Medio: **DIRECTOR TIC**
Fecha: **01/12/2016**
Página: **48** Documento: **1/2**
Autor: **REDACCIÓN**

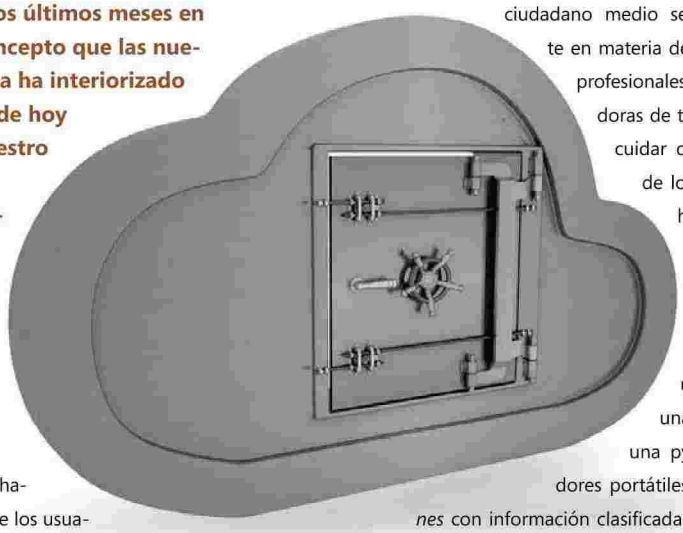
Valor (vpe): **2.535,58€**
Difusión: **6.007**
Audiencia: **24.028**
Ocupación aprox. (%) : **37,91**

PALABRA DE

IR A: Arsys | Qualcomm | Sinnaps |

La realidad de la seguridad en un mundo cloud

Que la forma de consumir e interactuar con el mundo ha cambiado, es un hecho innegable. La transformación digital, de la que tanto se habla en los últimos meses en cualquier foro empresarial, es un concepto que las nuevas generaciones de consumidores ya ha interiorizado y añadido a su vida cotidiana. A día de hoy compramos por Internet, leemos nuestro correo en cualquier lugar y en cualquier dispositivo, gestionamos nuestras cuentas bancarias a través de aplicaciones web, hacemos cientos de trámites administrativos por Internet y consultamos los resultados de nuestras pruebas médicas de forma *online*.



Que estas actividades se hayan convertido en habituales, ha provocado que las expectativas de los usuarios respecto a la funcionalidad, inmediatez y accesibilidad de sitios web, aplicaciones y servicios *online*, también se hayan elevado extraordinariamente. Pero por encima de todo, se ha multiplicado la necesidad de ofrecer y transmitir seguridad a la hora de operar a través de la Red.

La recurrente aparición de noticias sobre filtraciones de contraseñas, espionaje cibernético, robo de datos *online* o ciberataques, ha hecho que el ciudadano medio sea altamente exigente en materia de seguridad, y que los profesionales y empresas proveedoras de tecnología tengan que cuidar dichas cuestiones más de lo que jamás lo habían hecho.

En el mundo empresarial la evolución ha sido similar. Ahora, los empleados de una empresa (sea esta una gran corporación o una pyme) utilizan ordenadores portátiles, *tablets* o *smartphones* con información clasificada sin estar cifrados. No hace tanto tiempo nos parecía una locura acceder desde un cibercafé a alguna aplicación que manejara datos sensibles. Ahora, simplemente nos conectamos al WiFi de cualquier cafetería y empezamos a trabajar.

IR A PÁGINA SIGUIENTE

Medio: DIRECTOR TIC
Fecha: 01/12/2016
Página: 49 Documento: 2/2
Autor: REDACCIÓN
Valor (vpe): 2.535,58€
Difusión: 6.007
Audiencia: 24.028
Ocupación aprox. (%) : 36,66

PALABRA DE

IR A: Arsys | Qualcomm | Sinnaps |

Situación crítica

Así pues, si la securización de los servicios IT siempre había sido una cuestión importante para los proveedores *cloud*, con la irrupción de un nuevo modelo de usuario, permanentemente conectado, multidispositivo y en movilidad, la situación se ha vuelto crítica. Ahora los proveedores de servicios y soluciones *cloud* tienen que abordar las cuestiones de seguridad desde un doble punto de vista: desde dentro y desde fuera.

De un lado están las habituales medidas de seguridad internas. Es decir, los sistemas de redundancia, monitorización, segregación y aislamiento que deben implementarse sobre las cinco capas que componen todo proyecto *cloud*: software, capacidad de computación, almacenamiento, redes y *datacenters*. Sin embargo, estas medidas ya no son, ni mucho menos, suficientes. Ahora, si vamos a sumar a nuestro proyecto una aplicación accesible desde Internet, debemos sumar forzosamente medidas específicas como sistemas de monitorización y alerta temprana a todos los niveles, cortafuegos de red y de aplicación, herramientas de detección, prevención y protección frente a intrusiones, ataques DDoS, código malicioso y por supuesto, copias de seguridad.

Pero no solo eso, cuando en nuestro proyecto se vean involucrados datos personales, que suponen un alto nivel de seguridad, y que están específicamente protegidos por el Reglamento de Protección de Datos (RLOPD) habrá que implementar, prácticamente por defecto, medidas como el cifrado de datos y comunicaciones, la creación y externalización de copias de seguridad y la generación de registros de accesos que identifiquen a usuarios, fechas y horas de acceso, ficheros consultados, etc.

Así pues, hoy más que nunca, la gestión de la seguridad de cualquier proyecto IT requiere de profesionales altamente cualificados y especializados. Todas las complejidades actuales en materia de seguridad deben ser asumidas por proveedores que puedan ofrecer estas dobles medidas de seguridad que, bajo un modelo internalizado, simplemente no se podrían amortizar.

La realidad ha cambiado y, en consecuencia, las formas en las que proteger la información en este nuevo mundo digital deben ser mucho más completas y abordarse desde diferentes perspectivas, tanto internas, como externas.

Juan Manuel Robles
Director de Cloud Solutions en Arsys

IR A PÁGINA SIGUIENTE