Cloud Security Alliance-España adapta Cloud Controls Matrix 3.0.1 al ENSv2

Beatriz Blanco

Miembro de Cloud Security Alliance España de ISMS Forum Spain. IT Audit Manager de Amadeus IT Group

Jorge Laredo

Miembro de Cloud Security Alliance España de ISMS Forum Spain. Manager de Hewlett Packard Enterprise

CLOUD SECURITY ALLIANCE España, continuando en su actividad de adecuar la matriz de controles de referencia para la seguridad *cloud* (CCM) al entorno español, ha incorporado las especificaciones de la última versión del Esquema Nacional de Seguridad (RD 951/2015) y actualizado las referencias al Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

El objetivo principal de este ejercicio es impulsar la adopción de servicios de *cloud* en España, permitiendo tanto el cumplimiento normativo como la seguridad efectiva de los datos.

Cloud Security Alliance España (CSA-ES), iniciativa impulsada por ISMS Forum (Asociación Española para el fomento de la Seguridad de la Información), ha publicado una guía que recoge los controles de referencia más importantes de seguridad en *cloud*. Esta guía, que es una revisión del trabajo que CSA-ES realizó en una versión anterior de la misma, toma como base los controles publicados en la Cloud Controls Matrix v3.0.1[1] (en adelante CCM o la matriz) y los mapea con los requisitos de la normativa española más relevante actualmente en materia de seguridad y privacidad:

- RLOPD: Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal. Se compara con el "Título VIII de las medidas de seguridad en el tratamiento de datos de carácter personal".
- ENSv2: Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica.

(La Cloud Controls Matrix v3.0.1, con la inclusión del mapeo actualizado, está disponible para su descarga en de la web de ISMS Forum Spain a través del enlace: https://www.isms-forum.es/CCM301ENS2)

Como resultado del trabajo realizado, proveedores y clientes disponen en la guía de la referencia nacional más completa para la evaluación de riesgos de seguridad en el ámbito del *cloud* y, en particular, en la Administración Pública dada la referencia actualizada al ENS. El objetivo principal de la versión española del CCM es impulsar la adopción de servicios de *cloud* en España, permitiendo tanto el cumplimiento normativo como la seguridad efectiva de los datos.

La versión 3.0.1 del CCM actualiza la versión 3.0 y contiene un total de 133 controles de referencia que cubren tanto aspectos de cumplimiento y gobierno, como de arquitectura y de tipo técnico, lo que permite reducir los riesgos, las amenazas y las vulnerabilidades en la nube. La versión mundial (publicada por Cloud Security Alliance Global) incluye el mapeo con diversas normas y estándares tanto internaciones como nacionales (principalmente de Estados Unidos, aunque también de Europa, Canadá, Alemania y México), entre las que cabe destacar COBIT 5, ENISA IAF, Directiva 95/46/EC, FedRAMP, ISO/IEC 27001:2013, NIST sp800-53 R3 y PCI DSS v3.0.

Desde CSA-ES se vio la utilidad de establecer también la correspondencia entre la CCM y las principales regulaciones españolas, el RLOPD y el ENS. Este mapeo hace evidente que el CCM va más allá del mero cumplimiento normativo, por lo que

algunos de sus controles no pueden ser relacionados directamente con requisitos de carácter regulatorio.

Cualquier entidad que pretenda gestionar datos de carácter personal en un entorno *cloud* no solo debería tener en cuenta los controles del RLOPD coincidentes con el CCM, sino que también debería considerar la evaluación del resto de controles de esta matriz. Ahora bien, dado que el RLOPD pone más énfasis en las medidas de seguridad orientadas a preservar la privacidad de los datos, mientras que la CCM incluye controles relacionados con la seguridad desde un punto de vista más amplio, en torno al 42 por ciento de los controles de la matriz no puede ser relacionados de forma directa con artículos del RLOPD.

Actualización al ENSv2

En la anterior adaptación de la versión 3 ya se hacía el mapeo con el RLOPD y el ENS, por lo que la 'novedad', aparte de usar la última versión del CCM, es la actualización al ENSv2. El Esquema Nacional de Seguridad tiene una guía de controles con una distinción por niveles de seguridad en función de la criticidad de la información, la cual se ha tenido en cuenta en el mapeo. Asimismo el ENSv2 recoge medidas relacionadas con la propiedad intelectual del *software* propietario, las restricciones de acceso al código fuente de las aplicaciones o programas, ciertos requisitos contractuales y reglamentarios en relación con el acceso de terceros o las medidas de seguridad concretas sobre el uso de redes inalámbricas. Considerando el amplio espectro de medidas de seguridad que cubre el ENS, tan solo un 10 por ciento de los controles del CCM v3.0.1 no se pueden relacionar directamente con medidas contenidas en el ENS.

Dada la utilidad del mapeo, el propio Centro Criptológico Nacional (CCN) ha decidido incluir el mapeo elaborado por CSA-ES de CCM con el ENSv2 como un anexo adicional en su *Guía de Seguridad de las TIC CCN STIC* 823. Dicha guía incluirá, además del mapeo mencionado con CCM v3.0.1, el mapeo con el estándar ISO/IEC 27001.

Los controles de la matriz CCM ayudan a cumplir con los requerimientos del ENS en un entorno *cloud* y aportan medidas de seguridad adicionales de interés para las administraciones públicas. En su estado de madurez actual se puede considerar como una referencia ineludible en la valoración de la seguridad de un entorno *cloud*. De este modo, las administraciones públicas pueden contar con esta herramienta y utilizarla como marco de referencia para evaluar el grado de cumplimiento de sus proveedores de *cloud*, ya sean servicios internos o externos, con respecto a sus requerimientos y expectativas en materia de seguridad y mapear asimismo si dichos requerimientos están alineados con las exigencias del ENS.

Posibilidades de la CCM

Las posibilidades que ofrece el uso de la CCM son numerosas y muy prácticas; entre otras, puede tomarse como base para la evaluación de proveedores de *cloud* en la fase de selección y licitaciones, así como en renovaciones posteriores, y como herramienta para monitorizar y auditar a aquellos terceros que ya estén prestando un servicio de *cloud*. Del mismo modo, también resulta una herramienta muy práctica desde el punto de vista de los propios proveedores de *cloud*, quienes pueden usarla como referencia para calibrar su nivel de cumplimiento con respecto a los estándares que sus clientes pueden estar requiriendo en base a sus necesidades de seguridad o cumplimiento normativo o regulatorio.

Al igual que la seguridad en el *cloud* evoluciona, es propósito de Cloud Security Alliance España (CSA-ES) mantener actualizados sus trabajos. En relación al CCM se tienen en el horizonte dos objetivos: traducir al español el Cloud Control Matrix v4, tras su publicación por CSA en inglés, y adecuar el mismo al ENSv2 y a la regulación de protección de datos adaptada a la nueva regulación europea. Con ello, el mercado español dispondrá de forma actualizada a sus necesidades el principal catálogo de controles para la seguridad en el *cloud* a la vez que se facilita el cumplimiento de los diferentes estándares y normas que una entidad puede estar obligada a cumplir. ■

[1] Descargable desde la página web de CSA en https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/