2018

GUÍA DE FALSOS MITOS
sobre Cloud

Ametic

Contenido

1. LOS SERVICIOS DE CLOUD NO PUEDEN CUMPLIR CON EL RGPD

Los servicios Cloud están en perfectas condiciones de cumplir totalmente con los requerimientos que se contemplan en el nuevo Reglamento General de Protección de Datos (RGPD).

En ocasiones se plantea la objeción de que los servicios Cloud generalmente implican transferencias de datos fuera de la Unión Europea. Pues bien, El RGPD no exige en absoluto que los datos deban permanecer en territorio de la UE. A lo que obliga la normativa es a que el responsable del tratamiento informe al interesado de las posibles transferencias internacionales de datos fuera de la UE y se adopten las medidas jurídicas apropiadas.

Por otra parte, el RGPD obliga tanto a responsables como a encargados a adoptar medidas técnicas y organizativas, adecuadas al riesgo, para garantizar la seguridad e integridad de los datos. Los principios de privacidad por defecto (*privacy by default*) y privacidad desde el diseño (*privacy by design)* articulan esta obligación. A este respecto, el RGPD contempla medidas como, entre otras, la pseudonimización o encriptación; medidas que los principales proveedores de servicios Cloud impulsan. Además, los principales proveedores de servicios cloud cumplen con robustos mecanismos de control de accesos, se someten a auditorías y cuentan con certificaciones y estándares internacionalmente reconocidos de privacidad y seguridad[1].

Finalmente, cabe destacar que normalmente en el contexto del Cloud empresarial, el proveedor actúa como encargado del tratamiento (processor), mientras que el cliente actúa como responsable del tratamiento (controller). Ello es así porque el modelo de seguridad en la nube responde a un esquema de responsabilidad compartida. Como ejemplo, en un escenario de Infraestructura como Servicio (IaaS), el proveedor del servicio asume la responsabilidad de garantizar la seguridad física de sus infraestructuras, de la capa de virtualización y la actualización de los equipos para hacer frente a las amenazas de ciberseguridad, etc. Mientras, el usuario de estos servicios debe desarrollar igualmente una cultura de seguridad, administrando el sistema operativo, lo que incluye aplicar las actualizaciones y parches de seguridad, así como los cambios en los recursos que se identifiquen como necesarios.

En consecuencia, de acuerdo con el RGPD, responsables y encargados del tratamiento tienen distintas obligaciones. Para las obligaciones propias del responsable de tratamiento (por ej.: notificación de data breaches, registro de actividades de tratamiento, facilitar a los interesados el ejercicio de sus derechos), los proveedores de servicios cloud colaboran y ponen a disposición del responsable información y mecanismos para que el cliente pueda cumplir con sus obligaciones como responsable de tratamiento.

[1] Por ejemplo: ISO 9001, 27001, 27017, 27018; PCI DSS; SOC 1,2 y 3; DOD CSM niveles 1 a 5; ENS nivel 1 a 3; SSAE 16.

2. LA SEGURIDAD DE LOS SERVICIOS CLOUD SE VE COMPROMETIDA SI LOS DATOS NO SE UBICAN EN UN ÚNICO LUGAR.

La ubicación geográfica de los datos es una de las cuestiones que más preocupa en materia de seguridad. Históricamente, el control de los datos se ha asociado al alojamiento local de la información en instalaciones que se encontraban físicamente en un único país. Sin embargo, las vulneraciones más comunes no requieren acceso físico a un servidor, sino que, por el contrario, explotan una falta de controles de seguridad lógicos implementados de manera eficaz, sin que la ubicación física de los datos tenga relevancia alguna a la hora de hacer frente a las amenazas existentes:

- En primer lugar, cualquier sistema conectado a Internet expone a una organización a diferentes amenazas, que se pueden propagar desde cualquier lugar. Por ejemplo, el reciente ransomware llamado Petya afectó los servicios de atención médica, debilitando sus operaciones y su capacidad para atender a los pacientes. Este fue el resultado de un malware que afectó su centro de cómputo local y se difundió a través de la red. A pesar de un enorme esfuerzo para asegurar los sistemas interconectados a través de firewalls y otros dispositivos anti-intrusión, la experiencia ha demostrado que la seguridad perimetral es una parte muy pequeña de un sistema protegido.

- En segundo lugar, los procesos manuales no son inmunes a los errores humanos. De este modo, los fallos que comenten las personas suelen ser la principal causa de incidentes en ciberseguridad. Un ejemplo común es la no aplicación de parches en sistemas vulnerables con actualizaciones de software publicadas meses antes de un ataque. El proceso manual de actualización de los sistemas es difícil y no siempre se puede realizar de forma regular sin automatización. Otros fallos de seguridad vienen provocados por comportamientos involuntarios o malintencionados por parte de personas que acceden al sistema con cuentas autorizadas para ello (pérdida de credenciales; ataques de phishing e ingeniería social, etc).

En ninguno de estos supuestos la ubicación física de los datos en un único lugar ayuda a mitigar los riesgos. De hecho, consciente de ello, la Comisión Europea está trabajando en el concepto de "Free flow of data", reforzando el abanico de libertades que ya existen en el marco de la Unión Europea. Y es que, prevenir incidentes de seguridad y accesos no autorizados pasa por la adopción de medidas apropiadas y por la implementación de robustas capacidades preventivas y detectoras. Los sistemas deben ser diseñados para limitar la expansión de cualquier tipo de intrusión, de forma que un nodo comprometido tenga un impacto mínimo sobre cualquier otro nodo en la empresa. Asimismo, los proveedores de servicios en la nube desarrollan herramientas de seguridad para permitir a usuarios y clientes cifrar sus comunicaciones e implementar protecciones contra la manipulación de la información. Estas prácticas incluyen desde la encriptación de contenidos, la tokenización, la desintegración de datos o hacer ininteligible el contenido tanto para el proveedor como para cualquier tercero que pretenda acceder al mismo.

En consecuencia, no es extraño que las organizaciones líderes en investigación de tecnología avalen la seguridad de este tipo de servicios, manifestando que el cloud es una de las infraestructuras más seguras del momento. Inversiones que no siempre son posibles para Administraciones Públicas y empresas, que corren el riesgo de obsolescencia con lo que ella supone para la seguridad de los servicios que prestan a la ciudadanía.

3. El BANCO DE ESPAÑA NO PERMITE EL USO DEL CLOUD PARA EL SECTOR FINANCIERO

El Banco de España y el Banco Central Europeo permiten el uso del Cloud por parte de las entidades financieras, como una modalidad de externalización de servicios. Desde el punto de vista de las autoridades de supervisión financiera, el cloud es considerado una forma de externalización, por lo que se aplica la misma normativa aplicable a ésta. En España, la adopción del Cloud por las entidades financieras está sujeta a varios requisitos (ver la Norma 46.ª de la Circular 2/2016 del Banco de España[2]). En este sentido, las entidades financieras deben remitir notificación al supervisor financiero antes de externalizar un servicio en la Nube. Por su parte, la Autoridad Bancaria Europea (EBA por sus siglas en inglés) publicó en diciembre de 2017 —con efectos desde el día 1 de julio de 2018— las recomendaciones sobre la delegación de funciones en proveedores de servicios en la Nube[3], que aplican por igual a toda institución financiera en el ámbito europeo.

4. EXISTEN POLÍTICAS Y CERTIFICACIONES COMO EL ESQUEMA NACIONAL DE SEGURIDAD QUE IMPIDEN EL USO DEL CLOUD EN LA ADMINISTRACIÓN PÚBLICA

No existe ninguna política en la Administración Española que impida la adquisición de servicios en la nube como tal. Si bien, y como en cualquier otra forma de provisión de servicio, existen exigencias derivadas del cumplimiento de políticas de seguridad tales con el Esquema Nacional de Seguridad que habrán de contemplarse y mostrar su adecuación a ellas en los niveles de exigencia que correspondan.

En este sentido el Centro Criptológico Nacional (CCN) especifica cuáles habrán de ser los requisitos que una provisión de servicio basa en la nube deberá cumplir.

[2] Circular 2/2016 del Banco de España: https://www.boe.es/boe/dias/2016/02/09/pdfs/BOE-A-2016-1238.pdf.

[3] European Banking Authority's Recommendations on outsourcing to cloud service providers (December 2017): https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers.

5. LAS ADMINISTRACIONES PÚBLICAS SOLO PUEDEN CONTRATAR EL CLOUD COMO SERVICIO.

Tras la aprobación de la Ley 9/2017 de Contratos del Sector Público, la tradicional duda inherente a la contratación de Cloud ha sido corregida, ya que la nueva ley contempla la contratación de Cloud como **Suministro** (lo mismo que el software tradicional) y no con la categoría de "servicio", que se sigue reservando para la confección de software a medida[4]. Esta modalidad de contratación permite ofertar un coste unitario, sin necesidad de especificar el consumo exacto de cantidades.

[4] Artículo 16.3 de la Ley 9/2017: "*En todo caso, se considerarán contratos de suministro los siguientes: … b) Los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos,* ***en cualquiera de sus modalidades de puesta a disposición****, a excepción de los contratos de adquisición de programas de ordenador desarrollados a medida, que se considerarán contratos de servicios*". El inciso en negrita fue agregado durante la tramitación del proyecto de Ley en el Congreso de los Diputados, mediante la Enmienda 451, que explícitamente hace referencia al Cloud: www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-2-2.PDF#page=384.