# El cloud empresarial para garantizar la transición digital: 6 aspectos cruciales

OVHcloud

vmware®

La tecnología cloud se ha impuesto con firmeza en el panorama informático actual. Con una transformación digital a toda máquina en todos los sectores, las empresas confían en las estrategias multicloud para adaptarse mejor a las nuevas exigencias del mercado. Uno de los elementos clave de este enfoque es el cloud privado, considerado por naturaleza como una solución más segura que el cloud público[1].

Si bien es cierto que un cloud privado empresarial le ofrece un mayor control sobre el entorno físico y posibilidades cuasi ilimitadas de personalización, construir su propio cloud privado no está exento de riesgos...

# Brechas de seguridad

Violaciones de datos personales, claves de acceso filtradas, sistemas de autenticación deficientes, interfaces y API hackeadas...: los últimos años han estado marcados por diversos fallos masivos de seguridad. Cada semana se registran nuevos ciberataques y fallos de seguridad que no contribuyen a mitigar la desconfiada asociada a la tecnología cloud.

Esto hace que muchas empresas crean que sus datos están más seguros si se alojan «in-house», en sus propias infraestructuras cloud. Pero la realidad es que los entornos cloud alojados son tan (o incluso más) seguros que las infraestructuras «on-premises», ya que los primeros están diseñados y gestionados por expertos en seguridad que conocen los desafíos asociados al cloud y saben cómo afrontarlos correctamente.

# Ataques DDoS

Los ataques por denegación de servicio distribuidos (DDoS) siguen siendo una de las grandes preocupaciones para las empresas digitales. Los atacantes han ido perfeccionando sus estrategias durante los últimos años, y la aparición de nuevas tecnologías, como el internet de las cosas (IoT), trae aparejadas nuevas amenazas.

Los ataques DDoS buscan sobrecargar los servidores web para inhabilitar el acceso a los sitios web durante horas o incluso días, provocando grandes pérdidas no solo en términos de ingresos, sino también de confianza de los clientes. Así pues, una protección DDoS sólida ya no es una funcionalidad más para las empresas, sino que constituye un elemento imprescindible para cualquier sistema de seguridad. Y, en este sentido, la protección de las infraestructuras on-premises nunca estará al nivel de los sistemas líderes del sector a la hora de mitigar ataques DDoS.

[1] *IDC Infobrief, junio de 2019*

*«OVHcloud, como proveedor de servicios cloud, recibe y mitiga más de 2000 ataques DDoS cada día. Nuestro sistema anti-DDoS protege a todos los clientes por defecto. Hay una razón muy obvia detrás de esta política: un ataque DDoS, si no se mitiga, puede provocar daños colaterales y afectar no solo al objetivo del ataque, sino a todos los servidores anexos del rack. El VAC de OVHcloud, una combinación de tecnologías desarrolladas por la empresa gala para mitigar los ataques DDoS, solo se activa cuando se detecta un ataque de este tipo. En el caso de clientes con necesidades específicas en materia de seguridad, OVHcloud ofrece un filtrado constante del tráfico, es decir, una suerte de activación permanente del VAC».*

**Jakub Słociński, Network Innovation Manager de OVHcloud**

# Seguridad física y redundancia

La mayoría de las empresas no disponen de las funcionalidades de seguridad física que ofrecen los datacenters de terceros, y esto supone un riesgo para el alojamiento de datos sensibles. Un datacenter fiable debe ser como una fortaleza y contar con estrictas medidas de acceso, incluyendo la protección perimetral del edificio mediante vallas de alambre de púas. Los sistemas de videovigilancia y de detección de movimiento funcionan las 24 horas, al igual que los sistemas de detección y extinción de incendios.

Actualmente, la accesibilidad constante, la alta disponibilidad y la resiliencia son elementos clave para muchos servicios informáticos. Conseguir el mismo nivel de redundancia en un cloud alojado a nivel interno puede resultar una tarea titánica. Además, la doble alimentación eléctrica, los generadores de energía, los sistemas de alimentación ininterrumpida (SAI) y los enlaces de red redundantes conllevan elevados costes de mantenimiento y requieren un alto nivel de experiencia por parte de los equipos.

# Conformidad

La norma PCI DSS incluye más de 250 puntos de control y medidas de protección necesarias para ofrecer un tratamiento seguro de los datos de las tarjetas bancarias. Un cloud privado garantiza un mayor control en materia de seguridad, pero no facilita los procesos de conformidad normativa.

Cumplir con las normativas vigentes debe ser una prioridad para cualquier estrategia de planificación, máxime cuando existen diferentes tipos de datos regulados, como los datos de las tarjetas de pago, la información comercial sensible o los datos de clientes. Se trata de un proceso largo y costoso, que a menudo requiere la intervención de expertos informáticos con un buen conocimiento de las reglamentaciones vigentes. Además, los equipos informáticos deben monitorizar de forma permanente los sistemas de seguridad, establecer procedimientos claros en caso de incidencia y utilizar el cifrado de datos para garantizar que la empresa cumple en todo momento con los requisitos de conformidad pertinentes.

# Problemas de rendimiento

Los problemas de rendimiento son un viejo conocido para los entornos virtualizados dinámicos, en los que es difícil predecir cómo los cambios a nivel de infraestructura afectarán al rendimiento de la aplicación. Y es que incluso una simple actualización de software puede alterar el funcionamiento de un ecosistema cerrado. Para sacar el máximo partido a su infraestructura, esta deberá integrar un sistema de monitorización del rendimiento de las soluciones cloud existentes. Con cada nuevo despliegue o cambio relevante, deberá realizar pruebas de rendimiento realistas, preferiblemente automatizadas, que permitan detectar los posibles fallos a tiempo. La implementación de estos procedimientos evitará costes innecesarios para su empresa y le permitirá mantener un estrecho control sobre la relación precio-rendimiento.

# Adquisición innecesaria de recursos

Si quiere desplegar su propio cloud privado con OpenStack o VMware, deberá plantearse la siguiente pregunta: ¿cómo gestionar una infraestructura interna sin renunciar a la agilidad y la escalabilidad?

Y es que, para aumentar de capacidad en una infraestructura propia, necesitará adquirir nuevos equipos de hardware. Al no poder predecir con exactitud la capacidad necesaria, los equipos informáticos suelen adquirir más recursos de los que en realidad necesitan para adaptarse a posibles picos de carga. Como resultado, la empresa debe hacer frente a elevados costes de inversión y a una capacidad de escalado muy limitada.

Cabe preguntarse si una infraestructura «on-premises» puede convertirse realmente en «el cloud», ya que esta tecnología se caracteriza por su gran flexibilidad y escalabilidad, sin necesidad de invertir en hardware adicional. Sin embargo, aunque muchos usuarios creen que un cloud privado significa «on-premises», lo cierto es que no tiene por qué ser así. Un cloud privado es una infraestructura al servicio de una única empresa, por lo que sus recursos no se comparten, sino que están aislados y dedicados a un único cliente. Un cloud privado alojado proporciona a las empresas los medios necesarios para aumentar la flexibilidad y la eficacia operativa, al tiempo que reduce los riesgos asociados a las infraestructuras cloud de empresa.

Un entorno cloud privado alojado con un proveedor de servicios fiable le permitirá delegar en este tercero parte del control y la responsabilidad en materia de seguridad. Así pues, elegir un proveedor de servicios adecuado y con una amplia experiencia en materia de seguridad resulta fundamental para afrontar con éxito los desafíos ligados al cloud.


OVHcloud es un proveedor mundial y líder europeo del cloud que gestiona 400 000 servidores en sus 32 datacenters ubicados en 4 continentes. En sus más de 20 de años de historia, el grupo ha desarrollado un modelo integrado que garantiza un control completo de su cadena de valor, desde el diseño y la construcción de los servidores y datacenters hasta la orquestación de su red de fibra óptica. Este singular enfoque permite que OVHcloud proporcione sus servicios, de manera independiente, a 1,6 millones de clientes en 140 países. Hoy en día, OVHcloud ofrece a sus clientes soluciones de última generación que combinan rendimiento, precios previsibles y una soberanía total de los datos para impulsar su crecimiento con total libertad.