Vida&artes

# La nube digital también amenaza tormenta

## Grandes fugas de datos como la sufrida por Sony alertan sobre la seguridad de los contenidos alojados en la Red - Los expertos avisan de los riesgos y apelan a la responsabilidad del usuario

**ABEL GRAU** 02/08/2011

El gran gurú del futuro digital ha oteado el horizonte y vaticina nubes. El consejero delegado de Apple, Steve Jobs, pronostica que el centro de gravedad de la vida digital ya no será más el PC y su disco duro, sino la nube (es decir, los servidores de empresas como Google, Microsoft, Amazon o la misma Apple). El usuario se independizará de su terminal y accederá a todos sus documentos, programas, música, correo, películas y fotos indistintamente desde el móvil, la tableta, el portátil o el ordenador fijo. Su nuevo PC será la Red entera. Pero en la nube brillante que anuncia Jobs, otros ven indicios de tormenta.

Los expertos avisan con frecuencia de los riesgos que conlleva almacenar datos fuera del control del usuario (más allá de su PC), pero el pasado abril los temores se confirmaron. Un intruso accedió a los datos personales de 77 millones de miembros de la plataforma en línea PlayStation Network de Sony. A través de las videoconsolas PlayStation 3 y PSP, los clientes facilitan sus datos personales y bancarios a la compañía para poder jugar en red, navegar y descargar contenidos. El pirata obtuvo detalles de los clientes como nombre, dirección, país, correo electrónico, fecha de nacimiento y nombre de acceso, entre otras. Incluso los números de las tarjetas de crédito habrían quedado expuestos (aunque sin la cifra de control).

Es el mayor robo de datos detectado, según el Instituto SANS, que examina la seguridad informática. En España, con tres millones de usuarios registrados en la red de PlayStation, unas 330.000 tarjetas de crédito habrían quedado expuestas. La Agencia Española de Protección de Datos ha abierto de oficio una investigación. Hasta ahora no se ha denunciado ningún uso fraudulento, según indican desde Sony, pero la vulnerabilidad de todo el sistema ha quedado demostrada una vez más. Su caso se suma a muchos otros recientes: la empresa de *marketing* Epsilon (millones de direcciones electrónicas); AT&T (los correos de unos 100.000 iPad)...

Son riesgos considerables, dado que la nube está cada vez más integrada en nuestra vida cotidiana. La empleamos constantemente. Al buscar en Google, cuando revisamos el correo electrónico, al escuchar música sin descargarla, al ver vídeos en YouTube o al entrar en las redes sociales. Nada de todo eso está en nuestros terminales, sino en un lugar indeterminado, de ahí que se le denomine "la nube". En realidad, están almacenados en un conjunto de servidores situados en un lugar que el cliente ignora. Las ventajas son numerosas, pero los riesgos también.

Puesto que el volumen de datos personales que volcamos en ese entorno etéreo es enorme, el peligro también lo es. "La nube constituye un gran repositorio de información, con datos de empresas, cuentas bancarias y todo tipo de datos delicados; el riesgo es muy grande", sostiene Fausto Montoya, experto en criptografía e investigador de Física aplicada del Consejo Superior de Investigaciones Científicas (CSIC). Montoya emplea el servicio en nube Dropbox -una especie de escritorio y almacén virtual- que permite trabajar desde casa o simultáneamente con otros colegas.

Los expertos coinciden en identificar cuatro grandes riesgos. Uno: la pérdida de datos, ya sean robados por piratas informáticos o a través de agujeros de seguridad. Dos: el abuso o negligencia en la gestión de los datos acumulados por las empresas que suministran servicios en la nube. Tres: las responsabilidades jurídicas de las empresas. Cuatro: la dependencia de la conectividad; sin acceso a la Red, la nube no sirve de mucho.

El experto estadounidense Nicholas Carr -que vaticinó en 2008 el advenimiento de la nube digital en el ensayo *El gran interruptor* (Deusto)- enumera que los peligros más destacados son: "La pérdida de datos, agujeros de seguridad, violaciones de la privacidad y caídas del proveedor de servicios". Casos como el de Sony prueban que no son exageraciones. Pero considera que estos riesgos no son específicos de la nube: "Algunos están presentes también cuando te conectas a internet (incluso si almacenas tus datos en el disco duro)", señala por correo electrónico.

Los expertos aconsejan fijarse en el prestigio y el historial del proveedor. "Confías y te dices que nadie va a poder *hackear* Google o Amazon", sostiene Álvaro Ibáñez, del blog tecnológico Microsiervos. "No es lo mismo un ataque a Sony que a una compañía que se dedica específicamente a la computación en nube; se supone que sus controles de seguridad son mayores". Cuestión de confianza, pues. "La información está deslocalizada y es complicado fiarte, tienes que hacer un acto de fe y confiar en que las empresas aseguren los datos", señala desde Barcelona Jordi Torres, catedrático del departamento de arquitectura de computadores de la Universitat Politècnica de Catalunya. Pero matiza: "El riesgo es mayor si te roban el portátil. Ningún sistema es seguro al 100%".

El consejo más frecuente es usar el sentido común. "La única seguridad es la de tomar las decisiones con responsabilidad, haciendo el esfuerzo de informarse lo mejor que se pueda", recomienda Torres, autor del manual *Empresas en la nube* (Libros de cabecera), donde aborda las posibilidades que ofrece la nube para la gestión de las empresas (como el ahorro en infraestructura). Por ejemplo, Google, Amazon o Salesforce suministran este tipo de servicios.

El segundo riesgo es que los datos sean mal gestionados por las empresas, sin necesidad de ningún ataque pirata. Un caso reciente lo protagonizó Facebook el pasado otoño. Algunas de sus aplicaciones más populares reenviaban los datos de los usuarios a compañías de publicidad y de análisis (incluso aunque esa información estuviera fijada como privada), según probó un reportaje del *Wall Street Journal*. Son aplicaciones que recopilan el número único de cada miembro, llamado Facebook ID. Introduciéndolo en un buscador se pueden obtener detalles del usuario o de sus amigos: la edad, residencia o trabajo. Son datos muy jugosos para las compañías de publicidad, porque cruzándolos pueden conocer muy bien las actividades, gustos, preferencias e intereses de los usuarios. Y diseñar anuncios específicos para ellos.

Todo ese rastro que dejan los usuarios forma un inmenso caudal de información que las compañías pueden utilizar de muchas maneras, bien en publicidad o con otros fines menos confesables, advierte José Antonio Millán, experto en tecnologías de la información y autor del *Manual de urbanidad y buenas maneras en la Red* (Melusina). Los más conocidos son los estudios para percibir los intereses y gustos de los usuarios. "Se trata de estudios de agregación. No usan datos personales individuales sino de forma agregada; es decir, sumando los de todos", explica Álvaro Ibáñez, de Microsiervos. "Son muestras que no te permiten reconstruir individualmente lo que hace cada persona, sino visiones de conjunto". Un ejemplo sería Google Trends, que muestra los términos más solicitados a través de su buscador y ofrece un panorama de lo que buscan los usuarios. Muchos de estos usos son legales, porque la letra pequeña de los contratos de las redes sociales, correos electrónicos y otros servicios en nube suelen incluir cláusulas sobre cesión de datos para estudios demográficos o estadísticas.

De hecho, los gigantes del sector, Microsoft, Apple y Google, han estado recopilando durante los últimos meses todo tipo de datos de localización de clientes de telefonía móvil sin que estos lo supieran. "Las empresas tienen mucha información sobre nosotros que probablemente no van a usar de forma personal", añade Millán, "pero sí que pueden utilizarla para determinar tendencias; por ejemplo mediante análisis léxicos en Gmail pueden cribar temas y elaborar perfiles publicitarios más finos". "Otra cuestión" -añade Millán- "es con qué fines menos santos puedan emplearla". Uno de los más extremos sería el control social: "En un momento de involución, unos algoritmos más finos -que rastreasen tu correo electrónico, tus fotos, tu opinión y tus documentos- podrían marcarte como un sujeto dudoso". No es nada descabellado. El ensayista bielorruso Evgeny Morozov ha advertido de esta posibilidad en *The Net Delusion*, un correctivo para ciberutópicos. Recuerda el caso de las protestas de Irán en 2009, cuando el Gobierno empleó los perfiles de los manifestantes en Twitter y Facebook para buscar su información personal, sus fotografías y su localización.

El tercer riesgo atañe a las responsabilidades jurídicas de las empresas. Toda esa información concreta y personalizada que acumulan las redes sociales, la proporcionan sus propios usuarios voluntariamente. Facebook registra miles de millones de acciones (fotos, palabras, listas de amigos). Son detalles que se usan para elaborar anuncios personalizados que aparecen cuando navegamos. La red social servirá este año más de un billón de anuncios, según recoge *The New York Times*. Aun así, en EE UU no hay ninguna autoridad federal que supervise el uso de estos datos o sus garantías de seguridad.

En España, las compañías tienen el deber legal de asegurar la seguridad de la información personal. El artículo 9 de la Ley de Protección de Datos obliga a las empresas a adoptar medidas que garanticen la seguridad de los datos y eviten su alteración, pérdida o acceso no autorizado. Además, una directiva europea de 2009, pendiente de transposición en España, obliga a los proveedores de servicios de comunicaciones

electrónicas a notificar las brechas de seguridad a la autoridad nacional competente. Y también a particulares si la violación de datos puede afectar a su intimidad o información personal. En EE UU, en cambio, no hay ninguna ley federal que cubra semejantes vulneraciones de la privacidad, como recuerda *The New York Times*.

El cuarto gran riesgo es el de la conectividad. Sin acceso a la Red, la nube no sirve de nada. En España, la infraestructura aún no se puede comparar con la de países vecinos (por no hablar de EE UU o Japón), según Millán. "Con todo, mejora rápidamente", añade Ibáñez, aunque sostiene que queda pendiente igualar la velocidad de subida y de bajada. "O al menos que se reduzca la desproporción actual; a menudo tienes 10 megas de bajada y 500k de subida, que es fundamental para trabajar en la nube, subiendo fotos o vídeos". La conectividad es el gran reto, considera Torres. "La nube está deslocalizada, y no se puede depender de un centro de datos al otro lado del mundo; debe haber un suministro de nube próximo y garantizado dentro del territorio español o europeo". Lo ilustra con una comparación: "La informática será un servicio, como el agua, la electricidad o el gas; y no es bueno depender de fuera y dejar de producir aquí".

Lo recomendable sería un modelo mixto, opina Millán, "con los documentos menos sensibles o necesarios en la nube, y la información sensible en soporte, con un disco duro externo". Todos los expertos coinciden en que el cambio de modelo del PC a la nube es claro. Queda por ver si las nubes que anuncian los visionarios traerán un paisaje sereno o tiempos tormentosos.

## Almacenes privados

Las empresas con necesidades de poder de computación pueden contratarlo como un servicio más -hay quien lo compara con la electricidad o el agua- a proveedores de **nubes** -Google, Amazon, y muchos otros-, así disponen de una mayor capacidad sin preocuparse del mantenimiento. Pero existe otra opción: crear una **nube** privada. Se trata de la que solo ofrece servicios y recursos compartidos en la propia empresa, a diferencia de la **nube** común (o pública), según señala Jordi Torres, de la Universidad Politécnica de Cataluña. Es costoso, por lo que solo está al alcance de las grandes compañías, las que pueden mantener sus propios centros de datos con servidores (CPD), es decir, la propia empresa se encarga del mantenimiento de su infraestructura. Al ser interna y no estar subida a la gran **nube** de Internet, ofrece unos altos niveles de seguridad.

"El futuro será un punto de encuentro entre los dos *clouds*

**[nubes]**, el público y el privado", vaticina Torres. Desde el punto de vista de la seguridad que la **nube** ofrece a las empresas, Torres señala que "después de WikiLeaks, quién puede garantizar al cien por cien la privacidad de unos datos", y recuerda que los informes diplomáticos del caso fueron filtrados de uno de los sistemas más seguros del mundo. Como todo sistema de seguridad, depende del factor humano. Una cadena es tan resistente como su eslabón más débil, como decía Sherlock Holmes. "Así que el *cloud* puede ser tan seguro como cualquier otro servicio externalizado que esté usando una empresa", señala. Subraya que las autoridades nacionales o europeas deberían garantizar un servicio de **nube** local para no depender de los proveedores extranjeros.

---

## Prácticas seguras en la nube

Al usar el entorno de la **nube** (buscadores, redes sociales, correo electrónico, comercio electrónico, intercambio de archivos), la Agencia Española de Protección de Datos aconseja:

- No grabar ni publicar imágenes ni vídeos de terceros sin su consentimiento.

- El perfil de usuario debe estar configurado con una seguridad adecuada. La información puede aparecer publicada en los buscadores donde puede ser accesible.

- No publicar excesiva información personal, ni detalles que permitan saber la localización física.

- Si le piden datos pero no dicen para qué los van a usar o no entiende la solicitud, nunca los dé. En la Red no todo el mundo es quien dice.

- Borre con regularidad las *cookies* (dispositivos que las compañías instalan en el PC del usuario y que permiten conocer su navegación), los archivos temporales y el historial de navegación.

- Cuidado con publicar datos sobre dónde se encuentra el usuario o terceros (viajes, geolocalización, etcétera)

- Los menores deben navegar acompañados por adultos.

- En el comercio y trámites bancarios, asegúrese de que la conexión es segura y desconfíe de los correos que piden datos personales y claves de acceso.

- Lea con atención las políticas de privacidad.

---