Seguridad en la gestión de proveedores o encargados de tratamiento.

ISO/IEC 27018 y RGPD

En este artículo vamos a explicar cómo gestionar la seguridad con nuestros proveedores, haremos una breve introducción a éste estándar internacional sobre la seguridad en cloud, que facilitará a responsables y encargados de tratamiento el cumplimiento del Reglamento General de Protección de Datos, en adelante RGPD.

Empecemos con algunos datos obtenidos por el INE del primer trimestre de 2017, donde concluye entre otros datos, que 1 de 4 empresas compra algún servicio cloud, y que entre las empresas que compran servicios de Cloud, el 74,4% se decantan por el e-mail, más del 70% almacena ficheros, o más del 60% ubica los servidores de bases de datos en la nube. Puede consultar más datos en la tabla obtenidos de la fuente:

Cloud Computing. Porcentajes

	1er Trim. 2017	1er Trim. 2016
Empresas que compran soluciones de Cloud Computing	24,6	19,3
Servicios comprados por las empresas:		
E-mail(1)	74,4	71,2
Almacenamiento de ficheros(1)	70,8	68,7
Servidor de bases de datos de la empresa(1)	63,4	59,6
Software Office (procesadores de texto, hojas de cálculo…)(1)	42,3	38,5
Aplicaciones de software para tratar información sobre clientes(1)	31,7	29,5
Capacidad de computación para ejecutar el propio software de la empresa(1)	28,5	30,0
Aplicaciones de software financiero o contable(1)	31,0	27,6

(1)Porcentaje sobre el total de empresas que compran soluciones de Cloud Computing

Fuente: INE-Instituto Nacional de Estadística

Es evidente la evolución en el uso de estos servicios, por diversos y heterogéneos motivos, véase por disponer de sistemas fiables y actuales, por mejorar el soporte y la especialización del servicio, por la flexibilidad y capacidad de crecimiento, o incluso por las medidas de seguridad que, se supone, podemos obtener al contratar servicios en la nube.

Cualquier organización, como responsable de los datos que trata, y según el nuevo *principio de responsabilidad proactiva*, del inglés accountability, deberá elegir a sus proveedores o encargados de tratamiento, de forma que éstos garanticen y estén en condiciones de demostrar que el tratamiento se realiza conforme el RGPD, es decir, que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento, garantía que se debe propagar a posibles subcontrataciones, si las hubiera.

¿Y cómo hago esto? Me preguntan clientes en los proyectos, y algunos alumnos en nuestras formaciones. Yo lo explico de la siguiente forma y parece entendible…

Lo que tenemos que hacer es **asegurar que nuestro proveedor o encargado de tratamiento no sólo es capaz de aplicar las medidas de seguridad** (confidencialidad, integridad y

disponibilidad) sobre nuestros datos, de acuerdo a la apreciación de riesgos que hallamos realizado, **sino que también que es capaz de demostrarlo**.

Para demostrar la capacidad de aplicar la medidas que nosotros requerimos, normalmente vamos a buscar un proveedor de cierto prestigio o confianza, que en la descripción técnica del servicio incluya información sobre las medidas de seguridad, y fundamentalmente que en el contrato que regula el servicio contratado se encuentren descritas, entre otras: gestión de incidentes, disponibilidad de sistemas, monitorización, cifrado de comunicaciones, datos y bases de datos, backup y restauración, control de acceso y autenticación, planes de contingencia en caso de incidentes incluso en caso de fuerza mayor, etc.

Pero lo anterior no es suficiente para cumplir con el RGPD, ni garantía de nada. Ahora viene lo complejo, que el proveedor demuestre su capacidad para llevar a cabo estas medidas y la efectividad de las mismas. Para ello existen diversas opciones, cual aplicar en cada caso dependerá del tipo de cliente y proveedor, tamaño, tipo de relación entre las partes, etc. Se describen a continuación:

- Incluir en el contrato el derecho a realizar una auditoría o verificación de las medidas de seguridad, que sería llevada a cabo según los plazos y planificaciones estipuladas. Los costes de la misma se pueden negociar.
- Incluir en el contrato la obligación al proveedor de realizar auditorías de las medidas de seguridad, utilizando una empresa especializada, y remitir el informe o un resumen de las conclusiones del mismo.
- Solicitar el proveedor adherirse a códigos de conducta o certificarse en estándares o esquemas que ayuden a demostrar el cumplimiento del RGPD. Este mecanismo es adicionalmente, sin duda, una herramienta para obtener ventaja competitiva por parte de proveedores comprometidos con la seguridad y privacidad, frente a otros menos maduros. Consulte si su proveedor se encuentra certificado.

Hablando de las certificaciones, y lo que nos quedará por ver en este ámbito de la privacidad…, vamos a hablar brevemente de cómo ISO/IEC 27018 puede ayudar a responsables (PII controller) y proveedores (PII processor) al cumplimiento del RGPD.

ISO/IEC 27001, conocida y extendida norma internacional, especifica los requisitos para establecer, implementar, operar, revisar y mejorar un sistema de gestión de seguridad de la información , en adelante SGSI, **que además es certificable**. Permite establecer un modelo de responsabilidades y de gestión para la seguridad de la información, incluida la privacidad, y se apoya en la apreciación de riesgos y un conjunto de 114 controles para proteger la información en sus tres dimensiones: confidencialidad, disponibilidad e integridad (para más detalle sobre los controles consulte ISO/IEC 27002).

ISO/IEC 27018 Código de práctica para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores PII, se centra en la protección de los datos personales en la nube. Su contenido especifica un conjunto de guías basadas en los controles de ISO/IEC 27002, teniendo en cuenta los requisitos regulatorios para la protección de información de identificación personal. Su contenido se puede resumir de la siguiente forma:

- Guías que complementan alguno de los 114 controles de ISO/IEC 27002
- Anexo A. Conjunto de controles extendidos, que especifica nuevos controles y guías.

Antes de entrar en mayor detalle, hay que especificar, que las entidades de certificación están realizando auditorías y emitiendo certificados ISO/IEC 27018, sólo bajo un SGSI certificable, ya que la norma no es certificable en sí misma.

A continuación se indican el nivel de cambio o modificación que supone el estándar respecto a la guía base, como se aprecia no son muchos.

ISO27001 – ISO27002	ISO27018
5. Information security policies	Cambios menores
6. Organization of information security	Cambios menores
7. Human resource security	Cambios menores
8. Asset management	Cambios menores
9. Access control	Cambios menores
10. Cryptography	Cambios menores
11. Physical and environmental security	Cambios menores
12. Operations security	Cambios moderados
13. Communications security	Cambios menores
14. System acquisition, development and maintenance	Sin cambios
15. Supplier relationships	Sin cambios
16. Information security incident management	Cambios menores
17. Information security aspects of business continuity management	Sin cambios
18. Compliance	Cambios menores

Finalmente, se describen a alto nivel los nuevos controles, algunos coinciden con los principios del RGPD:

- A1. Consentimiento
- A2. Propósito de legitimidad y especificación
- A3. Limitación de la colección
- A4. Minimización de datos
- A5. Limitación de uso, retención y divulgación
- A6. Exactitud y calidad
- A7. Transparencia
- A8. La participación individual y el acceso
- A9. Responsabilidad
- **A10. Seguridad de la información (13 nuevos controles)**
- A11. Cumplimiento de la privacidad

Los nuevos controles están relacionados con: acuerdos de confidencialidad, restricción para obtener copias impresas de datos, control y registro de restauración de datos, protección de los datos sobre dispositivos de almacenamiento que salen de las instalaciones, uso de dispositivos removibles no cifrados, cifrado de datos sobre redes abiertas, eliminación segur de copias impresas, identificadores de usuario únicos, registro de usuarios autorizados, gestión de identificadores de usuarios, medidas en los contratos, procesamiento subcontratado, acceso a datos sobre espacio previamente utilizado.

Antonio Martínez

Responsable GRC

Áudea Seguridad de la Información