ISO 27018: Cloud Computing

La certificación ISO 27018 publicada el 29 de Julio de 2014 , es un código de buenas prácticas en controles de protección de datos para servicios de computación en la nube. Esta norma se une a la anterior ISO / IEC 27001 e ISO / IEC 27002 en el ámbito de gestión de la seguridad de la información y que se dirige específicamente a los proveedores de servicios de nube.

El objetivo abiertamente perseguido por la norma es crear un conjunto de normas, procedimientos y controles a través de los cuales los proveedores de servicios en la nube que, en conformidad con la normativa europea en materia de privacidad, actúan como «procesadores de datos», puedan garantizar el cumplimiento de las obligaciones legales en materia de tratamiento de los datos personales. Al mismo tiempo proporciona a los consumidores potenciales de servicios cloud una herramienta comparativa útil para ejercer su derecho de verificar y auditar a los niveles de cumplimiento de las regulaciones establecidas por el proveedor.

Entre las medidas innovadoras recogidas por la norma ISO 27018 señalaría las siguientes:

- El proveedor, como responsable del tratamiento, tendrá que proporcionar las herramientas adecuadas para permitir y facilitar el ejercicio por el interesado, de los derechos de acceso, rectificación y cancelación en

relación con el tratamiento de los datos.

- En relación con los fines del tratamiento, el proveedor debe velar por el cumplimiento del tratamiento a los únicos usos descritos al cliente en el momento de la contratación del servicio, en particular garantizando que los datos no serán utilizados para fines distintos de los especificados por el cliente, ni para el propósito de marketing directo o publicitario, a menos que haya consentimiento explícito, consenso de que, en cualquier caso, nunca será un requisito establecido por el proveedor para la función del servicio.
- Salvo que exista una prohibición establecida por la ley, la solicitud de divulgación de los datos personales por parte de las autoridades administrativas o judiciales será notificada sin demora al consumidor de servicios de nube.
- En cuanto al tema de la subcontratación, la norma establece, de forma particularmente incisiva, el derecho del cliente a conocer, incluso antes de empezar a utilizar el servicio, toda la cadena de los subcontratistas, los países en los que se establecen, la ubicación de los data centers utilizados por ellos y sus obligaciones en relación con el tratamiento de los datos. También se reconoce el derecho del cliente a oponerse a eventuales cambios en la cadena de los subcontratistas, o de rescindir del contrato.
- El proveedor deberá notificar inmediatamente al cliente toda violación de los datos personales de los que derivan de una pérdida, destrucción, alteración, divulgación o acceso no autorizado, con el fin de permitir que el propietario y los interesados lo□□ notifiquen a las autoridades de control en los plazos establecidos por la ley.

- El acuerdo de servicio debe establecer una política de traslado que detalla el método de restitución, transferencia y / o cancelación de sus datos en poder del proveedor en el cese de los efectos de dicho contrato.
- En relación con las medidas de seguridad de la información, sería conveniente que todo el personal del proveedor y de los subcontratistas estuviese vinculado a un acuerdo de confidencialidad, recibiese una formación adecuada, accediesen a los datos mediante operaciones de autentificación y login.