EXPANSION
MADRID
06/11/12
Prensa: Diaria
Tirada: 58.556 Ejemplares
Difusión: 37.495 Ejemplares
Cód: 63295801
Página: 30
Sección: POLÍTICA - ECO Valor: 9.327,00 € Área (cm2): 805,4 Ocupación: 84,03 % Documento: 1/1 Autor: Núm. Lectores: 177000

ENCUENTRO ESPECIALIZADO

"Es necesario crear un marco legal para regularizar el uso de la nube"

CONCLUSIONES DE LOS EXPERTOS/ Una regulación específica también aportaría mayor seguridad a usuarios y proveedores de 'cloud computing', una tecnología de la que todavía muchas empresas recelan.

Expansión. Madrid

La implantación de la tecnología *cloud computing* (o computación en nube) en el funcionamiento diario de empresas e instituciones aporta un gran número de ventajas, como el ahorro de costes y la maximización de recursos, pero al mismo tiempo genera importantes dudas entre sus usuarios, en especial en lo relativo a la seguridad.

Estas incertidumbres son, en buena parte, provocadas por la falta de "un marco común de normas técnicas y aspectos legales" en la Unión Europea, algo que deriva, según diferentes estudios, en que "sólo el 33% de proveedores de *cloud* permiten la eliminación de datos de acuerdo algún estándar reconocido", tal y como apunta Gianluca D´Antonio, presidente de ISMS Forum Spain.

Esta es una situación de la que UE es consciente, y por ello tiene como objetivo marcar "unas normas básicas" para que, tanto proveedor como usuario, puedan hacer un mejor uso de la tecnología *cloud*, tal y como aseguró D´Antonio en el encuentro especializado *Seguridad de la información, los retos de la nube* organizado por Unidad Editorial y patrocinado por IBM en colaboración con Microsoft y Arsys.

De izquierda a derecha: Javier Gil, director de Smarter Cities de IBM; Javier López Tazón, redactor jefe de Ariadna; José Miguel González, gerente de informática del Ayuntamiento de Madrid; y Manuel Escalante, director general de Inteco.

Gianluca D' Antonio
ISMS Forum Spain

"La UE tiene como objetivo crear una serie de normas básicas para el uso del *cloud computing*"

Marta Martínez Alonso
IBM

"Tenemos que intentar implantar medidas a la misma velocidad que crece la tecnología"

Manuel Escalante
Director general de Inteco

"Es necesario concienciar a la sociedad para que entienda qué es el *cloud computing*"

Olof Sandstrom
Dir. de operaciones de Arsys

"No hay grandes diferencias de seguridad entre un entorno *cloud* y otro convencional"

Javier Gil
IBM

"En el futuro será necesario definir qué información es crítica y debe ser protegida de manera especial"

Héctor Sánchez
Microsoft

"La computación en la nube es una tecnología que está aquí para quedarse y no es una moda"

José Miguel González
Ayuntamiento de Madrid

"Madrid está trabajando en un nuevo enfoque de ciudad inteligente con tecnología *cloud*"

Juan Claudio Agui
IBM

"La seguridad en la nube es un proceso conjunto entre proveedor de servicio y cliente"

Ignacio Heras
G-Data

"El usuario debe proteger su tableta y su *smartphone* igual que lo hace con su ordenador personal"

David Alonso
Samsung Electronics

"El 70% de los empleados usan su teléfono móvil personal para uso profesional"

Desconocimiento

El otro gran escollo para la implantación de esta tecnología que ofrece la posibilidad de acceder a servicios de computación alojados de forma externa a través de Internet, es el desconocimiento que gran parte de la población todavía tiene de la misma.

Olof Sandstrom, director de operaciones de Arsys, asegura que su compañía lleva "tres años ofreciendo servicios de *cloud* público y el mayor problema lo encontramos en que los clientes no entienden lo que es el *cloud*".

Según Sandstrom, "no hay grandes diferencias de la seguridad entre un entorno *cloud* y un entorno convencional", y eso es algo que los clientes no entienden, por lo que es necesario realizar "un gran trabajo de concienciación" en la sociedad, tal y como apunta Manuel Escalante, director general de Inteco.

Parte de esa tarea, asegura Juan Claudio Agui, manager de ofertas de servicios de Global Technology Services de IBM, también debe tener como objetivo difundir que "la seguridad en el *cloud* no es algo limitado al proveedor, sino que es un proceso conjunto entre proveedor y cliente".

Información crítica

Una vez que se superen estas barreras, la imparable evolución de una tecnología "que está aquí para quedarse y que no es una moda" tal y como asegura Héctor Sánchez, director de tecnología de Microsoft, provocará que la cantidad de información alojada en la nube aumente de forma exponencial.

Por ello, será necesario "definir qué es lo que se va a proteger, ya que va a haber millones de datos y no se pueden proteger todos", apunta Javier Gil, director de Smarter Cities de IBM.

Este proceso de selección será fundamental para las *smart cities* o ciudades inteligentes, caso en el que existirá información crítica que estará localizada en la nube y que resulta imprescindible para el desarrollo de la vida ciudadana.

Un ejemplo de ello es el Ayuntamiento de Madrid que, según su gerente de informática, José Miguel González, está "trabajando en un nuevo enfoque de ciudad inteligente" y que ya aplica las nuevas tecnologías en procesos tan esenciales como la apertura y el cierre de compuertas o la medición de niveles del agua.

Por todo ello, Marta Martínez Alonso, vicepresidenta de Global Technology Services de IBM, asegura que es necesario que la sociedad sea capaz "de poner medidas a la misma velocidad que avanza la tecnología", algo que hasta ahora no ha ocurrido y que lastra la capacidad del *cloud computing* para realizar negocios y mejorar el nivel de vida de la sociedad.

Protección informática para los smartphones

Los teléfonos inteligentes o *smartphones* y las tabletas "están en el centro del debate de la seguridad" ya que ambos dispositivos "son pequeñas computadoras y los *hackers* buscan en ellos lo que en el pasado buscaban en los ordenadores", afirma Ignacio Heras, responsable de marketing de G-Data. Un dato de lo extendido que está el uso de este tipo de terminales móviles es que "en junio, Google registró 900.000 activaciones diarias de dispositivos con tecnología Android", lo que, en palabras de Heras, supone un "gran atractivo para los piratas informáticos que buscan extender un *malware* o un virus informático". Por ello, continúa Heras, es imprescindible que el usuario se conciencie de que es necesario proteger sus teléfonos móviles inteligentes y tabletas al igual que lo hace con sus ordenadores personales, algo que no ocurre ya que la mayoría de los dispositivos no tienen ningún tipo de solución de protección instalada. Pero esta es una realidad que no sólo afecta a la información personal, no en vano "el 70% de los empleados usan un teléfono móvil personal para uso profesional", tal y como afirma David Alonso, responsable de B2B de la división de telecomunicaciones de Samsung Electronics. Además, cada vez más trabajadores tienen acceso a un teléfono de empresa, lo que no hace más que incrementar las posibilidades que tienen los *hackers* de acceder a información confidencial si los dispositivos electrónicos no están convenientemente protegidos. Pero estas soluciones ya no sólo permiten la protección ante un virus, también ofrecen la posibilidad de, por ejemplo, "eliminar por remoto todos los datos que tiene la terminal" en caso de pérdida, tal y como apunta Heras, evitando que se pueda acceder a contactos y correos electrónicos personales o profesionales.