



## Entrevista a John Sabo

**Director  
Global Government Relations  
CA**

REALIZADA POR  
**Antonio Ferrer**

**J**ohn Sabo es Director de Relaciones con el Gobierno en la multinacional CA, antes de prestar sus servicios en el sector privado fue director de los Servicios Electrónicos de la Seguridad Social en los EE.UU.

John es reconocido como un líder en el desarrollo de servicios de gobierno electrónico, siendo un orador habitual en los simposios internacionales de seguridad y colabora con diversas revistas con artículos y estudios técnicos sobre seguridad, privacidad y confianza. También ocupa el cargo de Presidente de la International Security Trust and Privacy Alliance (ISTPA) que ha establecido las normas básicas de los servicios de privacidad.

Para resumir podemos decir, sin miedo a equivocarnos, que es un sabio en temas de seguridad y confianza. Por todas estas razones no hemos podido resistir la tentación de entrevistarle para que comparta sus conocimientos con nuestros lectores.

**¿Cuáles son hoy en día los principales retos relacionados con la seguridad de la información, la privacidad de la información y la confianza?**



El primer reto es el de gestionar los sistemas, aplicaciones e información basadas en TI, cada vez más complejos, interdependientes y conectados. Esto es un problema de base porque cada vez más gobiernos y empresas integran servicios tanto de cara a usuarios internos como externos usando las innovaciones de la Web 2.0, SOA y funciones de negocio externalizadas. Comprender y gestionar todo el entorno informático y sus interdependencias es fundamental para la seguridad y la privacidad.

Existen soluciones disponibles para ayudar a resolver este problema, a menudo basadas en estándares como COBIT e ITIL, o en estándares de seguridad, como ISO 27001/2, SAML, WS-Federation, entre otros.

Un segundo reto es evaluar y gestionar el riesgo en privacidad y seguridad en este nuevo entorno mundial basado en el protocolo de Internet. Esta cuestión, que ya se destacó en un informe de la Business Roundtable [www.businessroundtable.org](http://www.businessroundtable.org), también se está abordando a nivel técnico en un proyecto de la

administración y la industria TI en Estados Unidos que consiste en desarrollar una nueva metodología para evaluar el riesgo en ciberseguridad. Esto es vital no sólo para crear soluciones que gestionen el riesgo, sino también para guiar las inversiones en I+D.

**Algunas cifras que manejan varios fabricantes de soluciones de seguridad indican que cerca de 50% de los ordenadores personales están infectados por algún tipo de malware y esto está sucediendo a pesar de contar con buenas herramientas de protección. ¿Cómo cree que esto podría afectar a la privacidad de la información de los usuarios? ¿Qué pueden hacer los usuarios?**

En el entorno actual de la web, la innovación está creciendo enormemente, involucrando a miles de millones de individuos, usuarios conectados y dispositivos portátiles. Los usuarios se han convertido ahora en objetivos o son explotados como vectores de ataque para lanzar ataques sobre otros, y las amenazas son



internacionales. La ciberseguridad y la privacidad personal son ahora una responsabilidad compartida por muchas organizaciones y millones de usuarios.

La responsabilidad compartida no significa que "nadie es responsable", sino que los usuarios tienen un papel a desempeñar, por ejemplo, seleccionando un ISP que ofrezca protección de seguridad fuerte, usando software de gestión de amenazas y actualizando las firmas anticódigo maligno. Significa utilizar contraseñas fuertes, o tokens, para la autenticación, comprobar los certificados SSL del sitio web para asegurarse que es legítimo y educar a los niños sobre prácticas seguras en el uso de Internet. Los usuarios que participan en redes sociales o están en sus puestos de trabajo tienen un papel a desempeñar. Y es ahí donde son vitales las iniciativas educativas y de concienciación en España y en todas partes del mundo.

**¿En su opinión, cómo se podría mejorar la privacidad de la información, tanto en las empresas privadas como en los organismos gubernamentales?**

Según mi experiencia, cuando piensan en privacidad, muchos expertos técnicos se centran sólo en



la seguridad de la información (en la confidencialidad de los datos). La impresión general es que el único problema es la pérdida de discos duros con información personal no encriptada. Pero la privacidad de la información incluye la autenticación de usuarios y aplicaciones, el control de accesos, la integridad de los datos y la disponibilidad de los sistemas.

Y la gestión de la seguridad sola no puede asegurar completamente la privacidad. La directiva de datos de la

Unión Europea y la mayoría de leyes internacionales sobre privacidad la definen como un amplio conjunto de requisitos, incluyendo la minimización de datos, aviso y consentimiento, acceso individual a los datos sujetos a información, calidad de datos, responsabilidad y obligación de cumplimiento. Recomiendo el estudio "Analysis of Privacy Principles: An Operational Study," publicado [www.istpa.org](http://www.istpa.org) como buen punto de partida para comprender cuáles son los requisitos de la privacidad de la información.

Los arquitectos tecnológicos deben comprender todos los requisitos de privacidad aplicables a sus servicios conectados y garantizar el apoyo a las políticas, prácticas y controles técnicos de privacidad. Es un problema serio porque la explosión de estándares, tecnologías y soluciones interoperables que intervienen en los servicios web no ha venido acompañada de un desarrollo similar de estándares y soluciones de privacidad. Y también, el flujo mundial de la información significa que las leyes, regulaciones y políticas también deben interoperar más allá de las fronteras jurisdiccionales.





Un buen inicio es empezar por la gestión de riesgos de seguridad, incluyendo la gestión básica de las identidades y la autenticación. La seguridad TI es una disciplina madura con muchos estándares y soluciones disponibles, pero aún hay trabajo por hacer en estándares y soluciones para los requisitos de privacidad.

### ¿Es la confianza una cuestión estratégica para empresas y gobiernos? ¿Por qué?

La confianza es una cuestión estratégica. En la conferencia ISSE de Madrid, se preguntó si la comunidad de seguridad TI podía aprender alguna lección de la crisis financiera mundial. Y lo cierto es que sí vimos paralelismos entre el colapso de la confianza financiera y riesgos similares en la compleja infraestructura conectada en la que se basan los servicios TI y comunicaciones mundiales, opaco para los usuarios finales, y sinceramente, para muchos ejecutivos de empresas y de la administración pública.

Nuestra infraestructura TI conectada es muy compleja y su gobierno y responsabilidad están distribuidos. El DNS raíz y los operadores Generic Top Level Domain (GTLD), los ISPs, las compañías de software y hardware, los proveedores de servicios de seguridad, los integradores de sistemas TI y los usuarios de las empresas y de las AAPP son algunos de los componentes del entorno mundial conectado. Y también lo es el usuario final. Todos ellos sostienen la confianza de Internet, que a su vez, sostiene la confianza de la sociedad y la empresa.

Los mundos físico y lógico se están convirtiendo en algo conectado e integrado y es prácticamente imposible retroceder a sistemas de papel y a las viejas tecnologías. Mantener la confianza (por ejemplo, la integridad de los datos de la administración pública, autenticar un sitio web



bancario, tener una resolución fiable del nombre del dominio o garantizar unos precisos registros sanitarios) será cada vez más importante porque aumentan los servicios y dispositivos interconectados y las aplicaciones son más interdependientes.

### Si una organización le pide las grandes líneas de un Política Integral de Privacidad, ¿cuál sería su respuesta?

En mi opinión una política integral de privacidad de la información debe abordar todos los principios de privacidad y las prácticas que exigen las regulaciones, las leyes y las necesidades de la empresa, y hacerlo en términos de los sistemas interconectados y relaciones de la compañía o administración pública.

Idealmente, también debería poder configurarse la política, es decir, que hubiera un soporte automatizado para los requisitos de sistemas y procesos exigidos por las diferentes jurisdicciones. Por ejemplo, los requisitos de privacidad pueden ser distintos en cada país, pero una multinacional puede estar manejando información personal de usuarios de varios países. Debemos abordar la privacidad en su conjunto cuando se

desarrollan políticas de privacidad y se toman medidas para que se cumplan en los sistemas TI y en los servicios en los que se recopila, comunica, procesa y almacena información personal.

### ¿Cómo contribuye CA en la mejora de las políticas de privacidad de la información de empresas y gobiernos?

Las tecnologías y soluciones Enterprise IT Management de CA hacen posible la gestión integrada del gobierno, la infraestructura y la seguridad, que es justo el modelo necesario para soportar el nuevo entorno TI integrado de personas, servicios y cosas, y garantizar la gestión de los riesgos de privacidad y seguridad. Creo que la contribución de CA es muy valiosa porque, además de la labor de difusión, contribuye con visión y soluciones a una gestión integral de la privacidad. El trabajo de CA en apoyo de la ISTPA, organizaciones de estándares y nuestra propia visión EITM son formas de garantizar que las políticas de privacidad sean más que palabras, que realmente pueden implementarse en un complejo entorno mundial. ♦