ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

75/2012 2 octubre de 2012

*Luis de Salvador Carrasco**

CLOUD COMPUTING Y LA ESTRATEGIA ESPAÑOLA DE SEGURIDAD



# CLOUD COMPUTING Y LA ESTRATEGIA ESPAÑOLA DE SEGURIDAD

## Resumen:

Los servicios de Cloud Computing, aquellos en nubes públicas y de grandes proveedores, implican riesgos que han de ser analizados más allá del ámbito individualizado de una empresa, sino de una forma global a la luz de la Estrategia Española de Seguridad. El uso de Nubes de operadores que se encuentran fuera de nuestro país supone aumentar tanto nuestra dependencia tecnológica, como las amenazas a la confidencialidad y disponibilidad de la información. Aunque existe una tendencia a migrar servicios al Cloud con el propósito de un ahorro de recursos a corto plazo, hay que considerar las implicaciones negativas que tiene el que importantes sectores económicos, y en particular la Administración Pública, tengan sus servicios de comunicación y proceso de datos en manos de terceros sujetos a regulaciones, políticas y autoridades de otros países.

*Abstract:*

*Cloud Computing services, those implemented on Public Clouds from main providers, derive risks to be analyzed further the scope of a single company, but globally under the Spanish Security Strategy document. The use of Cloud providers located outside our country means to increase our technological dependency, and threats regarding with data confidentiality and availability. Although there is a trend to migrate services to the Cloud, mainly to save budget at short-term, we have to take into account the negative consequences for main economical sectors, and public bodies, to contact communication and data processing services with third parties under foreign regulations, policies and authorities.*

Palabras clave: Cloud computing, Estrategia Española de Seguridad, Ciberdefensa

*Keywords: Cloud computing, Spanish Security Strategy, Cyberdefense*

*__NOTA:__ Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

## INTRODUCCIÓN

El paradigma de la Computación en la Nube, el Cloud Computing, se está extendiendo con fuerza a todos los niveles en nuestra sociedad: de la empresa privada a la pública, del particular en su móvil a los procesos de negocios de la corporación. La Nube ha ido penetrando de la mano de las aplicaciones orientadas a particulares: correo personal[1], redes sociales, chats, almacenamiento, etc., que se han ido transformando en herramientas colaborativas para empresas e incluso soporte de sus procesos de negocio.

Utilizando una agresiva estrategia comercial y política[2], el Cloud se ha presentando como la única alternativa posible en la política TIC (Tecnología de la Información y las Comunicaciones) del próximo futuro, como un camino inevitable en la implementación de los sistemas de información. Abrazar una solución de Cloud se racionaliza en función del ahorro de costes a corto plazo y las facilidades que ofrece para el acceso a la información. Pero ha de ser la evaluación del riesgo a largo plazo, y no sólo el ahorro inmediato, lo que ha de servir de guía para la selección de una solución de Cloud. Es más, los servicios de Cloud están concentrados en unos pocos proveedores, pues la obtención de beneficio se basa en la aplicación de economías de escala, lo que supone concentrar el riesgo en entidades que no están físicamente en España, incluso no lo están fiscalmente.

La materialización de una amenaza sobre un servidor de Cloud se convertirá en una brecha que afectará a un conjunto significativo de empresas o entidades de forma simultánea. Estas amenazas podrán ser ataques sobre los servicios de Cloud, caídas de servicio por problemas técnicos en el Cloud o en la red, y accesos indebidos a la información por los proveedores o por las propias autoridades que controlan los servidores.

Por lo tanto, estudiar el riesgo que supone abrazar soluciones de Cloud limitándolo al efecto que tiene para un empresa individual no es razonable, sino que ha de realizarse desde un punto de vista global, estudiando el posible impacto que tiene sobre las infraestructuras y los intereses de nuestro país, basándose en los principios señalados en la Estrategia Española de Seguridad[3], y adoptando una posición crítica ante postulados que persiguen otros intereses[4].

---

[1] Léase: Gmail, Hotmail, Yahoo…

[2] Véase lo que se ha llamado el "Cloud First Policy" dibujada en la Federal Cloud Computing Strategy http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf.
Su autor Vivek Kundra, antiguo asesor de Obama como Federal Chief Information Officer, es una de las personas más influyentes en lo que a política de Cloud Computing se refiere. Sus esfuerzos están orientados al impulso de una migración global de los gobiernos, de los servicios estatales de cualquier país, a la Nube. Actualmente, asesora a la comisaria Neelie Kroes, vicepresidenta de la Comisión Europea responsable de la Agenda Digital Europea http://ec.europa.eu/information_society/activities/cloudcomputing/index_en.htm. Vivek Kundra (1974) es psicólogo, con un Master en IT, ambos por la universidad de Maryland (la 55ª en el ranking US) y desde los 27 años ostenta responsabilidades políticas.

[3] *Estrategia Española de Seguridad Una responsabilidad de todos*
http://www.lamoncloa.gob.es/NR/rdonlyres/D0D9A8EB-17D0-45A5-ADFF-46A8AF4C2931/0/EstrategiaEspanolaDeSeguridad.pdf

[4] Ver nota 2.

## LA SOLUCIÓN EN LA NUBE

Cuando se plantea la opción Cloud Computing se habla de las grandes ventajas que pueden traer, en particular en su empleo en las Administraciones Públicas, como podrían ser: ahorro de costes, modernización, movilidad, ubicuidad de los servicios, nuevas aplicaciones para los clientes/ciudadanos, más facilidad para el acceso a la información, etc.

Este discurso obvia que las anteriores ventajas no son exclusivas de los servicios implementados en Cloud. Además, no se tienen en cuenta que bajo el nombre genérico de Nube se engloban productos que son radicalmente diferentes a la hora de evaluar su impacto en seguridad, tanto en lo relativo a la continuidad de los procesos de empresa como la confidencialidad de su información[5] [6].

En un extremo están las Nubes Privadas, y de entre éstas las que se acceden a través de enlaces dedicados, y que son una evolución de los tradicionales centros de proceso de datos de una entidad. En el otro extremo están las que aquí nos ocupan, la Nubes Públicas de empresas localizadas total o parcialmente fuera de España, que son grandes proveedores de servicios con una posición dominante en el mercado, y que basan su estrategia de negocio en las economías de escala y en la subcontratación dinámica con centros distribuidos a lo largo del globo[7].

Los aspectos que resultan preocupantes en estos tipos de Nubes no son sólo la amenaza a la confidencialidad de la información, sino la disponibilidad del servicio que ofrecen y la portabilidad de los datos y procesos, es decir, la capacidad de migrar entre proveedores. Asimismo, en relación a la confidencialidad de los datos, es necesario tener en cuenta tanto el contenido de la comunicación, como la metainformación asociada al contenido, en su mayor parte información de tráfico: localización geográfica de los comunicantes, identidad de los mismos, interlocutores destacados, red de relaciones, información sobre los dispositivos conectados, el volumen de información transmitida por un actor y el volumen de tráfico de la entidad tanto estadísticamente como puntualmente, etc. Esta metainformación es aún más interesante cuando se toma en consideración la Nube móvil[8].

---

[5] *Riesgos y amenazas en Cloud Computing* INTECO http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

[6] *Cloud Computing. Retos y Oportunidades*, ONTSI, Observatorio Nacional de las Telecomunicaciones y del SI, en colaboración con Deloitte, Mayo 2012.

[7] No todas las Nubes públicas cumplen lo anteriormente señalado, p.e., la solución de Arsys http://www.arsys.es/cloud-hosting/cloudbuilder-comparativa.html, o cumplen de forma parcial, p.e., http://www.interxion.com/locations/

[8] Un ejemplo de ello ocurre con las redes sociales: *We Know Your House' Shows How Many People Reveal Their Home Address On Twitter.* Agosto de 2012 http://newrisingmedia.com/all/2012/8/14/we-know-your-house-shows-how-many-people-reveal-their-home-a.html

## RIESGOS GENERADOS POR LA NUBE[9] [10]

Una de las palabras más repetidas cuando un proveedor presenta una solución de Cloud es la palabra "seguridad" y cuando se plantea la posibilidad de que se produzca una brecha en dicho sistema la respuesta es "imposible". La experiencia nos demuestra que siempre hay una amenaza que hasta entonces nadie había planteado, y que se hace real[11]. Ya ha habido casos en los que la seguridad de la Nube se ha comprometido, y se ha comprometido gravemente[12].

La implementación de los procesos de empresas y entidades sobre soluciones de Cloud trasciende a lo que es un problema interno a las mismas, o a una discusión en la que sólo se han equilibrar cuestiones técnicas, logísticas y contables. Al contrario, su extensión y sus implicaciones obligan a que se estudien desde una perspectiva global, desde el punto de vista de los intereses de nuestro país, y por lo tanto desde la óptica de la Estrategia Española de Seguridad, ya que las cuestiones de ciberdefensa ocupan un apartado importante de la EES en relación a "su protección y capacidad de resistencia y recuperación, y más preocupante su vulnerabilidad".

### DEPENDENCIA TECNOLÓGICA

La EES muestra su preocupación por la dependencia externa en sectores estratégicos, y en particular por la dependencia tecnológica, de forma que una de sus líneas de actuación es el "Apoyar el desarrollo de empresas privadas nacionales en un sector estratégico como éste, en el que puede ser peligrosa la dependencia de empresas extranjeras" y en particular "reduciendo la dependencia de la tecnología de seguridad de terceros países".

Las soluciones de Cloud (recordad que al principio del texto nos centramos en las Públicas de grandes proveedores), suponen descansar en servicios externos, física y fiscalmente fuera de España, gran parte de nuestros datos y procesos. El empleo masivo de soluciones Cloud supone dar un paso más en nuestra dependencia de las redes de comunicaciones, pues añade una adicional: la que supone el propio proveedor de los servicios de Cloud.

El que gran parte de los recursos para el proceso de la información, y los datos en sí mismos, puedan estar fuera de nuestras fronteras va en contra de la afirmación de la EES que "Debemos asegurar la capacidad de respuesta. España debe disponer de la capacidad de reaccionar" en el marco de un entorno de crisis. La migración masiva a las soluciones Cloud

---

[9] *Cloud Computing Security Risk Assessment*, ENISA 2009 http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

[10] *Top Threats to Cloud Computing v.10* CSA 2010 https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[11] El caso de robo de material criptográfico de la empresa RSA comprometió la seguridad, entre otros, de los servicios de Google: McMillan R. *RSA warns SecurID customers about hack*. IDG News Service 18 de marzo de 2011 http://www.computerworlduk.com/news/security/3265825/rsa-warns-securid-customers-about-hack/

[12] Mah P. *Dropbox's multiple security problems*, 19 de agosto de 2011 By http://www.fiercecio.com/techwatch/story/dropboxs-multiple-security-problems/2011-08-19. Otro caso: *Epsilon Breach Deals Another Blow to Cloud Security*, 8 de abril de 2011 http://www.infosecisland.com/blogview/12814-Epsilon-Breach-Deals-Another-Blow-to-Cloud-Security.html

supone desmantelar una infraestructura material y sobre todo humana: personal con el know-how de la entidad y los procesos técnicos. Esta infraestructura en caso de necesidad, será muy difícil de recuperar[13].

#### DISPONIBILIDAD DE DATOS Y SERVICIO

La libre disponibilidad de datos y servicios es uno de los problemas que presenta el actual paradigma Cloud y que mayor dependencia genera al usuario respecto al proveedor. Ninguno de los dos contempla la posibilidad de trasladar, desde la Nube originalmente contratada a otra Nube distinta, tanto los datos como los procesos. Y todo ello con un coste razonable en tiempo y recursos. A esto se le denomina portabilidad y, actualmente, resulta problemática debido a que los formatos de los datos y las aplicaciones son propietarios de cada Cloud.

Sin que se hayan previsto mecanismos para la portabilidad de la información y procesos entre plataformas, el cliente se encuentra cautivo ante situaciones como un aumento unilateral del coste de los servicios, una modificación/suspensión de las condiciones de prestación de los mismos, un cambio de estrategia empresarial, por absorciones, por el cierre de la compañía o por situaciones de crisis.

La gestión de las contingencias relativas a la caída permanente o puntual de los servicios TIC se ha desplazado de los responsables de la empresa al proveedor de Cloud. Y aunque estos últimos dan la impresión de que sus plataformas ofrecen una cantidad ilimitada de recursos, a través de la subcontratación dinámica, esto no totalmente correcto. Igual que las redes de comunicaciones, o de energía, están dimensionados para ofrecer servicio al máximo número de usuarios con los mínimos recursos, en base a una estimación estadística de carga. En un momento dado, el tener que soportar sobre una misma red una enorme cantidad de solicitudes, hace a los enlaces de datos susceptibles de sobrecarga, independientemente de que existan clausulas de acuerdo de niveles de servicio (SLA) en los contratos[14].

Estudios británicos estiman que la pérdida debido a la caída de servicios de Cloud ha tenido un impacto de 45 millones de libras desde 2007, incluso los expertos consideran que esta cifra está calculada a la baja[15]. Algunos clientes han equilibrado el uso de nubes públicas con privadas, para limitar el riesgo, aunque esto sólo está al alcance de grandes entidades.

---

[13] Este análisis se realizó en el caso de la migración de los servicios de la ciudad de Los Ángeles al servicio de cloud, concluyéndose que: "si la Ciudad decide utilizar estos servicios …. será prohibitivo en coste volver a la actual estructura gestionada por la propia Ciudad". Jansen W. *Guidelines on security and privacy in public cloud computing.* NIST National Institute of Standards and Technology, diciembre 2011.

[14] Una referencia a las recientes caídas de servicio de Google, Twitter, Blackberry…. *Cuando los gigantes se colapsan: problemas en Twitter y Gmail* 31 de julio de 2012 9: http://www.solomarketing.es/cuando-los-gigantes-se-colapsan-problemas-en-twitter-y-gmail

[15] Essers L. *Cloud downtime has cost more than £45 million since 2007* IDG News Service, 12 de junio de 2012 http://www.computerworlduk.com/news/cloud-computing/3364982/cloud-downtime-has-cost-more-than-45-million-since-2007/?intcmp=in_article;related.

### SERVICIO CRÍTICO

La EES contempla "las amenazas y riesgos a la seguridad económica" y su propósito también es "garantizar la capacidad de los servicios críticos económicos y financieros… esenciales para el normal funcionamiento del país" incluyendo los servicios que proporcionan cohesión al territorio nacional como son transportes[16], comunicaciones, energía etc. Es decir, proteger las infraestructuras críticas de "Fenómenos naturales extremos, atentados terroristas o ciberataques, entre otros de las amenazas y riesgos analizados, pueden dañar las infraestructuras críticas, suministros y servicios críticos que sustentan nuestra vida y el desenvolvimiento de nuestra sociedad. Debemos proteger y garantizar su normal funcionamiento…".

Por su propia naturaleza, el hacer uso masivo de los servicios de Cloud proporcionados por unos pocos proveedores supone la concentración en unos pocos puntos singulares de gran parte de los procesos que realizan entidades (públicas y privadas) en España. Esto aumenta la probabilidad de que se materialice la amenaza dibujada en la EES de que "un grupo terrorista o un país enemigo colapsara el tráfico en el ciberespacio", que un tercer país pueda paralizar la actividad de todo un sector, sino de una parte significativa de todos los sectores económicos[17].

### ATAQUES EXTERNOS

La caída de los servicios de Cloud puede estar originada por fallos internos del proveedor o por fallos de la red, aunque el hecho de la existencia de Nubes facilita la acción de los hackers ya que no tienen que atender a infinidad de objetivos, sino que pueden alcanzar gran efectividad focalizando sus actuaciones sobre un puñado de proveedores.

En principio, por qué ha caído el servicio tiene una importancia secundaria, a menos que esté sincronizada con otro tipo de evento, circunstancia que sí ha alarmado a los propios servidores de Cloud, que han reconocido que son objetivos de ataques respaldados por estados[18].

La mayor amenaza externa a la que se enfrentan los proveedores de la Nube es un ataque distribuido de denegación de servicio a nivel de aplicación, que esté orientado a acabar con la disponibilidad de la infraestructura del proveedor de la nube para todos sus clientes, que

---

[16] Microsoft presenta varios casos de éxito de implantación en Cloud de la venta de billetes de Transmediterránea, los sistemas de Ferrovial o la gestión de paquetes con MRW http://www.microsoft.com/spain/enterprise/soluciones-microsoft/soluciones-de.aspx?tema=cloud-computing.

[17] Las operadoras planean demandar a Blackberry por la caída del servicio. Los servicios de mensajería y acceso a internet de Blackberry volvieron a sufrir cortes ayer. Millones de clientes se vieron afectados en Europa, África, Asia y Latinoamérica. RIM no dio ningún tipo de explicación sobre los motivos. Las quejas de los usuarios cayeron sobre los operadores, que niegan que la culpa sea suya, y amenazan con posibles demandas por daños y perjuicios contra RIM. Santiago Millán y Mar Jiménez, Madrid 12/10/2011 - http://www.cincodias.com/articulo/empresas/operadoras-planean-demandar-blackberry-caida-servicio/20111012cdscdiemp_3/.

[18] Security warnings for suspected state-sponsored attacks, Tuesday, June 5, 2012 12:04 PM Posted by Eric Grosse, VP Security Engineering.

es difícil de combatir con las medidas de seguridad existentes y que se pueden materializar empleando herramientas muy sencillas.

### ACCESO A LA NUBE

Uno de los principios de seguridad es que la accesibilidad física a la información ha de estar restringida a lo estrictamente necesario. Esto quiere decir que, si un dato no es necesario que esté accesible a través de la red[19], no se ha de almacenar en un sistema conectado (ya sea a intranet o Internet). Y si hay que transmitirlo entre dos puntos, que el canal sea lo menos accesible posible[20].

El concepto del Cloud supone exactamente lo contrario. La propia naturaleza del servicio ha de proporcionar acceso a terceros a los recursos de la Nube, la implementación de una arquitectura multi-tenancy implica que otros ejecutan procesos sobre los mismos sistemas (HW/SW), y el tráfico de datos se realiza a través de redes públicas. Esto permite múltiples tipos de ataques como los secuestros de sesiones, o la suplantación de portales[21].

Además, muchos proveedores de Cloud proporcionan parte de sus servicios de forma gratuita, sin necesidad de más identificación que una dirección de correo electrónico. Esto facilita enormemente el explotar vulnerabilidades del servicio en la Nube por usuarios completamente anónimos. Entre las posibles amenazas, está la de utilizar el Cloud para implementar botnets[22] que afecten tanto a usuarios de la Nube, como a otros externos[23].

De esta forma, tanto la información como la metainformación están altamente expuestas a ataques a la confidencialidad y a la disponibilidad, y por parte de atacantes asimétricos como por actores estatales.

### LA NUBES PERSONALES

El uso del Cloud a veces escapa del control de los responsables TIC, ya que es común que los empleados y directivos de entidades utilicen servicios no corporativos en Nube para resolver sus necesidades de comunicación, principalmente servicios de Nube móvil. Entre dichas aplicaciones están los servicios de mensajería (y algo más) desde WhatsApp a

[19] Es más, cuando un dato no es necesario mejor bloquearlo, es decir, sacarlo de cualquier sistema lo que no implica que se irrecuperable.
[20] Un enlace WIFI o inalámbrico siempre es lo más expuesto, mientras que en el otro extremo de la seguridad tendríamos una línea de fibra dedicada y enterrada.
[21] *Detectado kit para suplantar la página de inicio de Tuenti. Afecta a usuarios que accedan a la página web falsa que suplanta a Tuenti e introduzcan su nombre de usuario y contraseña.* http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/detectado_kit_suplantar_pagina_inicio_tuenti_20120813.
[22] Constantin L. *Cybercriminals Use Zeus Malware to Target Cloud Payroll Services.* IDG News 2012, http://www.pcworld.com/businesscenter/article/253505/cybercriminals_use_zeus_malware_to_target_cloud_payroll_services.html.
[23] Comazzetto A. *Botnets–The Dark Side of Cloud Computing* Sophos 2012, http://www.infosecurity-magazine.com/view/24987/comment-botnets-the-dark-side-of-cloud-computing/.

GoogleDocs[24] o DropBox. Estos usuarios finales no son totalmente conscientes que están utilizando aplicaciones en Cloud, ni de la cantidad de información sensible de su entidad que están procesando en la Nube fuera de las políticas de la empresa.

Las Nubes personales son un agujero de seguridad que permite acceder a los sistemas de la empresa cuando, desde el dispositivo corporativo, el usuario accede a las dos Nubes de forma simultánea, la profesional y la personal.

#### FALTA DE VISIBILIDAD

No siempre es el usuario final el que toma la iniciativa de usar dichos servicios de mensajería, sino que es la política de IT (Tecnologías de la Información) de la empresa la que los facilita.

A la hora de fijar la política y levantar la infraestructura TIC de una empresa, es necesario realizar un análisis de riesgos, de las posibilidades de fallo y las medidas de seguridad a aplicar de forma integral, es decir, desde el sistema de cableado hasta las aplicaciones corporativas.

Al elegir una solución de Cloud la transparencia que se obtiene del anterior análisis se pierde, al no tener los responsables TIC visibilidad sobre los procesos en la Nube. Se podría decir que, en estos casos, las entidades utilizan la táctica del avestruz, ya que al no conocer los riesgos que se están asumiendo, simplemente se están aceptando situaciones que no se considerarían razonables para la propia infraestructura.

Como se ha visto anteriormente, muchos servicios de Cloud se construyen sobre una cadena dinámica de subcontrataciones, en las que es crítico conocer las condiciones de seguridad de cada contratista y, sobre todo, su localización física. Por lo tanto, el servicio de Cloud ha de poder ser auditable o transparente (en el sentido de la palabra inglesa "accountable") y proporcionar información precisa de dónde, cuándo, cómo y quién ha almacenado o procesado sus datos.

En otro caso, nos encontraremos con un servicio opaco al usuario, en el que éste no tiene opción alguna de obtener información precisa de qué ha ocurrido con sus datos, ni herramientas para auditar el servicio que se le está proporcionando, y en el que su propia información escapa a su control.

#### SOMETIMIENTO A LAS REGULACIONES LOCALES

La localización de los proveedores o subcontratistas de la Nube es una cuestión de capital importancia. Aunque se diga que Internet no tiene fronteras, esas fronteras sí que existen a la hora de aplicar las regulaciones locales, y por más que se emplee el concepto de Nube en

[24] Bradley T. *More than E-mail at Stake in Google Gmail Attack*. PCWorld 3 de junio de 2011 http://www.pcworld.com/businesscenter/article/229320/more_than_email_at_stake_in_google_gmail_attack.html

relación a distribución de los datos, el único que está en la "nube" es el usuario final, los datos están físicamente en un sitio muy concreto en cada momento.

Como señala la EES, "no son sólo los factores tecnológicos los que incrementan las posibilidades de que las ciberamenazas se materialicen, sino también los legales". Las regulaciones locales afectan a la prestación servicio de dos formas. Por un lado, obligan a unas garantías mínimas de seguridad y de confidencialidad a las compañías subcontratistas en la Nube (independientemente de las fijadas por contrato). Por otro lado, habilitan el acceso a la información a las autoridades locales, con mayor, menor o ningún control judicial, e imponen unas obligaciones de conservación de datos[25], es decir, de retener la información del usuario incluso cuando el usuario cree que ha sido eliminada.

No todos los países ofrecen las misma garantías por ley, algunos muy pocas, y otros, aunque de forma nominal ofrecen unas garantías jurídicas y técnicas elevadas, también disponen de los recursos legales necesarios para saltarse las políticas de seguridad de cualquier proveedor de Cloud[26].

De todos es conocido que la Patriot Act permite a las autoridades norteamericanas la interceptación y la inspección de cualquier información almacenada o procesada en Estados Unidos, o por empresas estadounidenses aunque sus instalaciones estén en cualquier otra parte del mundo. Por ejemplo, Microsoft admitió que ofrecía a las Autoridades Federales la información almacenada incluso en sus servidores situados en la Unión Europea, sin necesidad de solicitar el consentimiento ni notificarlo a los legítimos dueños de los ficheros, o a las personas afectadas por los datos almacenados. Este tipo de declaraciones tuvieron como consecuencia que la empresa de defensa británica, BAE Systems, decidiera abandonar sus planes de implementación[27] sobre Microsoft 365 por no tener una garantía de confidencialidad[28].

La intervención de una autoridad puede ir más allá de un ataque a la confidencialidad, puede implicar directamente un ataque a la disponibilidad de los datos, como fue el caso de la intervención de Megaupload. Para lo que nos ocupa, no era importante si la actuación del FBI perseguía un fin lícito o no, lo importante es que causó un perjuicio directo a un conjunto de usuarios españoles a los que se dejó sin servicio y sin capacidad alguna de reacción[29].

---

[25] Vijayan J. *DOJ seeks mandatory data retention requirement for ISPs* 25 de enero de 2011 http://www.computerworld.com/s/article/9206379/DOJ_seeks_mandatory_data_retention_requirement_for_ISPs

[26] Messmer E. *Security experts say US government may have back door into RSA SecurID*. Network World US. 23 de marzo de 2011. http://www.computerworlduk.com/news/security/3266653/security-experts-say-us-government-may-have-back-door-into-rsa-securid/?intcmp=rel_articles;scrty;link_2

[27] Mandalia R. *BAE Systems Abandons Microsoft Cloud Plans Citing Patriot Act.* 8 diciembre de 2011 http://www.itproportal.com/2011/12/08/bae-systems-abandons-microsoft-cloud-plans-citing-patriot-act/

[28] Hay que tener en cuenta, que aunque no se utilicen los servicios de Cloud para manejar información clasificada, sólo con conocer correos, viajes y reuniones ya es suficiente para hacerse una idea de qué es lo que está pasando.

[29] Sanz J. *EEUU ignora al Gobierno de España en relación a la posible recuperación de ficheros de Megaupload*, 19 de marzo 2012, http://www.adslzone.net/article8200-eeuu-ignora-al-gobierno-de-espana-en-relacion-a-la-posible-recuperacion-de-ficheros-de-megaupload.html

### RESPONSABILIDAD

Debido a lo ocurrido con Megaupload, desde el sector de la PYME se ha aconsejado leer cuidadosamente los términos de servicio de proveedores de Cloud como DropBox o Box.com[30]. La EES destaca el papel del sector privado en la seguridad, ya que muchas empresas son propietarias o gestoras de servicios e infraestructuras críticas y, por lo tanto, tienen la responsabilidad de proteger aquellas áreas que son de su competencia.

No pueden existir garantías en la prestación de un servicio de Nube sin que la relación entre cliente y proveedor quede reflejada en un contrato. Este ha de incorporar en sus clausulas los términos en los se fijan las responsabilidades, tanto a la hora de prestar el servicio, como a la hora de hacer frente a las consecuencias de la ejecución (o la mala ejecución) de los mismos[31] y, sobre todo, que quede claramente fijada que la propiedad de los datos continúa en manos del contratante en cualquier caso.

En la mayoría de los casos lo que se oferta son unas clausulas contractuales cerradas, (SLA o Service Level Agreement), en las que el proveedor de Cloud fija las condiciones con un contrato tipo igual para todos sus clientes, sin que el usuario tenga ninguna opción para negociar sus términos y, en general, obviando/rechazando cualquier responsabilidad o sujeción a las regulaciones nacionales. Este último caso es el más común, sobre todo cuando se encuentra el cliente en una situación de desequilibrio ante un gran proveedor.

### PROTECCIÓN DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

El poder de las autoridades para la intervención de sistemas de información y la falta de unas garantías contractuales efectivas, como se ha señalado en los dos anteriores apartados, incrementan los riesgos de sufrir ataques sistemáticos a la confidencialidad de los datos almacenados en los servicios de Cloud.

Hay que tener en cuenta que técnicas como cifrado, empaquetado, etc., ponen dificultades al acceso al contenido de la comunicación si están correctamente implementadas, aunque no lo hacen imposible[32]. Y, en cualquier caso, esto no impide el acceso a la metainformación de tráfico. Detrás de todo ello, se encuentra la amenaza del espionaje, especialmente económico, otra de las preocupaciones señaladas en la EES en cuanto a "su impacto potencial es cada vez mayor por su capacidad de dañar el sistema económico y afectar al bienestar de los ciudadanos".

La confidencialidad de los datos ha sido considerada siempre un aspecto clave en la seguridad de la información y cuya garantía se ve más amenazada a mayor posibilidad de acceso a las bases de datos. Si el acceso a información sensible a través de la red interna de

[30] de Juana R. *Qué implica el cierre de Megaupload para las pymes*. 7 de febrero de 2012 http://www.muypymes.com/2012/02/07/que-implica-el-cierre-de-megaupload-para-las-pymes

[31] Como lo expresa el término inglés "liability"

[32] *El robo de credenciales de acceso online, un problema cada vez mayor.* Europa Press, 21 de julio de 2012 http://www.europapress.es/portaltic/internet/noticia-robo-credenciales-acceso-online-problema-cada-vez-mayor-20120721100008.html

la entidad es un riesgo, mucho mayor cuando ese acceso se puede realizar desde redes externas, cuál será el nivel de riesgo que se está asumiendo cuando los datos ni siquiera están en la propia entidad, sino al contrario, es la entidad la que tiene que acceder a ellos.

Aunque existen iniciativas para la autorregulación en el tema de seguridad en Cloud, como la CSA[33] , así como de las certificaciones de seguridad, tipo ISO 27001[34] que obtienen los proveedores, esto no compensa la falta de transparencia y "accountability" de los mismos y obliga a confiar en la honestidad de dichos proveedores[35]. Desde cualquier punto de vista, este nivel de riesgo resulta inaceptable. Pongamos el caso de la e-Sanidad sobre la Nube, uno de los escenarios para los que se recomienda el uso de Cloud, y el riesgo que puede suponer el compromiso de los historiales clínicos como elemento de presión político o económico[36].

La confidencialidad del contenido está a la merced, en gran medida, de los proveedores del servicio, y su vulneración puede ser debida a la falta de honestidad de los gestores de servicio[37], sus obligaciones ante autoridades locales, ataques de intrusos o simplemente errores. Más aun, las garantías que ofrece el proveedor están sujetas a cambios, muchas veces unilaterales, de las condiciones del servicio. Un caso notorio es el caso de Skype, que presumía de emplear un cifrado "imposible de romper", y tras la adquisición por Microsoft, ha sufrido "mejoras técnicas" que permiten que tanto las conversaciones como el servicio de chat sean monitorizados a voluntad de la compañía[38].

Relacionado también con la responsabilidad, es necesario tener garantías sobre los periodos de conservación de datos en el proveedor de Cloud una vez que la relación se ha extinguido. Más complejo es obtener garantías sobre la limpieza de los sistemas del proveedor, o lo que es lo mismo, la garantía de que cuando se borra una información en la Nube, esta no queda de forma residual en los soportes del proveedor y accesible a los ataques de un tercero (habitual en el caso de ficheros temporales de información descifrada)[39].

## CONCLUSIONES

La utilización masiva de servicios de Cloud basados en nubes públicas de grandes proveedores y alojados en terceros países, genera problemas de dependencia y riesgos que van en contra de la filosofía de la Estrategia Española de Seguridad.

---

[33] *Cloud Security Alliance* CSA https://cloudsecurityalliance.org

[34] Nguyen A. *Google Apps receives ISO 27001 security certification* Computerworld UK 28 Mayo 2012 http://www.computerworlduk.com/news/security/3360345/under-embargo-google-apps-receives-iso-27001-security-certification/

[35] *Acusan a Facebook de mentir sobre la verificación (de seguridad) de aplicaciones. La red social recibió miles de dólares para supervisarlas y no lo hizo, según la Comisión Federal del Comercio de EE.UU*. ABC http://www.abc.es/20120814/medios-redes/abci-facebook-seguridad-aplicaciones-201208140849.html

[36] *El robo de la identidad digital de un periodista expone los riesgos de la nube* ABC 9 de agosto de 2012 http://www.abc.es/20120807/tecnologia/abci-roban-identidad-digital-periodista-201208071413.html

[37] *El "hacker" de la red de venta de datos se adjudica el Centro de Ciberseguridad*. El País, 30 de julio de 2012.

[38] *Polémicos cambios en la privacidad de Skype*, ABC tecnología, 23 de julio de 2012

[39] Kissel R. et al. *Guidelines for Media Sanitization, Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-88 September 2006

La amenaza que supone la utilización sin control de dichos servicios puede proceder tanto de grupos más o menos incontrolados, como de acciones realizadas por agentes estatales de los países en los que se alojen los servicios con el propósito de obtención de información o bloqueo de la misma como elemento de fuerza en situaciones de crisis.

No se fundamenta justificar la decisión de la migración a la Nube, incluso la migración de "sólo" los servicios de correo, basándose en el ahorro de costes a corto plazo o como una solución fácil en época de crisis. Lo que procede es racionalizar mejor los servicios disponibles. De lo contrario, se estará desmantelando una infraestructura técnica, y sobre todo humana, que en caso de necesidad, será muy difícil de recuperar.

Esto no supone renunciar a la utilización de la tecnología Cloud, pero siempre con ciertas limitaciones, entre ellas la utilización de Nubes Privadas[40] para la Administración Pública[41], desalentar el uso de oligopolios de Cloud que no se someten a la regulación nacional y la potenciación de proveedores de Cloud públicos que estén localizados físicamente en España. Esta última iniciativa se enmarca dentro de las líneas estratégicas de acción que el EES señala como prioritarias, dentro del aspecto de la ciberdefensa, como es el "apoyar el desarrollo de empresas privadas nacionales en un sector estratégico como éste, en el que puede ser peligrosa la dependencia de empresas extranjeras".

Tanto en entidades públicas como privadas es importante regular la utilización de "nubes personales" en paralelo con los servicios de comunicación y proceso corporativos. Ya existe un movimiento en determinadas compañías para bloquear el uso indiscriminado por parte de los empleados de estos servicios[42], y es necesario aplicar dicha política para evitar filtraciones de información.

La contratación de servicios de Cloud no puede suponer una delegación de las obligaciones de gobernanza de los sistemas de información. Cada entidad ha de realizar un análisis crítico de su modelo de seguridad en relación a cómo se adapta el Cloud al mismo, qué información no puede estar en el Cloud (si es que puede estar alguna), estimar los riesgos a largo plazo en relación a la confidencialidad, disponibilidad y portabilidad de la información y disponer de planes de contingencia para prever el fallo, puntual o permanente, del proveedor.

Como señala la EES, "hay que concienciar a las Administraciones Públicas, empresas y ciudadanos sobre los riesgos, mejorar la cooperación nacional e internacional y elaborar mapas de riesgos y catálogos de expertos, recursos y buenas prácticas", en particular, "… desarrollar el Esquema Nacional de Seguridad reforzar su aplicación y realizar auditorías que verifiquen la seguridad de los sistemas de la Administración…". Actualmente está en elaboración la Agenda Digital Española y la nueva Estrategia de Ciberseguridad por lo que

[40] Recordad que una Nube Privada no significa que el proveedor sea una empresa privada, sino que el proveedor es la misma entidad, o una subcontrata particular para implementar de forma exclusiva sus servicios.
[41] Siempre hay excepciones en función del tipo de datos, como es la implementación de la gestión de la Unidad de Arbolado Urbano del Ayuntamiento de Madrid que se ha implementado sobre Windows Azure
[42] Savvas A. *Most firms block BYOS in the cloud*, Computerworld UK, 17 de julio de 2012 http://www.computerworlduk.com/news/cloud-computing/3370488/most-firms-block-byos-in-cloud/

sería de gran interés que aparecieran indicaciones concretas, en particular para el caso de las Cloud "personales" tanto en ellas como en el Esquema Nacional de Seguridad[43].

Finalmente, es importante analizar el fenómeno Cloud Computing con la perspectiva del impacto que han tenido en crisis anteriores una excesiva dependencia (energética o económica), los problemas originados por el abuso y la dependencia de las redes sociales, el acceso a datos por parte de autoridades de otros países o las recientes caídas de servicios desde Blackberry a Google.

i

*Luis de Salvador Carrasco**
*Profesor Informática en la UEM*



[43] Como la realizada por el gobierno USA en el documento Federal Cloud Computing Strategy, ya referenciado, aunque sus conclusiones son opuestas a las aquí presentadas por razones obvias.