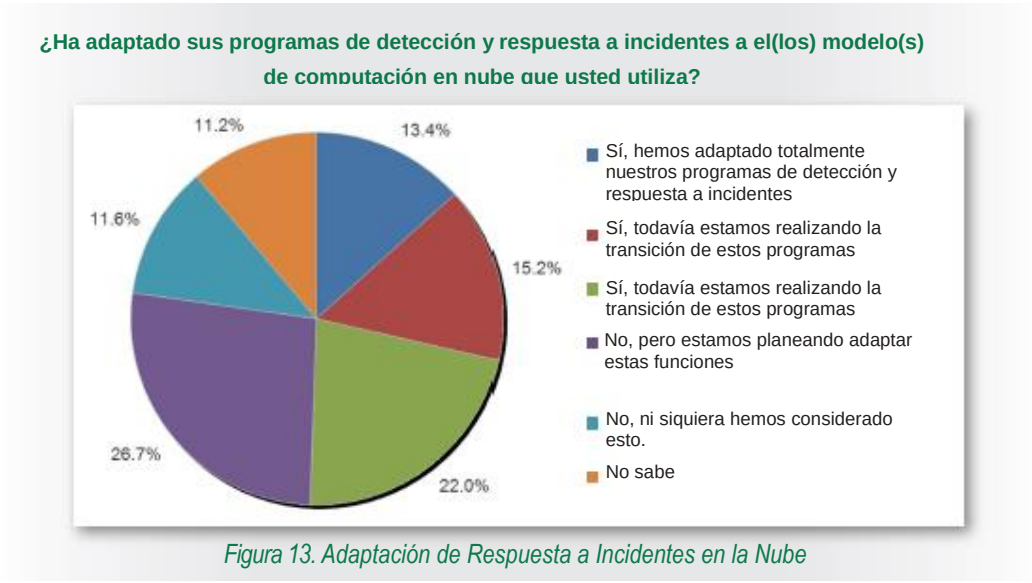


Figura 13. Adaptación de Respuesta a Incidentes en la Nube

Para aquellas organizaciones que han comenzado a adaptar sus funciones de respuesta a incidentes para la computación en nube, ha habido problemas. El mayor problema, que se remonta al problema de la visibilidad de las operaciones del proveedor de nube interna, es la falta de acceso a los archivos de registro y otros artefactos forenses, experimentado por 53% de los encuestados. Otro 46% dijo estar confuso en cuanto a qué tipo de información deben poner a disposición los proveedores de nube para las capacidades apropiadas de respuesta a incidentes (ver Figura 14).

Preocupaciones de Seguridad en la Nube (CONTINUACIÓN)

TEMA IMPORTANTE:
Enfóquese en revisar su acceso a la cuenta de servicios en nube y en determinar si sus proveedores de seguridad interna también ofrecen productos y servicios compatibles con la nube. Comience a trabajar con sus proveedores para coordinar las pruebas de penetración y los procesos de respuesta a incidentes si todavía no lo hace.

¿Qué desafíos ha enfrentado al adaptar su respuesta a incidentes y análisis forenses a la nube? *Seleccione todo lo que aplique*

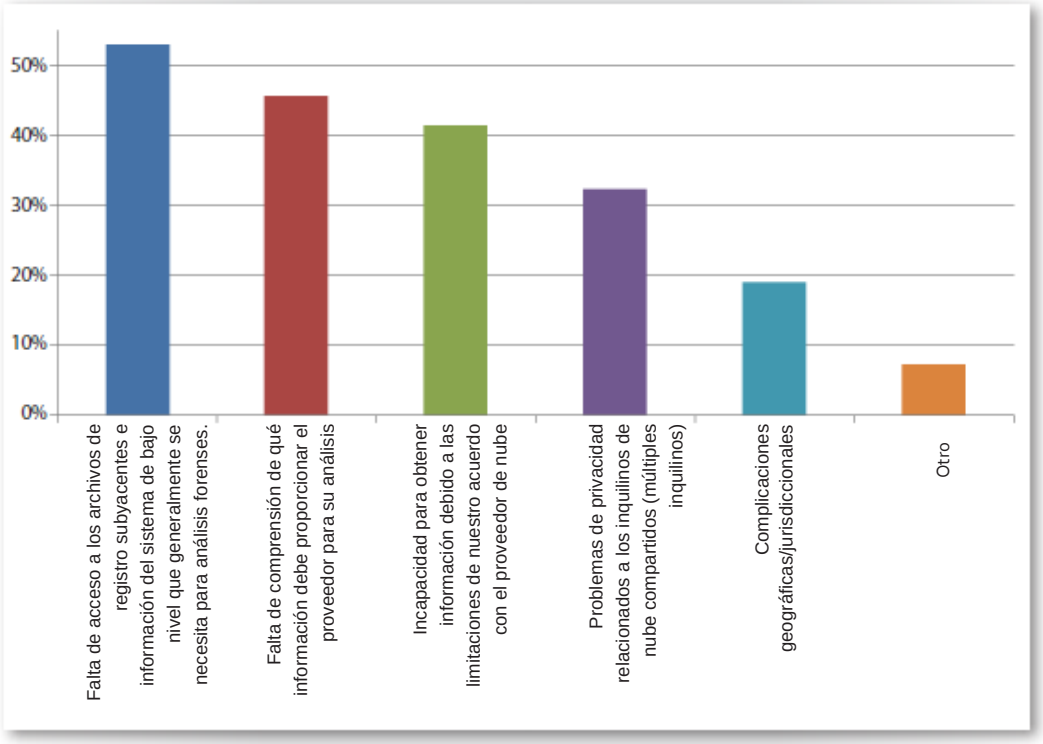


Figura 14. Incident Response Challenges in the Cloud

Los participantes de la encuesta proporcionaron muchas respuestas abiertas a esta pregunta que indican que muchos de los equipos de seguridad están luchando no sólo para lidiar con los proveedores de nube, sino también con los equipos internos en sus esfuerzos por detectar y responder a incidentes basados en la nube de forma efectiva. Algunos dijeron que tenían desafíos para capacitar al personal de seguridad interno para trabajar con las APIs de proveedor de nube para extraer datos, mientras que otros mencionaron barricadas políticas cuando TI no entrega datos o información relevante del proveedor de nube de manera oportuna. Algunas de las respuestas fueron al extremo de decir que la respuesta a incidentes basada en la nube es imposible o casi imposible.

Aunque la mayoría de las organizaciones no han sufrido una brecha en la nube, los equipos de seguridad están preocupados con el acceso ilícito a cuentas y datos, mantener la conformidad e integrarse con los controles de seguridad en las instalaciones. Además, la visibilidad hacia los entornos de nube sigue siendo un desafío, al igual que implementar procesos de respuesta a incidentes y pruebas de penetración enfocados en la nube.

SEGURIDAD COMO SERVICIO
Servicios de nube orientados hacia la seguridad a los que los consumidores se suscriben, al igual que servicios de nube tradicionales

Existen muchos tipos diferentes de controles de seguridad disponibles para la nube hoy. "Ciclo de Publicidad para la Seguridad de la Nube, 2015" de Gartner[8], establece una serie de tecnologías y estándares que están actualmente en uso o en evolución en la computación de nube. Dada la atención y enfoque en seguridad y conformidad que se observan en las respuestas a la encuesta y la investigación de terceros, las ofertas nuevas e innovadoras están evolucionando rápidamente para proteger sistemas, aplicaciones y datos en la nube.

Adaptación de Seguridad de la Nube

Muchos proveedores de seguridad tradicionales están adaptando sus ofertas a algunos entornos de nube, y los proveedores de nube están añadiendo rápidamente más opciones de seguridad nativas para los consumidores de la nube. Amazon Web Services ofrece controles de acceso a la red, numerosos modelos de gestión de claves y cifrado, y acceso a su servicio CloudTrail. Microsoft Azure ofrece anti-malware incorporado, así como cifrado y controles de acceso a la red.

Los proveedores de nube cada vez ofrecen más servicios, pero en el informe Ciclo de Seguridad, Gartner enumera algunas de las ofertas y tendencias comerciales que están conformando la seguridad en la nube hoy9. Muchas de las nuevas tecnologías que discute caen en la categoría de seguridad como servicio (SecaaS), servicios de nube orientados hacia la seguridad a los que se suscriben los consumidores, de manera parecida a los servicios de nube tradicionales. Estos servicios suelen integrarse con entornos de proveedor de nube o proteger datos en arquitecturas de nube híbrida.

Algunos de los controles exitosos y en rápida evolución que están ayudando a avanzar a la seguridad en la nube incluyen los siguientes:

- **Gestión de identidad y acceso (IAM).** Generalmente bajo la forma de gestión de identidad federada, los servicios IAM pueden ayudar a las organizaciones a integrar Active Directory y otros IDs de usuarios en numerosos entornos de aplicaciones e infraestructuras de nube sin necesidad de complicadas y desordenadas soluciones IAM en las instalaciones.
- **Corredores de seguridad de acceso a la nube (CASBs).** Los CASBs pueden monitorear y controlar el tráfico destinado a Internet y los servicios de nube específicamente, aplicando monitoreo de datos y políticas de control para prevenir la TI oculta y las fugas de datos, así como las infecciones de malware. Muchas herramientas CASB también pueden implementar cifrado y otras técnicas de protección de datos.
- **Recuperación de desastres como un servicio (DRaaS).** Los servicios nube que proporcionan recuperación de desastres (DR) y planificación de continuidad de negocios (BCP) bajo la forma de VM y copia de seguridad de datos, mensajería y servicios de coordinación, aplicaciones y paneles de planificación para DR están creciendo constantemente. El mantener capacidades completas de DR y BCP internas o en sitios en standby está disminuyendo en favor del almacenamiento en nube mucho más accesible y opciones de planificación.

[8] "Ciclo de Publicidad para la Seguridad en la Nube, 2015,"www.gartner.com/doc/3096419/hype-cycle-cloud-security- (se requiere cuenta de Gartner).
[9] "Ciclo de Publicidad para la Seguridad en la Nube, 2015"

- **IDS/IPS (HIDS/HIPS)** basado en host. Las soluciones HIDS/HIPS para IaaS (y potencialmente PaaS) pueden ofrecer firewall, integridad de archivos, listas blancas de aplicaciones, configuración y gestión de parches, y más capacidades de detección y prevención de intrusiones estándar. Con menos control sobre los recursos de red, muchos están recurriendo a servicios que funcionan dentro de cada VM y pueden gestionarse desde una consola central de nube.

Los encuestados han tenido cierto éxito en la implementación de la seguridad y en las tecnologías y procesos de protección de datos en sus entornos de nube. Sin embargo, la inmensa mayoría de los controles de seguridad todavía son gestionados internamente por las organizaciones de los encuestados.

Los controles de seguridad tradicionales, como los controles de seguridad de aplicaciones y los firewalls son más predominantes, utilizados por 76% de los encuestados en general, lo cual es debido probablemente a las ofertas básicas de los proveedores de IaaS y a los controles integrados con la mayoría de ofertas SaaS, los servicios de nube predominantes actualmente en uso. Siguen el anti-malware y el análisis de vulnerabilidades, utilizados por 74% del total. Sin embargo, en la parte inferior de la lista, vemos el uso de soluciones de IAM y CASBs, citado por 50% y 43% de los encuestados, respectivamente. Ver Figura 15.

¿Cuál de las siguientes tecnologías de seguridad y protección de datos y procesos ha implementado con éxito en su(s) entorno(s) de nube?

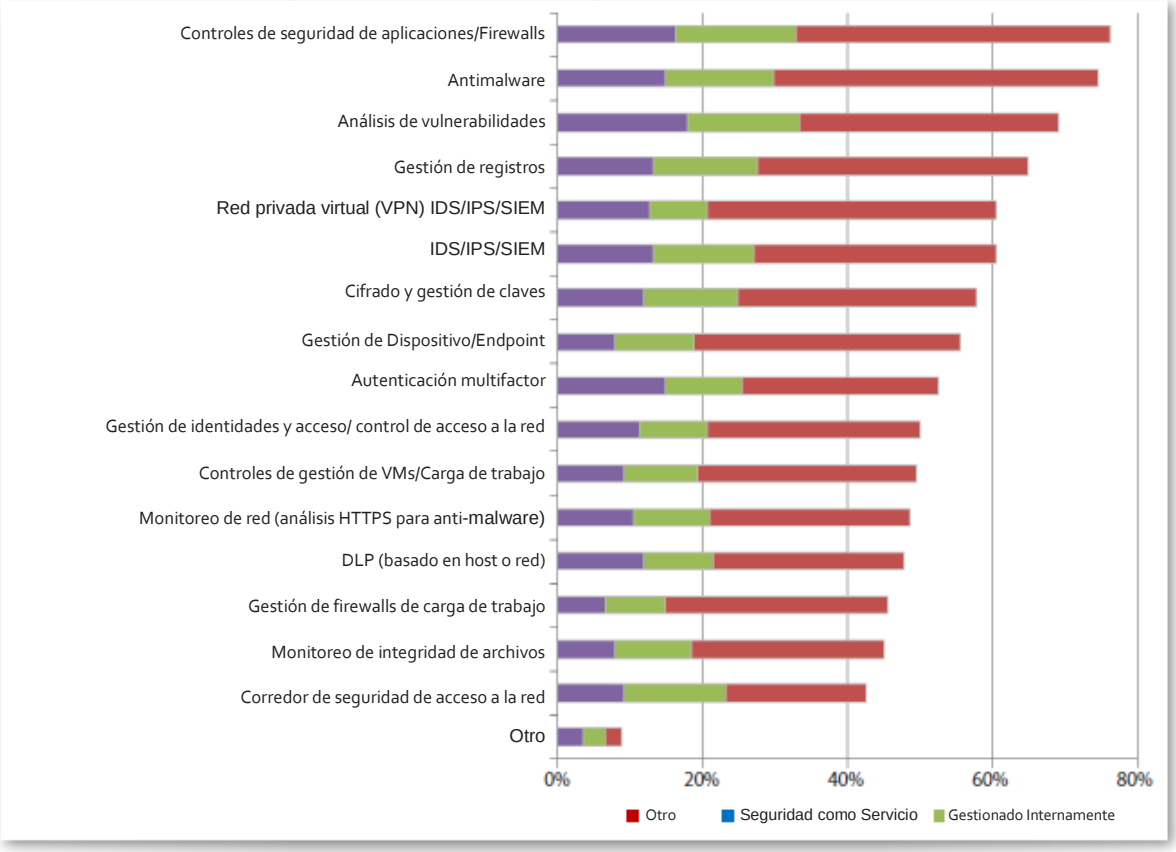


Figura 15. Controles de Seguridad de Nube en Uso

TEMA IMPORTANTE:

Aunque muchos controles todavía son gestionados internamente, SecaaS está emergiendo como un medio viable para mejorar la seguridad en la nube. Los equipos de seguridad deben comenzar a considerar el uso de las opciones de SecaaS al diseñar los modelos de seguridad en la nube

La mayoría de los controles que están en uso por más de 50% de las organizaciones (los controles entre "Controles de seguridad de aplicaciones /Firewalls" y "Autenticación multifactor" en la Figura 15) son controles de referencia comunes y muchos de ellos probablemente se requieren para la conformidad con mandatos. Otros controles, como IAM, prevención de pérdida de datos (DLP), monitoreo de integridad de archivos y CASBs, son más lentos para adaptarse a entornos de nube y menos susceptibles de ser ofrecidos por los proveedores de forma nativa.

Seguridad como un Servicio

Como se ha comentado anteriormente, la seguridad también está siendo alojada en la nube. La seguridad como servicio (SecaaS) es una aplicación muy adecuada para la nube, que ofrece a las organizaciones la posibilidad de descargar monitoreo, detección, y soporte de actualización e instalación de parches para aplicaciones tanto internas como basadas en la nube.

En esta encuesta, los principales seis controles de seguridad implantados en la nube como un servicio incluyen controles de seguridad de aplicación/firewalls, análisis de vulnerabilidad, antimalware, gestión de registros, IDS/IPS/SIEM y CASBs. A lo largo de los próximos 18 meses, el análisis de vulnerabilidades, la autenticación multifactor, DLP y las funciones de gestión de registros continuarán siendo robustas, y esperamos trasladar desde los entornos físicos hasta los entornos de nube. Ver Figura 16.

¿Qué servicios adicionales tiene pensado cambiar hacia una seguridad como servicio basada en nube durante los próximos 18 meses? *Seleccione todo lo que aplique*

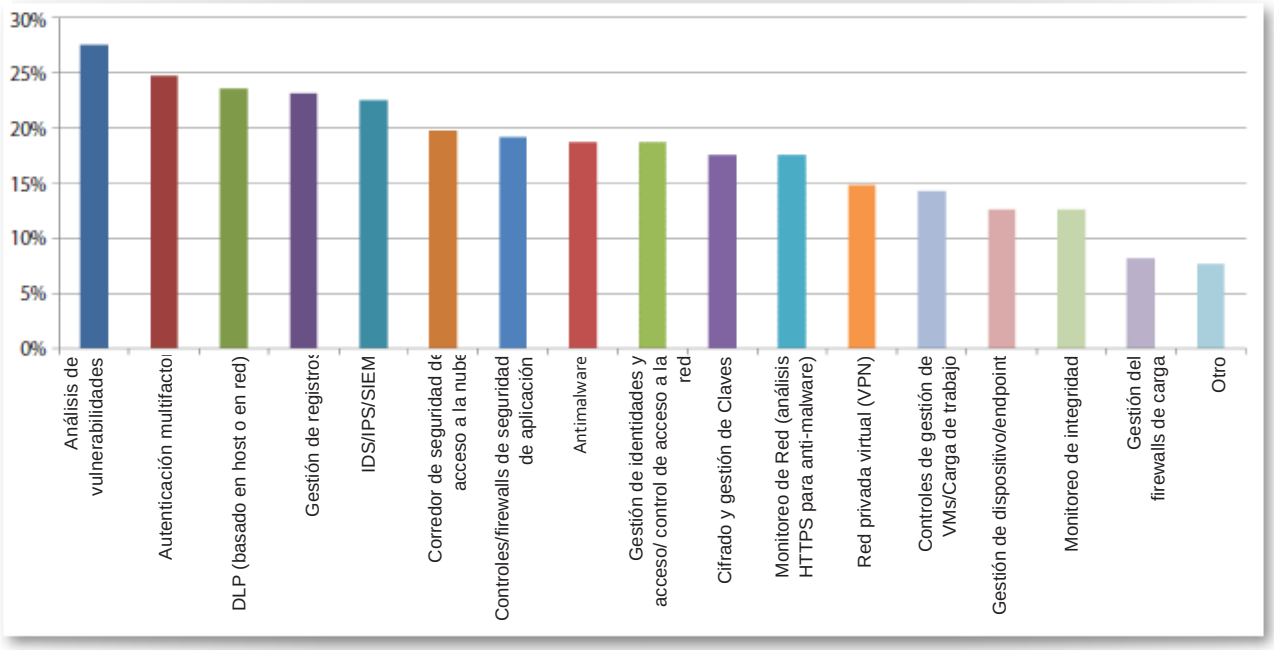


Figura 16. Inversión Futura en SecaaS

Esto se alinea con el informe de Ciclo de Publicidad de Gartner, que muestra que estas tecnologías están madurando rápidamente, con ofertas de proveedores más eficaces que aparecen todo el tiempo.

Control de Acceso

Muchas organizaciones están preocupadas con la utilización de los servicios de nube por parte de los empleados, especialmente cuando algunos servicios (como el almacenamiento basado en nube o mensajería) no han sido ni aprobados para su uso ni configurados de forma segura. SecaaS está empezando a hacer incursiones como originador viable de control para la gestión de cuentas de usuarios, que, aunque todavía se maneja esencialmente de manera interna, se originan por SecaaS para el 14% de los encuestados. En general, 45% están implementando opciones de CASB para monitorear, principalmente con gestión interna. La Figura 17 muestra los tipos de monitoreo que están implementando las organizaciones.

Si usted puede controlar y monitorear el uso de la nube por parte de los empleados, sírvase indicar si estas herramientas y procesos se originan desde dentro de su organización (gestionadas internamente), su proveedor de nube (seguridad como servicio) o ambos

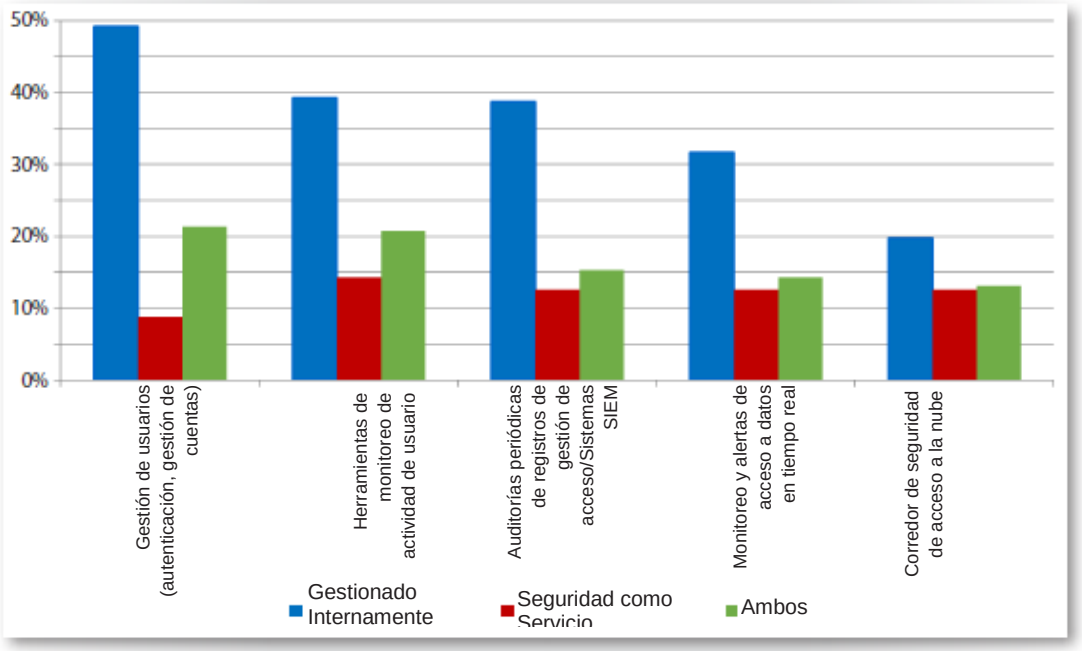


Figura 17. Opciones de Monitoreo de Actividad de Nube

Si bien es obvio que los equipos de seguridad se enfocan en el monitoreo del uso de los empleados de la nube, el controlar y monitorear los datos que atraviesan entre los dispositivos de los empleados y servicios en la nube puede ser difícil. La mayoría (54%) requieren el uso de una VPN basada en red o un proxy para acceder a los recursos corporativos en la nube, mientras que 41% brindan seguridad a los datos durante el transporte a través de un proxy. Otros se han enfocado en los endpoints, separando el contenido y aplicaciones, utilizando herramientas DLP o restringiendo las aplicaciones que se pueden instalar (listas blancas). La Figura 18 ilustra los métodos que utilizan los encuestados para monitorear los datos en tránsito entre los dispositivos de los empleados y la nube.

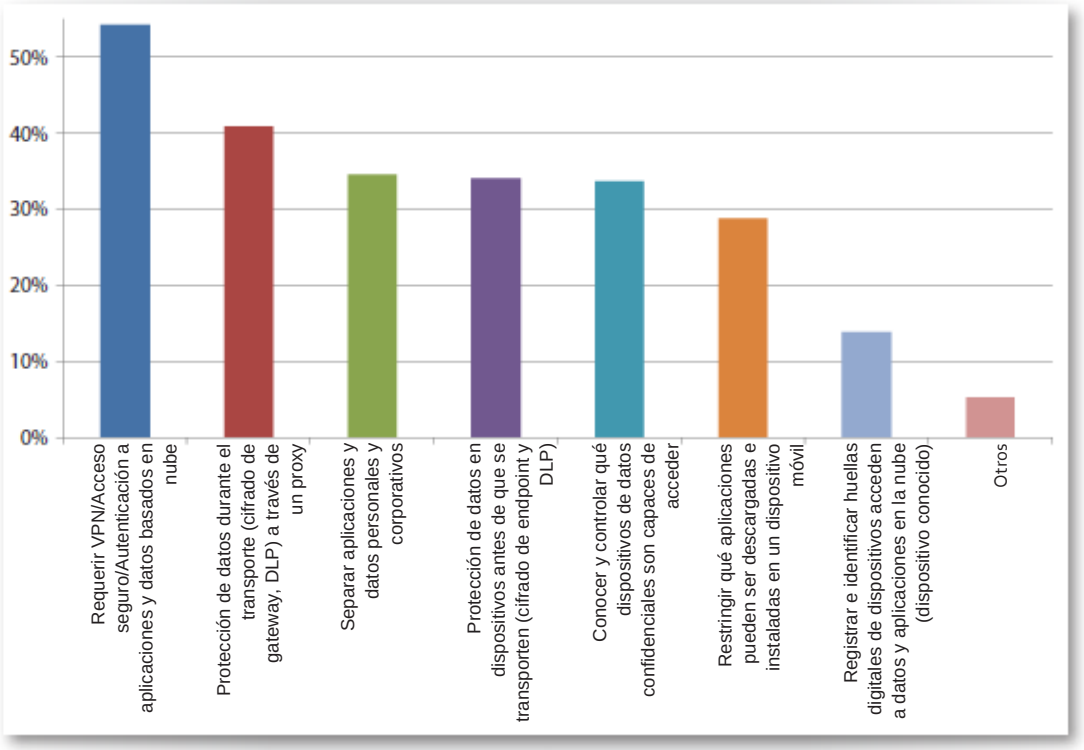


Figura 18. Monitoreo de Dispositivos de Empleados para Uso de Servicios en Nube

TEMA IMPORTANTE:

Para mejorar la eficacia de los controles de seguridad por capas, verifique los controles ofrecidos por el proveedor tales como registro, autenticación multifactor, cifrado y otros productos y servicios que pueden funcionar de forma nativa en la infraestructura de nube

La utilización de abordajes basados en la red para controlar el acceso a las aplicaciones, sistemas y datos en la nube representa una capa de la pila de seguridad de hoy, y seguirá creciendo y cambiando con el tiempo conforme la naturaleza del acceso y uso de la nube cambie. Ahora, muchos profesionales de la seguridad ven un cambio en la naturaleza de la forma en cómo sus controles de seguridad por capas funcionan cuando se traslada hacia los entornos de nube.

Las organizaciones que desean mejorar la eficacia de sus controles de seguridad por capas, deben observar los controles ofrecidos por los proveedores, tales como registro, autenticación multifactor, cifrado y productos y servicios compatibles que funcionen nativamente dentro de su infraestructura de nube. También se espera que aumente el uso de controles SecaaS, especialmente conforme los proveedores asociados con las compañías de servicios de seguridad ofrecen integración y funcionalidad más continua.

Conclusión

Los encuestados por SANS proporcionaron comentarios significativos al equipo de analistas sobre los desafíos que enfrentan y los pensamientos que tienen sobre la migración hacia la nube. No es de extrañar que algunos encuestados se muestran recelosos para trasladarse hacia entornos de nube, y muchos citan la falta de visibilidad hacia las prácticas y controles de los proveedores de nube como un motivo para ello.

Los equipos de seguridad necesitarán adoptar una mayor automatización y controles de seguridad compatibles con API que puedan ayudar a acortar la distancia entre las herramientas y procesos de seguridad internos y los que se ejecutan en los entornos SecaaS de nube

Varios de los encuestados también mencionaron específicamente la necesidad de mayor automatización de la seguridad, mediante la cual los equipos de seguridad tengan acceso a herramientas y scripts que se integren con el proveedor y con APIs SecaaS para proteger y monitorear mejor sus activos en la nube. Los equipos de seguridad están luchando para obtener suficiente visibilidad hacia la infraestructura, controles y procesos de los proveedores de nube, a través de contratos e informes de auditoría, y dicen que la naturaleza de la pila de seguridad de "defensa a profundidad" de las organizaciones tiene que cambiar también.

Los equipos de seguridad se enfrentan a la realidad de que el liderazgo empresarial quiere comenzar a utilizar servicios de nube, y esto ya está ocurriendo a un ritmo rápido. Muchas organizaciones están trasladando también los datos confidenciales, lo que implica que los equipos de seguridad tendrán que revisar cuidadosamente qué tipos de datos deben proteger en la nube y qué controles de seguridad (cifrado, DLP, servicios CASB, etc.) están disponibles para ayudarlos a protegerlos. El presionar a los proveedores de nube para que profundicen sus controles y procesos, tanto contractualmente como a través de los informes de auditoría estándar como SSAE 16 SOC, puede ayudar a las organizaciones a determinar la postura general de seguridad de proveedores potenciales, pero los profesionales de la seguridad debe además estar muy pendientes de los controles de protección que pueden gestionar.

Es necesario que los equipos de seguridad presten atención a las cuentas de nube de sus organizaciones, porque los atacantes están buscando activamente irrumpir en los servicios de nube y poner en riesgo los datos. También se deben proteger los datos en tránsito con VPN y otras opciones de cifrado, y monitorear qué tipos de servicios de nube utilizan los empleados. Más proveedores se están adaptando sus productos a los entornos de nube todo el tiempo, y SecaaS es acortando las distancias en muchos casos.

Las herramientas y controles de seguridad de endpoint, las ofertas de SecaaS que aprovechan APIs para integrar con proveedores de nube, y los controles en las instalaciones tales como gateways de cifrado de nube y soluciones de gestión de vulnerabilidades, tendrán que trabajar de forma flexible con los nuevos controles ofrecidos por los proveedores de nube. De hecho, conforme la adopción de los modelos de nube híbrida crezcan, y este parece ser el caso, los equipos de seguridad necesitarán adoptar una mayor automatización y controles de seguridad compatibles con API que puedan ayudar a acortar la distancia entre las herramientas y procesos de seguridad internos y los que se ejecutan en los entornos SecaaS de nube.

Acerca del Autor

Dave Shackleford es analista de SANS, instructor, autor del curso, director técnico de GIAC y miembro de la junta de directores del SANS Technology Institute, también es fundador y consultor principal de seguridad de Voodoo Security. Él ha brindado consultoría a cientos de organizaciones en las áreas de seguridad, conformidad regulatoria e ingeniería y arquitectura de red. Dave es un VMware vExpert y tiene una amplia experiencia en el diseño y la configuración de infraestructuras seguras virtualizadas. Anteriormente trabajó como director de seguridad de Configuresoft y CTO del Centro para la Seguridad de Internet. Dave actualmente ayuda a liderar el capítulo de Atlanta de la Cloud Security Alliance.

Patrocinador

SANS desea agradecer al patrocinador de esta encuesta: