INFORME

Preguntas para su proveedor de servicios en la nube

Sepa cómo se protegerán sus datos en la nube

INFORME

Preguntas para su proveedor de servicios en la nube

Sepa cómo se protegerán sus datos en la nube

La contratación de un proveedor de servicios en la nube (Cloud Services Provider, CSP) en forma de Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (Paas) o Software-as-a-Service (SaaS), se ha convertido en una práctica común para los departamentos de TI de las empresas. Es absolutamente fundamental elegir correctamente los proveedores y servicios, sobre todo por su relación con las prácticas de seguridad, la privacidad de los datos y las capacidades operativas. Asegúrese de someter a sus partners CSP potenciales a un exhaustivo escrutinio para conocer con exactitud de qué forma van a proteger su información más valiosa.

Con una demanda de servicios en la nube cada vez mayor, encontrar el CSP adecuado (o varios proveedores) es una enorme responsabilidad para los equipos de TI y los profesionales de la seguridad de las empresas. Hay todo tipo de proveedores de servicios en la nube: desde enormes empresas de ámbito mundial que ofrecen una amplia variedad de servicios en la nube, a negocios pequeños especializados en un número reducido de servicios. Están incluso los conocidos como intermediarios de servicios en la nube (CSB, Cloud Services Brokerage), que incorporan servicios en la nube de proveedores distintos con modelos de distribución de servicios diferentes: de integradores de sistemas y empresas de externalización a proveedores de software independientes y resellers de valor añadido.

Este laberinto de ofertas de CSP complica a las empresas la organización de las opciones, que por otra parte, es fundamental. Para normalizar la gran cantidad de diferencias entre los potenciales proveedores, es preciso hacerles preguntas claras sobre temas importantes. La seguridad debería encabezar siempre su lista de prioridades a la hora de seleccionar los partners CSP adecuados en su camino a la nube.

Los aspectos fundamentales de la seguridad deberían centrarse en una serie de cuestiones que permitieran acotar sus opciones. Estas preguntas le ayudarán a determinar qué proveedores comprenden de verdad todas los problemas e implicaciones relacionados con la seguridad, y cuáles tienen el enfoque que mejor se

ajusta a las prioridades, prácticas y tolerancia a riesgos de su empresa. Dedicaremos la mayor parte de este informe a preguntas específicas en tres áreas: seguridad, privacidad y operaciones, todas ellas relacionadas con la protección de los datos. Si sigue estas sugerencias y aplica su propia experiencia, el sentido común y el consejo de colegas que ya hayan pasado por este proceso, aumentará las posibilidades de encontrar uno o varios CSP que le ayuden a garantizar una seguridad robusta para sus activos de datos más importantes.

Investigación sobre los posibles CSP al más alto nivel

Un primer paso indispensable es evitar hacer suposiciones sobre lo que es o no la seguridad en lo que respecta a un proveedor. Todos los proveedores son distintos, tienen reglas, acuerdos de nivel de servicio (SLA), términos y condiciones diferentes. Como cliente, asegúrese de que entiende bien a qué se compromete con usted cada proveedor de servicios.

En segundo lugar, asegúrese de realizar preguntas relacionadas con la forma de gestionar la seguridad y la privacidad. Entre otras cosas, es necesario que sepa lo que esperan que haga su empresa, lo que hacen como proveedores y cómo lo hacen.

En tercer lugar, examine en profundidad sus términos y condiciones. Está claro que a nadie le gusta leer las interminables páginas de letra pequeña de un contrato, pero es necesario que comprenda esos detalles para que pueda elegir un proveedor que ofrezca el servicio adecuado y proporcione el nivel de confianza conveniente. No eluda sus responsabilidades en esta materia; no se conforme con hacer clic en "aceptar" sin más. Examine con detenimiento las distintas secciones de los términos y condiciones, y preste toda su atención a los aspectos relacionados con los datos.

En cuarto y último lugar, no dé por hecho que todos los servicios en la nube tienen las mismas directrices y objetivos de prestación de servicios, incluso del mismo proveedor. Revise los términos y las condiciones de cada servicio. Léalos todos, y no haga suposiciones sin fundamento o podría llevarse una enorme y costosa sorpresa.

Preguntas de seguridad

Afortunadamente las preocupaciones de seguridad en la nube han disminuido enormemente en los últimos años gracias a que los CSP elaboran un historial de prácticas de seguridad exitosas. Aun así, a muchos ejecutivos, así como a muchos consejos de administración, les preocupa saber si los datos de la empresa están verdaderamente seguros en la nube. Debería plantear preguntas específicas sobre los CSP potenciales a fin de conseguir el alto nivel de confianza necesario para minimizar preocupaciones y riesgos.

¿Quién tiene acceso a mis datos, tanto física como virtualmente?

El acceso físico es totalmente distinto al virtual. Es importante preguntar sobre ambos tipos de acceso.

- ¿De qué medidas de seguridad dispone la empresa cuando se accede a su centro de datos?
- ¿Tiene su personal autorización de seguridad, y se protege el acceso físico a los datos por parte de fuentes externas?
- ¿Cuáles son las directivas de la institución o del centro de datos, y cómo se protegen?
- ¿Quién tiene acceso virtual a los datos? ¿Desde dónde se accede y por qué?
- ¿De qué forma acceden a ellos los usuarios? ¿Utilizan una VPN? y, ¿están cifrados los datos? Si están cifrados, ¿cómo se protegen las claves de cifrado?

¿Externaliza el CSP el almacenamiento de los datos?

Muchas empresas utilizan empresas de externalización para prestar sus servicios, por lo tanto, es posible que su CSP externalice sus datos a otra ubicación o incluso a otro proveedor. En ese caso, debe decidir si se siente cómodo con esa situación.

¿De qué forma gestiona el proveedor las obligaciones legales en cuanto a revisión de los datos?

Independientemente de que los requerimientos provengan de sus clientes o de organismos públicos por razones legales o normativas, la gestión de estas solicitudes requiere discreción, experiencia y conocimiento de las directivas de gobernanza corporativa, así como de las exigencias de cumplimiento de normativas. No es extraño que la calidad de sus datos se vea afectada por los requerimientos legales, y debe conocer la trazabilidad de los datos y saber cómo se gestionan los requerimientos.

¿Cómo y cuándo se eliminan los datos?

Puesto que todos los proveedores son diferentes, es importante comprender la existencia de dificultades de almacenamiento dado el enorme volumen de datos que recorre el mundo en nuestros días. Le gustará conocer el volumen de datos que almacena su CSP y, en particular, el volumen de sus datos concretos que se almacena. Además, pregunte sobre el tiempo que se almacenarán los datos, cuándo se eliminan y cómo se toman las decisiones para eliminarlos.

¿Cuál es la arquitectura de datos?

Concretamente, pregunte cómo se aíslan sus datos de los de otros clientes en un entorno multiinquilino. Pida a su proveedor que le explique cómo se segmentan sus datos de los de otros clientes y cómo podría cambiar esto en el futuro.

¿Qué certificaciones y/o auditorías independientes se realizan?

Las certificaciones le permitirán conocer mejor el grado de madurez del proveedor, qué temas le preocupan y si está comprometido a realizar mejoras continuas. Desde el punto de vista de las auditorías por parte de terceros, necesitará saber con qué frecuencia el proveedor está dispuesto a realizar cambios y asegurarse de que cumple las expectativas de sus clientes y proveedores.

Preguntas sobre privacidad

La seguridad y la privacidad están estrechamente entrelazadas, pero hay algunas preguntas exclusivas sobre privacidad que debería plantear a su CSP. Y las preguntas sobre privacidad, aunque obviamente basadas en el cumplimiento, no se limitan exclusivamente a temas normativos.

¿Qué datos se recopilan de su empresa y cómo se garantiza su privacidad?

La privacidad varía ligeramente en función de la empresa, por lo que es especialmente importante definir el significado de privacidad para los principales implicados dentro de su organización.

¿Para qué se utilizan los datos?

A menudo sorprende conocer los distintos usos que se hace de los datos, y en algunos casos incluso pueden generar preocupación. Asegúrese de que su CSP conoce sus directivas de gobernanza sobre el uso aceptable de los datos.

¿Cuánto tiempo conserva sus datos el CSP?

Los términos y las condiciones pueden establecer que se recopilen datos durante 30 o 90 días, o incluso un año. Pero eso no necesariamente determina el tiempo que el proveedor puede conservar sus datos. Esto variará de manera importante entre proveedores, servicios y tipos de datos que se recopilen. Podría tener datos que se anonimizan, almacenan y utilizan para fines de pruebas durante muchísimos años, por lo que debe asegurarse que pregunta por la retención.

¿Cifra el CSP sus datos y de qué manera?

Es importante disponer de esta información para asegurarse de que todo lo que considere clasificado o privado, o bien le preocupe, no se empleará para otros usos por parte del CSP.

¿Dónde se almacenan los datos?

¿Cuenta con reglas o normativas de almacenamiento de datos de carácter geográfico que los CSP deben respetar? Los proveedores de servicios almacenan los datos en muchas ubicaciones para muchos y variados fines, y es encesario que conozca los detalles y cómo se ajusta esta política a sus prácticas empresariales.

¿Se transfieren o transmiten los datos a otras entidades internas o externas?

Todos sabemos que esta es una práctica generalizada en Internet y que existen muchos programas distintos de adhesión/cancelación. Es realmente importante saber si el CSP comparte los datos con alguien, cómo, cuándo y por qué lo hace, y dónde se transfieren.

Preguntas operativas

Más allá de la seguridad y la privacidad, las actividades de su CSP se cruzarán con muchas operaciones diarias de su empresa. Disponer de la información adecuada a este respecto le ayudará a determinar si los métodos que utiliza su CSP para gestionar sus datos y ponerlos a disposición de su personal mejoran u obstaculizan sus operaciones.

¿Cuál es el modelo de redundancia de la arquitectura de base de datos y almacenamiento?

La redundancia es particularmente importante porque se centra en la forma de afrontar fallos en la infraestructura sin afectar a la continuidad de la actividad.

¿Con qué frecuencia se realizan copias de seguridad?

Todos hemos oído este mantra desde que aparecieron las computadoras: hay que hacer copias de seguridad, hay que hacer copias de seguridad, hay que hacer copias de seguridad. Y es extremadamente importante conocer la frecuencia con la que los proveedores realizan copias de seguridad. Está claro que cuanto mayor sea la frecuencia, mejor será la redundancia. En caso de fallo, será más fácil para su proveedor restaurar el servicio a un punto y hora específicos.

¿Cuál es el tiempo de recuperación ante fallos?

Es inevitable pensar que, en algún momento, su proveedor tendrá un problema, y resulta absolutamente fundamental que sepa el tiempo que tardará su CSP en recuperar sus datos. ¿Lo hará en minutos, horas, días o semanas? Sin duda se producirán fallos, pero lo importante es saber cuánto tiempo llevará la recuperación de ese fallo cuando utiliza un proveedor de servicios.

¿Cómo podemos acceder o descargar datos del servicio?

Las respuestas a estas preguntas le ayudarán a conocer las distintas filosofías de los proveedores de servicios y tener una idea más clara de si esos pasos entran o no en conflicto con sus procesos operativos.

¿Qué herramientas analíticas podemos utilizar para ver nuestros datos?

El proveedor de servicios puede tener en su poder una gran cantidad de sus datos, y es posible que usted no quiera tener que extraer todos esos datos y utilizar herramientas analíticas de terceros para comprimirlos y poder hacer uso de los mismos. Es mucho mejor si el proveedor de servicios le ofrece ese servicio de manera que le permita llevar a cabo la agregación y modelado de los datos.

En caso de daños en los datos, ¿cuál es la pérdida de datos máxima que podemos esperar?

Esto debería ir asociado a las preguntas de redundancia y recuperación mencionadas anteriormente, y deberían estar estrechamente coordinadas. ¿Cuánto tiempo se tardará en recuperarse de un fallo de datos y de qué forma afectará realmente ese proceso de recuperación a la calidad de los datos?

Resumen

Las preguntas propuestas deberían ayudarle en el proceso de identificación, evaluación y selección de los proveedores de servicios en la nube, así como a trabajar con ellos. Además, estas cuestiones actúan como importantes puntos de verificación de la realidad en la evaluación permanente del rendimiento de su CSP actual, y sirven de vara de medir periódica para la contratación de nuevos servicios que satisfagan las necesidades de crecimiento de su empresa.

Recuerde que la selección de un CSP no es una tarea cualquiera. Una selección inadecuada puede tener un efecto enorme, incluso potencialmente catastrófico, en su empresa si la preparación respecto a la seguridad del CSP no se ajusta a sus necesidades, actuales y futuras. Al mismo tiempo, la selección del CSP adecuado puede ayudar a su empresa de muchas maneras; desde el punto de vista económico, con la asignación de recursos internos, respecto a la confianza en la seguridad e integridad de sus datos, etc.

Al llevar a cabo el proceso de evaluación de posibles CSP, estas cuestiones de seguridad, privacidad y de carácter operativo pueden mejorar su confianza en la selección última de partners CSP. Claro está que estas cuestiones deberían sopesarse y ajustarse para reflejar el modelo de negocio, las prioridades operativas y la cultura corporativa de su empresa. Plantear estas cuestiones será una manera eficiente y eficaz de tomar decisiones de asociación más inteligentes a medida que aumenta su uso de servicios en la nube.

Pueden parecer muchas preguntas, pero créanos, a largo plazo, agradecerá el tiempo dedicado a analizarlas. Es mucho mejor disponer de información que despeje dudas que tener que imaginarse las respuestas.

Acerca del autor

Jamie Tischart
CTO Nube/SaaS, McAfee

Jamie Tischart es director de tecnología (CTO) para la nube y las soluciones SaaS en McAfee y es responsable de liderar la creación de las soluciones para la nube de futura generación de McAfee® y de generar una ventaja competitiva y sostenible. Lleva en McAfee más de 10 años y ha ocupado una amplia variedad de cargos técnicos: director de ingeniería para la nube, director de operaciones e investigación en McAfee Labs, ingeniería y operaciones de calidad. Antes de incorporarse a McAfee, Tischart ocupó varios cargos ejecutivos, de dirección, de ingeniería y de arquitecto de QA, en empresas como MX Logic, Blackbaud, Openwave, Newbridge Networks y Corel. Tischart tiene un máster en administración de empresas (MBA) por la Universidad de Aspen. Vive con su familia en Colorado, donde da rienda suelta a su pasión por el desarrollo de soluciones SaaS, DevOps y operaciones en la nube, así como por el coaching Agile y el liderazgo en ingeniería de calidad (Quality Engineering Leadership), al tiempo que disfruta del esquí, la escritura y el hockey. Es voluntario activo en muchas organizaciones, como Habitat for Humanity, Ronald McDonald House Charities of Denver, Inc., y Food Bank of the Rockies.

Más información

Para obtener más información, visite **www.mcafee.com/mx/solutions/data-center-cloud-defense.aspx**.

Acerca de McAfee

McAfee es una de las empresas de ciberseguridad independientes más importantes del mundo. Inspirándose en el poder de la colaboración, McAfee crea actividades y soluciones de consumo que hacen del mundo un lugar más seguro. Al diseñar soluciones compatibles con los productos de otras firmas, McAfee ayuda a las empresas a implementar entornos cibernéticos verdaderamente integrados en los que la protección, la detección y la corrección de amenazas tienen lugar de forma simultánea y en colaboración. Al proteger a los consumidores en todos sus dispositivos, McAfee protege su estilo de vida digital en casa y fuera de ella. Al trabajar con otras empresas de seguridad, McAfee lidera una iniciativa de unión frente a los ciberdelicuentes en beneficio de todos.

www.mcafee.com/mx

McAfee™
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
www.mcafee.com/mx

62487wp_questions-cloud-service-provider_0616
JUNIO DE 2016