Decálogo de buenas prácticas

Riesgos en la nube

Los servicios en la nube ofrecen unas capacidades y ventajas extensas en su uso personal y profesional, permitiendo acceder a la información en tiempo real dónde y cuándo se quiera o ahorrar costes al evitar mantener una infraestructura local. No obstante, este tipo de servicios conlleva un riesgo directo para la seguridad de los datos y su acceso. ¿Cuáles son estos riesgos? ¿Qué podemos hacer para proteger la información confidencial e incluso a nosotros mismos?

¿Qué puede pasar?

El almacenamiento en la nube o el *cloud computing* pueden tener consecuencias nefastas si los servicios no son securizados correctamente:

Pérdida o fuga de la información: Una de las grandes ventajas de la nube es la posibilidad de acceder desde cualquier parte a los datos, aunque esto aumenta el riesgo de que los datos se vean comprometidos debido al mayor número de interacciones y a una base de usuarios más amplia. Todo ello puede provocar pérdidas económicas, daños en la imagen y en la confianza de la propia compañía.

Flujo transfronterizo de datos: La computación en nube suele carecer de una ubicación fija y, por tanto, el cliente puede verse incapaz de determinar en tiempo real la localización de los datos que están siendo procesados o almacenados. Los reguladores se enfrentan al mismo problema. Según la LOPD, la transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable a la legislación española sin autorización del Director de la Agencia Española de Protección de Datos, salvo en algunas excepciones, podrá considerarse como una infracción de tipo muy grave.

¿Cómo me protejo?

- Debe evaluarse, mediante planes de protección de la información, las consecuencias de una posible fuga de información: legales, económicas, personales…, a fin de identificar las medidas a tomar.
- La privacidad debe ser máxima, por lo que separar lógicamente los datos de la propia nube puede evitar el compromiso de ambos sistemas y que las pérdidas sean mayores.
- Tener en cuenta los diversos métodos de cifrado de la información para que, en caso de acceso no autorizado, ésta no pueda leerse fácilmente.
- Además del cifrado, puede hacerse uso de gestores de identidad y acceso e incluso sistemas de *tokens* o autenticación en dos pasos, controlando en todo momento quién accede a la información, por qué y cuándo, minimizando los riesgos.

AUDITORES
Instituto de Censores Jurados de Cuentas de España