NUEVOS DESAFÍOS TIC

ISO/IEC 27018

La Norma ISO/IEC 27018 permite a los proveedores de nube pública evaluar riesgos e implementar controles para la protección de los datos personales almacenados. Este documento incluye la privacidad en el modelo ISO para el gobierno de las TIC, que se suma a la calidad aportada por la Norma UNE-ISO/IEC 20000 y a la seguridad según las UNE-ISO/IEC 27001 e UNE-ISO/IEC 27002. Es el primer estándar internacional sobre privacidad en la nube.

Privacidad elevada a la nube

Carlos Manuel Fernández
Gerente TIC
AENOR

Miguel Recio
Socio-Director
Global Data Protection Consulting

El almacenamiento de información en la nube ha dejado de ser algo desconocido para muchas organizaciones, tanto del sector público como del privado. Su uso constituye un ejercicio de responsabilidad, tanto para proveedores como clientes de este servicio, en cuanto al cumplimiento en materia de protección de datos personales o privacidad y seguridad, sin perjuicio de tener que garantizar también la confidencialidad y seguridad de cualquier otro tipo de información. Incluso, en algunos casos, el uso de la nube puede ayudar a alcanzar dicho cumplimiento.

Una gestión adecuada de los activos de la organización, especialmente en lo que se refiere a los datos personales, debe implicar la adopción de medidas que sirvan para que el titular de dichos datos tenga constancia de que su derecho fundamental a la protección de su información es también uno de los objetivos estratégicos de la organización. Además, esta gestión es necesaria para mitigar el riesgo que implica todo tratamiento de datos personales. Y cuando este tratamiento se lleva a cabo en la nube pública, se plantea la necesidad de que el cliente de dichos servicios actúe de manera responsable, tanto desde el punto de vista de la responsabilidad corporativa como del principio de responsabilidad (*accountability*) en protección de datos ante todas las partes interesadas. Es decir, elegir un proveedor de servicios de nube es una decisión responsable que requiere prestar atención a los términos y condiciones del servicio.

En este marco, en 2014 la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) publicaron la Norma ISO/IEC 27018:2014 *Tecnología de la información. Técnicas de seguridad. Código de práctica para la protección de información personal identificable (IPI) en nubes públicas que actúan como encargados del tratamiento*. Se trata de una norma fundamental que se suma a otras sobre seguridad, como la UNE-ISO/IEC 27001:2014 *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos*. Además, están trabajando en el desarrollo de la ISO/IEC DIS 27017 *Information*

technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, cuyo objeto es proporcionar una guía adicional para la implementación de controles relevantes de la ISO/IEC 27002 y también algunos adicionales específicos para los servicios de nube.

Código de buenas prácticas

La ISO/IEC 27018 es el primer estándar internacional sobre privacidad en la nube. Esta norma se basa, fundamentalmente, en leyes y regulaciones emitidas en la Unión Europea. En este sentido, es importante tener en cuenta que la ISO/IEC 27018 puede ser tanto un estándar como un código de buenas prácticas para el proveedor de servicios de nube pública, según el caso, y que su publicación se ha adelantado a anuncios como el de la Comisión Europea de poner en marcha una iniciativa europea de computación en nube[1] e incluso al todavía futuro Reglamento General de Protección de Datos[2].

La ISO/IEC 27018 se basa fundamentalmente en leyes y regulaciones emitidas en la Unión Europea

Desde el punto de vista de protección de datos, la ISO/IEC 27018 se basa en un esquema en el que el cliente del servicio es el responsable del tratamiento, es decir, quien decide sobre el tratamiento de los datos; y el proveedor es el encargado del tratamiento y debe tratar dichos datos siguiendo las instrucciones del cliente (ver gráfico 1).

Proceso tratamiento de datos

Hasta ahora, los proveedores de estos servicios sólo podían certificarse en el ámbito de la seguridad de acuerdo con normas como la UNE-ISO/IEC 27001:2014, que proporciona un sistema flexible para establecer un Sistemas de Gestión de Seguridad de la Información (SGSI) que permita identificar riesgos generales y elegir los controles que hay que aplicar. Pero en la gobernanza de TI y responsabilidad del tratamiento de datos personales, la privacidad seguía siendo una incógnita al no haber parámetros internacionalmente reconocidos.

Con la ISO/IEC 27018 el panorama cambia sustancialmente, ya que ahora los clientes de servicios de nube, las autoridades de protección de datos y otras autoridades reguladoras pueden saber si el proveedor de estos servicios ha adoptado medidas en

Gráfico 1

Proceso de tratamiento de datos

NUEVOS DESAFÍOS TIC

ISO/IEC 27018

materia de protección de datos personales que son, además, auditables y verificables por terceros independientes. Asimismo, les ayuda con el cumplimiento de sus obligaciones en materia de protección de datos personales, lo que puede convertirse en una ventaja competitiva.

Hay que subrayar que desde el punto de vista de protección de datos personales, en concreto de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD), la ISO/IEC 27018 permite aclarar y reforzar las obligaciones exigibles al cliente de servicios, al responsable del tratamiento y al proveedor de servicios. Asimismo, el Esquema Nacional de Seguridad[3] puede beneficiarse tanto de la ISO/IEC 27018 y la futura ISO/IEC 27017. En este sentido, la Guía de Seguridad de las TIC (CCN-STIC-823) sobre utilización de servicios en la nube[4] hace referencia a la ISO/IEC 27001, de manera que las normas o estándares citados reforzarán los controles. También permitirán supervisar el cumplimiento del proveedor de servicios basándose en las auditorías que terceros hagan sobre el mismo, sobre la base de las ISO/IEC 27018 y la 27017, cuando sea publicada.

Privacidad, seguridad y gobierno de TI

Un buen modelo de gobierno de TI no está completo sin una norma sobre protección de datos personales. En la actualidad, casi todas las organizaciones tratan datos personales y, con independencia de cuál sea la estadística que se considere, cada vez más lo hacen en la nube. Ante esta realidad, la ISO/IEC 27018 constituye una herramienta clave. En el caso de proveedores de servicios de nube pública que estén certificados con la Norma ISO/IEC 27001, la ISO/IEC 27018 aporta un conjunto complementario de controles sobre privacidad. Es decir, sirve también para identificar a proveedores de nube pública que tienen un buen gobierno de TI.

Así, el modelo ISO en TIC referido a la nube pública incorpora la calidad (Norma UNE-ISO/IEC 20000), seguridad (Normas UNE-ISO/IEC 27001 e ISO/IEC 27002) y privacidad (Norma ISO/IEC 27018). Y permite que cualquier organización se beneficie de los factores críticos de éxito a los que da lugar este modelo[5]. Esto es, está orientado a los objetivos de negocio, ya sean nuevos proyectos o servicios; consta de dos elementos primordiales que son el ciclo PDCA (motor orientado a la mejora continua) y el control interno de tecnologías de la información (conocimiento); la simplicidad del ciclo PDCA orientado a los objetivos de negocio facilita la labor de gestión y gobierno en las TIC; consiste en aplicar el control interno de tecnologías de la información (considerando los objetivos de negocio) a cualquier nueva tecnología, negocio o servicio; incorpora la calidad y la seguridad en los servicios y proyectos; contempla indicadores (objetivo de la métrica) y métricas orientadas al negocio en el mundo de las TIC; y cualquier proyecto de innovación se puede incorporar en este modelo.

AENOR impulsa este modelo a través de las correspondientes certificaciones que contribuyen a que las empresas sean más competitivas. En el caso de la nube pública, y a través de

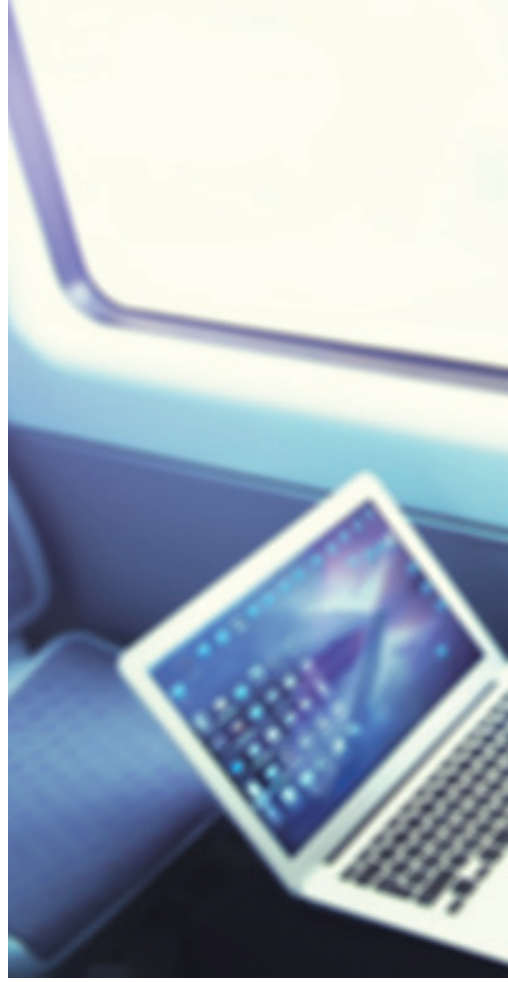

Gráfico 2

Modelo ISO en TIC

la Norma ISO/IEC 27018, facilita que proveedores y clientes de este servicio puedan satisfacer la necesidad de un alto nivel de protección de datos personales. Actualmente, AENOR ha certificado cerca de 300 organizaciones con la Norma UNE-ISO/IEC 27001 y 120 según la UNE-ISO/IEC 20000-1.

Ventajas de la Norma ISO/IEC 27018

Esta norma requiere que el proveedor sea transparente en los términos y condiciones de sus servicios, y en las prácticas de negocio que lleva a cabo; y demuestre compromiso con el cliente para ayudarle a cumplir con las leyes y regulaciones sobre protección de datos personales o privacidad, y seguridad. Además, le facilita la demostración de responsabilidad (*accountability*) en la adopción de medidas y en el desempeño de sus funciones como encargado del tratamiento, y facilita al cliente la prueba necesaria de que ha sido auditado de manera independiente y periódicamente.

En cuanto al cliente, hace posible que controle el tratamiento de los datos personales que ha encomendado al proveedor, pudiendo incorporar como parte del contrato o cláusulas contractuales los compromisos de dicho proveedor en virtud de la ISO/IEC 27018 y sabiendo qué información tiene que solicitarle. Además, tendrá garantías adicionales de limitación del uso de datos personales por parte del proveedor, que no podrá utilizarlos con fines de publicidad o marketing a menos que esté autorizado expresamente.

Por último, las autoridades de protección de datos y otras autoridades reguladoras podrán obtener fácilmente garantías de cumplimiento en caso de que sea necesario; podrán considerar la Norma ISO/IEC 27018 y otros estándares como una medida proactiva por quienes están sujetos al cumplimiento, ya sea el responsable o el encargado del tratamiento. Asimismo, les servirá de marco de referencia para impulsar buenas prácticas y esquemas de autorregulación en materia de protección de datos personales. ◗

NOTAS

(1) Al respecto, puede verse el comunicado de prensa de la Comisión Europea sobre "Un mercado único digital para Europa: la Comisión establece 16 iniciativas para conseguirlo" (IP/15/4919), Bruselas, 6 de mayo de 2015. Disponible en *http://europa.eu/rapid/press-release_IP-15-4919_es.htm*

(2) Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), COM(2012) 11 final, Bruselas, 25 de enero de 2012. Disponible en *http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012PC0011&qid=1431769787169&from=ES*

(3) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de Administración Electrónica. Disponible en *www.boe.es/buscar/doc.php?id=BOE-A-2010-1330*

(4) Disponible en *www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/823-Seguridad-en-entornos-cloud/823-Cloud_Computing_ENS.pdf*

(5) Véase FERNÁNDEZ SÁNCHEZ, Carlos Manuel y PIATTINI VELTHIUS, Mario (coords.) (2012), *Modelo para el gobierno de las TIC basado en las normas ISO*, España. Pág. 18.