STAR, certificación de la seguridad de los proveedores de servicio desde la nube

El año 2013 será señalado en el futuro por el establecimiento de la colaboración entre *Cloud Security Alliance* (CSA) y *British Standards Institution* (BSI) que ha permitido la publicación y puesta en marcha del esquema de certificación STAR. Un esquema de certificación del entorno *cloud* no ligado a un fabricante de tecnología concreto, que aborda las barreras encontradas para la correcta adopción de la nube por las organizaciones para ofrecer un entorno de confianza entre prestadores de servicios *cloud* y sus clientes/consumidores.

Agustín Lerma / Mariano J. Benito

La Certificación STAR

La Certificación STAR (*Security, Trust & Assurance Registry*) es una iniciativa conjunta de *Cloud Security Alliance* y de BSI para ofrecer al mercado, y en particular a los proveedores de servicio desde la nube, un mecanismo de certificación de los proveedores *cloud,* que sea global, confiable y siga las mejores prácticas de acreditación de certificados, de forma que se mejore la transparencia actual en estos servicios y la garantía de una prestación de servicio con las condiciones de seguridad necesarias.

STAR se configura pues como una certificación acreditada para quien provee servicios desde *cloud*, ya sea en modelo de nube pública como híbrida, comunitaria y/o privadas. De esta forma, el proveedor puede aumentar la confianza de sus clientes en sus servicios al ofrecer garantía de que la provisión de servicios se realiza en un entorno de seguridad adecuado y adaptado a las condiciones específicas de la prestación de servicios en *cloud*.

STAR se basa en un entorno de control extendido específico para entornos *cloud* (OCF, u *Open Certification Framework*), desarrollado por la *Cloud Security Alliance*, que se apoya en un Sistema de Gestión de Seguridad de la Información ISO 27001 y su marco de controles estándar ISO 27002.

El diseño y la ejecución de la Certificación STAR surge de la colaboración entre dos entidades líderes. Por una parte, CSA, *Cloud Security Alliance*, como asociación de profesionales especialistas en el modelo de servicios *cloud*, su seguridad y su operación, que aporta conocimiento experto en los distintos modelos de servicio que se pueden prestar en la nube y los mecanismos de control y de seguridad que son recomendables para que la prestación de servicios se desarrolle en condiciones de seguridad adecuadas.

Por otra parte, BSI son expertos en el desarrollo y certificación de esquemas acreditados que aporten todas las garantías de solvencia y veracidad exigibles a un esquema que pretenda aportar confianza y transparencia a sus usuarios.

Necesidad de la Certificación STAR

El concepto de *Cloud Computing* fue mencionado por primera vez en el año 2006 [1]. Sin embargo, la velocidad de adopción del concepto por las organizaciones y el alcance de dicha adopción es sustancialmente más reducido que el de otras tecnologías TI (en plazos de tiempo comparables) y más reducido que las expectativas que el potencial de este modelo de servicios ofrece.

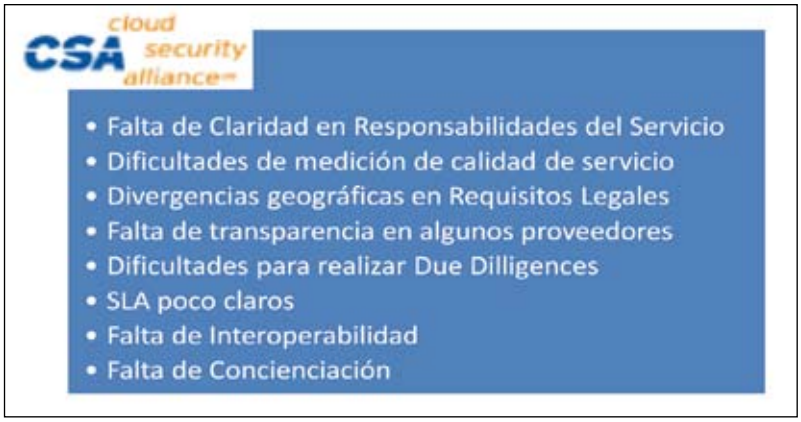

Figura 1. Barreras que entorpecen la adopción de *Cloud Computing*.

En un intento de identificar qué razones subyacen en esta situación, CSA ha identificado 8 barreras (ver **Figura 1**) que entorpecen la adopción de *Cloud Computing* por las organizaciones. Todas ellas apuntan en la misma dirección: la prestación de servicios *cloud* se está desarrollando en un entorno con ausencia de confianza entre los distintos actores. Este escenario se ve agravado en tanto que los servicios *cloud* son prestados por un tercero, por lo que las necesidades de los clientes no son únicamente de prestación correcta de servicio, sino del modelo de gestión de los servicios prestados, como ocurre en cualquier servicio prestado por un tercero. Y CSA sostiene que los consumidores no disponen de mecanismos sencillos para evaluar y/o comparar la resiliencia, capacidad de protección de la información e interoperabilidad de los proveedores *cloud* del mercado.

Obviamente, era preciso tomar acciones para solucionar el problema identificado. Algunos actores sostienen la necesidad de desarrollar regulaciones legales que exijan condiciones de transparencia en el servicio y, efectivamente, existen iniciativas de este tipo en el espacio UE y otros países. Sin embargo, si existiese un sello o certificación adecuado para entorno *cloud* enfocado a la creación y mantenimiento de esta relación de confianza, éste podría ser un mecanismo válido.

Origen de la Certificación. Elementos que la integran

La iniciativa STAR surge en el año 2011 dentro de las iniciativas de la *Cloud Security Alliance*, como mecanismo para mejorar la transparencia de la oferta de servicios *cloud.* Para ello se crea el registro STAR de forma que fuera una fuente públicamente accesible, consultable por los clientes. Esta iniciativa se basaba en el uso de cuestionarios de auto-evaluación [2] y la publicación de los mismos, de forma que estuvieran accesibles a los usuarios de servicios *cloud*.

CSA se apoyó para la confección de los cuestionarios en los trabajos previos realizados para el establecimiento y sistematización de una Base de Conocimiento de Mejores Prácticas sobre seguridad en *cloud* que se materializó en dos documentos básicos:

- La "Guía de Seguridad de Áreas Críticas en Cloud Computing" o CSA-Guide. Este documento, disponible en inglés [3] y en español [4], contiene la base de conocimiento de las mejores prácticas para la seguridad en la nube identificada por los miembros de CSA a nivel mundial.
- "Cloud Control Matrix" o CCM. Este documento también está disponible en inglés [5] en versión 3 y en español [6] en versión 2, y contiene una referencia del total de controles contenidos en la guía (136 en la versión 3), junto con la relación identificada entre los controles específicos para *cloud* y otras bibliotecas de controles de seguridad y/o regulaciones legales. La CCM es, asimismo, el índice de referencia de controles de

[1] http://www.wired.com/wired/archive/14.10/cloudware.html
[2] https://cloudsecurityalliance.org/star/#_registry
[3] https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/
[4] https://www.ismsforum.es/noticias/389/el-capitulo-espanol-de-csa-publica-la-traduccion-al-espanol-de-la-csaguide-v3.0/
[5] https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/
[6] http://www.ismsforum.es/ficheros/descargas/version-espanola-del-cloud-control.xlsx

seguridad *cloud* que se emplea en la certificación STAR.

Todos los documentos indicados están disponibles para su descarga en los enlaces referenciados, y su conocimiento y/o aplicación son necesarios para afrontar la certificación.

Los cuestionarios de autoevaluación son únicamente un primer paso en la certificación STAR, puesto que las garantías que proporcionan son inferiores a los que puede ofrecer una certificación acreditada. En ese contexto, surge la colaboración entre CSA y BSI y la certificación STAR.

Figura 2. Proceso de certificación de CSA-STAR.

CSA STAR e ISO 27001. El papel de los entornos de control extendidos

Además de la experiencia de BSI en la definición de estándares, auditoría y certificación de sistemas de gestión, el hecho de que la especificación original de definición de un sistema de gestión de seguridad de la información, BS 7799-2, fuera definido por BSI, influyó en la decisión de CSA para afrontar la definición de un ámbito de control extendido asociado a un sistema de gestión ISO 27001.

También la experiencia previa de BSI en auditoría y certificación de otros ámbitos extendidos de control de riesgo asociados a un sistema de gestión BS7799-2 o ISO 27001, como por ejemplo el estándar de seguridad para loterías, WLA-SCS:2006 / 2012 fue una buena referencia para CSA a la hora de elegir socios en este proyecto.

La certificación CSA STAR ha sido desarrollada para gestionar elementos de seguridad en *cloud* específicos como un elemento de control extendido de un SGSI definido según ISO 27001. Una de las principales razones para el desarrollo de esta certificación es que el 56% de las organizaciones desconocen qué hacen sus proveedores de nube para proteger los activos de información de sus clientes.

¿Cómo puedo certificarme en STAR?

El requisito necesario para poder emitir un certificado CSA STAR es disponer de un sistema de gestión certificado según ISO 27001, cuyos alcances sean coincidentes. Hay que indicar que la fecha de validez del certificado CSA STAR se adapta al existente de ISO 27001.

Una vez completados y validados los cuestionarios de Auto-Evaluación (Level 1, o STAR Self-Assesment) anteriormente mencionados, y con la consideración de las recomendaciones expuestas en el punto anterior, los pasos para optar a una certificación CSA STAR son los mismos que para cualquier otro sistema de gestión y módulo de control extendido:

- Una vez comunicado a BSI el interés en certificación CSA STAR, se requerirá información sobre el SGSI, certificado, alcance, Declaración de aplicabilidad, etc. para poder emitir una oferta de Auditoria de certificación.
- Una vez aceptada la oferta de certificación, se designa auditor y se fijan fechas y condiciones de auditoria.
- Se realiza la auditoria de certificación y se emite certificado con nivel de Oro, Plata o Bronce.
- Ser realizan auditorias de revisión anual (CAV, *Continuous Assessment Visits*, Visitas de Auditoria Continua) coordinadas entre ISO 27001 y CSA STAR.

Figura 3. Esquema de la certificación CSA-STAR.

El proceso de certificación continua garantiza que los niveles de cumplimiento y madurez del sistema de gestión y de los elementos de control de riesgo (ISO 27001 Anexo A, CSA STAR, PCI-DSS, WLA-SCS, etc.) se mantienen durante el periodo de validez del certificado ISO 27001 y CSA STAR.

Este proceso únicamente puede realizarse con la colaboración de BSI como entidad de certificación, puesto que STAR es el resultado de un esfuerzo conjunto de BSI y CSA.

Existen ya varios proveedores que han completado la certificación STAR y disponen de su certificado. Por ejemplo, Pulsant[7] o HP-UK[8].

¿De qué información dispongo para la certificación STAR?

Una de las ventajas implícitas en la certificación STAR es que la práctica totalidad de la información necesaria está disponible, publicada y puede obtenerse de forma gratuita. Entre esta información, se encuentran la matriz CCM y la CSA-Guide, antes mencionada. Adicionalmente, en los sitios web de CSA, tanto en inglés[9] como en español[10] puede conseguirse información adicional en ambos idiomas.

Por otra parte, la información precisa para la certificación ISO 27001 puede encontrarse a través de BSI[11][12], o en otros canales como ISO.

Conclusiones

Por todo ello, la iniciativa STAR ofrece a todos los actores del mercado *cloud*:

- Un marco de referencia completo que permite establecer requisitos de seguridad; tanto los que ha de satisfacer un Proveedor de Servicio *Cloud*; como los que debe exigir un cliente para poder disponer de garantía de seguridad suficiente en la nube.
- Un mecanismo de aseguramiento de la eficaz implantación de estos requisitos, que sea sostenible en el tiempo, verificado por terceros y verificable por cualquier parte.

De forma que se genere el entorno de confianza para *cloud* que todas las Partes (clientes, proveedores, reguladores, profesionales, ciudadanos) han señalado como necesario. ■

Agustín Lerma
Product Manager
BSI IBERIA
Lead Assessor
CSA STAR
Agustin.lerma@bsigroup.com

Mariano J. Benito
Coordinador CTO
CAPÍTULO ESPAÑOL DE CSA (CSA-ES)
CISO
GMV SOLUCIONES GLOBALES INTERNET S.A.U.
mjbenito@gmv.com

[7] http://www.bsigroup.com/LocalFiles/en-GB/cloud-security/STAR-certification/BSI-STAR-Case-Study-Pulsant-UK-EN.pdf
[8] http://www.bsigroup.com/LocalFiles/en-GB/cloud-security/STAR-certification/BSI-STAR-Case-Study-HP-UK-EN.pdf
[9] https://cloudsecurityalliance.org/
[10] https://www.ismsforum.es/csa-es
[11] www.bsigroup.es/cloudsecurity
[12] www.bsigroup.es/formacioncloudsecurity