Realizado por el Capítulo Español de la Cloud Security Alliance

Primer informe sobre Cumplimiento en "la Nube"

El pasado 26 de mayo de 2011, el Capítulo Español de la Cloud Security Alliance (CSA-ES) publicó el primer informe sobre el Cumplimiento en la Nube, aportando un enfoque práctico que ayude a abordarlo. No podemos ver solo los beneficios de la computación en la nube y obviar sus implicaciones y riesgos, en especial, en todo lo relacionado con las obligaciones legales y regulatorias. Tampoco podemos recurrir sistemáticamente a argumentos de seguridad y cumplimiento para paralizar las iniciativas en "la nube". Todo es cuestión de buscar un equilibrio, identificando qué servicios, cómo y cuándo se pueden ir implantando de manera adecuada en los diferentes modelos de computación en "la nube". La evolución será gradual y la capacidad de garantizar el cumplimiento determinará su velocidad.

Luis Buezo

¿Por qué un informe de Cumplimiento?

La computación en "la nube" está incrementando todavía más la brecha existente entre los requerimientos de cumplimiento con las diferentes regulaciones de carácter nacional e internacional que afectan a los servicios TIC y la capacidad real de garantizar dicho cumplimiento. Todos los meses hay noticias que ayudan a entender el verdadero reto al que se enfrentan las organizaciones y en foros de expertos se debate abiertamente la imposibilidad, en muchos casos, de garantizar el cumplimiento. Sirva como ejemplo la discusión a lo largo del mes de julio de 2011 sobre el comentario de una empresa proveedora admitiendo la posibilidad de entrega de cualquier dato al Gobierno de los Estados Unidos en cumplimiento con el "USA Patriot Act 2001", independientemente de dónde viva el usuario, de dónde están almacenados sus datos y de que el contrato sea con una subsidiaria local. Funcionarios de la Unión Europea se han declarado en contra de este planteamiento; especialmente cuando se ignora la garantía de privacidad de los datos almacenados en la Unión Europea. ¿Estamos hablando de incompatibilidad de requerimientos? Se puede añadir más complejidad cuando dentro de la misma Unión Europea existen regulaciones como la "UK Regulation of investigatory Powers Act 2000" ,que permite al Gobierno del Reino Unido acceder a datos almacenados en dicho país en garantía de los intereses del bienestar económico del Reino Unido y otros motivos.

Ilustración 1. Organización del contenido del documento

Una de las primeras conclusiones del informe es que, en la computación en "la nube", la simple determinación de la legislación aplicable ya es un reto. El informe propone diferentes recomendaciones; y también especifica que una empresa cliente establecida en el territorio del EEE, independientemente de dónde esté ubicado su proveedor de servicios en "la nube", será la responsable en términos de protección de datos y le será de aplicación la ley del Estado en que esté establecida.

Es obvio que en este contexto, el primer informe de cumplimiento no se presenta como la solución final a cualquier problema de cumplimiento en "la nube"; pero sí representa un primer paso hacia adelante para hacer frente a esta necesidad.

Un año de trabajo

El Capítulo Español de la Cloud Security Alliance (CSA-ES) se constituyó el 21 de mayo de 2010. Empezó impulsado por ISMS Forum Spain y Barcelona Digital, con 91 miembros fundadores, representativos de los distintos actores de la industria de la computación en "la nube" en España. En la actualidad, ya cuenta con más de 200 miembros.

Fue el primer Capítulo de ámbito nacional de la CSA y se fundó con la misión de avanzar en el desarrollo seguro de la computación en "la nube" en España, constituyendo un foro de discusión y aglutinamiento de los profesionales de seguridad en este entorno de trabajo. Cada Capítulo regional selecciona un ámbito específico de interés. El hecho de que la regulación europea y española sobre la privacidad sea un referente a nivel mundial, ha impulsado que CSA-ES seleccionara como propia el área de "Cumplimiento en la Nube", marcándose como objetivo desarrollar un informe sobre el cumplimiento.

Una vez constituido el Capítulo, se definieron 3 grupos de trabajo enfocados al desarrollo del informe. Cada grupo de trabajo se centraría en

un área específica:

• Privacidad y cumplimiento normativo en "la nube".

• SGSI y gestión de riesgos en "la nube".

• Contratación, evidencias electrónicas y auditoría en "la nube".

Los grupos trabajaron de forma autónoma, coordinados a su vez por el comité operativo de CSA-ES para garantizar la coherencia de los resultados. La Junta Directiva de CSA-ES, junto con el Consejo Asesor (órgano de CSA-ES formado por expertos, cuyo objeto es asesorar, proponer planes de acción al Capítulo y liderar la interlocución con las autoridades de control), garantizaron los niveles de calidad requeridos para el documento. Se han implicado 49 coautores que, tanto a nivel de grupos de trabajo, Junta Directiva, Comité Operativo como Consejo Asesor, han compartido sus conocimientos para poder hacer realidad este documento.

Enfoque y estructura del informe

El marco referencial para el desarrollo de este primer informe ha sido el ámbito "nacional", focalizándose en los aspectos de privacidad, pero también incluyendo otras normas exigibles en España, así como mejores prácticas, como la ISO/IEC 27001:2005 sobre Sistemas de Gestión de la Seguridad. Se ha prestado especial atención a aspectos relacionados con la contratación, evidencias y auditorías como piezas fundamentales de la relación entre cliente y proveedor de servicios en "la nube".

En la computación en "la nube" hay diferentes actores y el informe tiene que ser útil para todos. La única forma de mejorar en esta área es implementando un entorno común y válido que permita a todos la gestión de sus correspondientes cumplimientos. El estudio incorpora recomendaciones tanto para clientes como proveedores, además tiene en cuenta los diferentes tipos de servicio (SaaS, PaaS e IaaS) y de despliegues ("Nubes" públicas, privadas, internas, híbridas, etc.)

Con el objetivo de no generar información redundante, el informe se construye como complemento a otras investigaciones de referencia ya publicadas anteriormente, como es el caso de las principales amenazas sobre la computación en "la nube", detalladas en el documento "Top Threats to Cloud Computing v1.0" [Cloud Security Alliance, marzo 2010], o cómo realizar evaluaciones de riesgos en la computación en "la nube" a partir de la información incluida en el documento "Cloud Computing Security Risk Assessment v1.0" [ENISA, noviembre 2009]; así como otros documentos de INTECO o del WPF (World Privacy Forum).

Al abordar el informe, tal y como se puede ver en la figura 1, la problemática de cumplimiento se dividió en dos niveles: un primer nivel, en cuanto a inventario de normas, tanto de ámbito general (que aplican a cualquier organización) como de ámbito particular (que aplican con carácter individual a un contrato o normas sectoriales). diferenciando también aquellas de obligado cumplimiento (ordenamiento jurídico) de las voluntarias (mejores prácticas); y un segundo nivel en cuanto a la validación del cumplimiento en base a evidencias electrónicas (para demostrar hechos en entornos telemáticos) y auditorías (para validar que un determinado entorno cumple con una normativa específica).

Tabla 1. Roles y responsabilidades según el modelo SPI de implantación

Procesos	SaaS		PaaS		IaaS	
	Cliente	Proveedor	Cliente	Proveedor	Cliente	Proveedor
Desarrollo de aplicaciones	I	R	R	I	R	I
Gestión de la configuración	I	R	A	R	A/R	R
Gestión del cambio	I	R	A	R	A	R
Gestión del parcheado	I	R	A/R	R	A/R	R
Gestión de identidades	A	R	A/R	R	A/R	R
Gestión de acceso lógico	A	R	A/R	R	A/R	R
Cumplimiento legal y regulatorio	A/R	R	A/R	R	A/R	R
Gestión Ciclo de Vida de la Información	A/R	A	A/R	A	A/R	A
Gestión Continuidad de Negocio	A	R	A/R	R	A/R	R
Gestión Incidentes de seguridad	A	R	A/R	R	A/R	R
Gestión acceso físico	I	A	I	A	I	A
Activos de información						
Información	A	R	A	R	A	R
Aplicaciones	I	A/R	A/R		A/R	
Servidores (HW)	I	A/R	I*	A/R	I*	A/R
Almacenamiento	I	A/R	I*	A/R	I*	A/R
Sistemas Operativos	I	A/R	I*	A/R	A/R	
Red	I	A/R	I*	A/R	I*	A/R
Sistemas de seguridad	I	A/R	I*	A/R	A/R**	A/R**

R – Responsable / A – Aprobador / C – Consultado / I - Informado

En cuanto a la gestión de evidencias digitales, el informe constata la gran dificultad que a día de hoy existe para su correcta gestión; principalmente debido a la responsabilidad compartida, arquitecturas actuales, la distribución geográfica y la multiposesión. Se proponen una serie de recomendaciones desde la perspectiva de cliente a través de la implantación de un entorno confiable con el proveedor que permita procedimientos coordinados de gestión de evidencias, incluyendo medidas de protección de los registros de auditoría.

Privacidad y cumplimiento normativo en "la Nube"

La garantía de privacidad ha sido uno de los aspectos más trabajados en esta primera versión. En países como Estados Unidos, la protección de datos personales no está considerada como en Europa un Derecho Fundamental y tiene una regulación sectorial. La Directiva 95/46/CE constituye el marco europeo de referencia que los Estados miembros han tenido que trasponer en sus ordenamientos. En el año 2000, el Departamento de Comercio de los Estados Unidos acordó con la Unión Europea los "Safe Harbor Privacy Principles", principios de privacidad para las organizaciones estadounidenses, con el objeto de que las empresas que se adhieran a ellos puedan ser importadores de datos personales provenientes de la Unión Europea sin necesidad de autorización previa. Existen otros marcos, como el de la APEC (*Asia-Pacific Economic Cooperation*), que comparte los principios de protección de datos personales de la Directiva Europea, aunque no se garantiza la regulación desde el Estado. Especial mención tiene el esfuerzo conjunto de los garantes de la privacidad de diversos países, coordinados por la AEPD, que han publicado (con carácter no vinculante) la Resolución de Madrid sobre Estándares Internacionales sobre Protección de Datos Personales y Privacidad, plasmando múltiples enfoques e integrando diferentes legislaciones.

Por todo ello, una de las primeras conclusiones del informe es que, en la computación en

"la nube", la simple determinación de la legislación aplicable ya es un reto. El informe propone diferentes recomendaciones; como por ejemplo que las empresas proveedoras que utilicen medios situados dentro del territorio del EEE (Espacio Económico Europeo) para prestar servicios a sus clientes deberán ser conscientes de que exportan la legislación europea a todos aquellos que no estén establecidos en dicho espacio. El informe también especifica que una empresa cliente establecida en el territorio del EEE, independientemente de dónde esté ubicado su proveedor de servicios en "la nube", será la responsable en términos de protección de datos y le será de aplicación la ley del Estado en que esté establecida.

Otro aspecto a tener en cuenta en la computación en "la nube", es la delimitación de la figura del "Encargado de Tratamiento". Un proveedor de servicios en "la nube" podrá determinar hasta dónde llega su responsabilidad como encargado de tratamiento en función de la tipología de nube (pública, privada, comunitaria o híbrida) y del servicio que decida contratar el "Responsable de Tratamiento" de los datos de carácter personal; ya que en función del modelo de despliegue de los servicios en "la nube" (modelo SPI), las responsabilidades del proveedor serán diferentes. El proveedor siempre será responsable de proporcionar los controles de seguridad que exige la normativa, en base al servicio contratado, tal y como se detalla dentro del informe. Asímismo, el informe también detalla las responsabilidades del cliente.

Las transferencias internacionales de datos de carácter personal tienen una regulación específica que se ha de considerar para la computación en "la nube", dado el frecuente carácter transnacional de esta y sobre todo en el caso de países sin un nivel adecuado de protección de datos. En estos casos será necesario disponer de autorización de la Autoridad Competente y notificar la transferencia al Registro General de Protección de Datos. Los grupos multinacionales pueden optar por el modelo general basado en contratos caso por caso o adoptar y conseguir la aprobación por la autoridad competente de unas 'Binding Corporate Rules' en que consten las necesarias garantías.

La principal conclusión es que para garantizar la privacidad es necesario de forma urgente aumentar la transparencia entre clientes y proveedores. Sirva como ejemplo comentar que los clientes deben informar a los proveedores sobre los tratamientos de datos de carácter personal que están realizando, así como los proveedores deben informar a los clientes sobre localizaciones y subcontrataciones; junto con el establecimiento de mecanismos de coordinación para dar cumplimiento a los derechos de los afectados.

Aunque el foco de atención de esta primera versión del informe ha sido la garantía de privacidad, también propone diversas reflexiones y recomendaciones con respecto al Anteproyecto de Ley de modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones; Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos; Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico; Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y aspectos Jurídicos Laborales.

El informe propone una serie de recomendaciones para las auditorías en entornos de computación en "la nube" y en cuanto al marco auditor a aplicar, se recomienda seguir la evolución de CloudAudit, que permitirá mejorar el nivel de trasparencia actual, y seguir la labor de grupos como el "Security Metrics WG" de la Cloud Security Alliance, cuyos resultados serán complementarios al CloudAudit.

SGSI y gestión de riesgos en "la Nube"

El informe proporciona una serie de pautas para establecer, de forma práctica y eficaz, un adecuado Sistema de Gestión de Seguridad de la Información; especialmente en todos aquellos aspectos del establecimiento de un SGSI que sean característicos de la computación en "la nube". El informe considera que un SGSI es la manera adecuada de implantar el principio de mejora continua en la computación en "la nube". Esta incorpora diferencias en los niveles y mecanismos de gestión de riesgos con respecto a los servicios TIC tradicionales, lo cual no implica directamente tareas adicionales para el SGSI, pero sí que se debe afrontar de manera distinta, diferenciando el ámbito de actuación (usuario, cliente, proveedor), así como el tipo de servicio (SaaS, PaaS, IaaS).

Para hacer realmente factible la implantación de SGSIs en "la nube" es necesario implantar mecanismos de comunicación fluidos entre clientes y proveedores sobre valoraciones de riesgos e incidencias, variaciones de los niveles de riesgo, asignación clara de roles y responsabilidades, respuesta coordinada a incidentes, así como en tareas de seguimiento y auditorías. En la figura 2 se muestra una tabla en la que se puede visualizar un ejemplo que propone el informe, en formato de matriz RACI, de distribución de responsabilidades entre cliente y proveedor según el tipo de servicio (SaaS, PaaS, IaaS). El informe propone la inclusión en el contrato de servicio de una matriz de responsabilidades similar a la propuesta, que permitiría la implantación de "SGSIs encapsulados" en los casos en que el sistema de gestión de una de las partes esté incluido en el sistema de gestión de la otra a modo de "envoltorio".

Contratación, evidencias electrónicas y auditoría en "la Nube"

Dependiendo del cliente y de la información tratada en el ámbito de los servicios, existirán requerimientos legales y regulatorios que deben ser tenidos en cuenta a la hora de definir el marco contractual que rija la relación cuya parte fundamental estará representada por el Acuerdo de Nivel de Servicio (ANS). El ANS formaliza en el contrato las expectativas del cliente en cuanto a qué espera del servicio en "la nube" que ha contratado que, a su vez, debe coincidir con la capacidad real comprometida por el proveedor a tal efecto. Es por ello que, tanto el cliente como el proveedor del servicio en "la nube", deben tener muy claro que entienden del mismo modo los indicadores, métricas y penalizaciones/bonificaciones incorporadas al ANS.

El informe propone recomendaciones a incluir en el contrato en áreas especialmente sensibles, como son la determinación de la propiedad intelectual de los distintos elementos del servicio, el establecimiento de mecanismos de resolución de conflictos y "auditabilidad", o la especificación de las leyes y la jurisdicción aplicables.

En cuanto a la gestión de evidencias digitales, el informe constata la gran dificultad que a día de hoy existe para su correcta gestión; principalmente debido a la responsabilidad compartida, arquitecturas actuales, la distribución geográfica y la multiposesión. Se proponen una serie de recomendaciones desde la perspectiva de cliente a través de la implantación de un entorno confiable con el proveedor que permita procedimientos coordinados de gestión de evidencias, incluyendo medidas de protección de los registros de auditoría.

Finalmente, el informe propone una serie de recomendaciones para las auditorías en entornos de computación en "la nube". En cuanto al marco auditor a aplicar, se recomienda seguir la evolución de CloudAudit, que permitirá mejorar el nivel de trasparencia actual. También se recomienda seguir la labor de grupos como el "Security Metrics WG" de la Cloud Security Alliance, cuyos resultados serán complementarios al CloudAudit. (Para más información, el informe completo se puede descargar en http://www.ismsforum.es/csa). ■

LUIS BUEZO
Director EMEA IT Assurance
HP Technology Services
Presidente del Capítulo Español
CLOUD SECURITY ALLIANCE