

“La demanda de seguridad TIC por impulsos está dejando paso a un modelo de mercado basado en el desarrollo de planes globales plurianuales”



Teresa Núñez,
responsable de Consultoría
de Seguridad de
Schlumberger

Son escasos en España los consultores que aunan en su saber conocimientos actualizados sobre normas y estándares, técnicas de organización y gestión, análisis de riesgos y tecnologías de protección. Teresa Núñez, responsable de Consultoría de Seguridad de Schlumberger, además de disponer de dichos conocimientos, cuenta con una apreciable experiencia en el desarrollo de proyectos complejos, que son los que en su opinión van a marcar la pauta del mercado de seguridad en los próximos años.

– ¿En qué fase se encuentra hoy el mercado de seguridad TIC en España?

– Antes la seguridad se concebía como un conjunto de controles monolíticos y puntuales, sustentados casi siempre por mecanismos de protección tecnológicos contruidos sin visión evolutiva y al ritmo de determinados hechos puntuales. En la actualidad la tendencia, muy clara en EE.UU. y bastante definida en la UE, viene marcada por la concepción de la seguridad TIC como un programa o plan. Siguiendo esta tendencia, aún nueva en España, el programa o plan director de seguridad TIC se define con un presupuesto dedicado, con una base organizativa específica para gestión, con un método global y desde una óptica de oficina de proyecto.

– ¿Está colaborando Schlumberger en esta línea con algunos usuarios?

– En España el proyecto más paradigmático en el que estamos colaborando es el Plan Director CIS de Defensa, en el que desde el primer momento se concibió la seguridad TIC con esta visión de plan integral. Fuera de nuestro país hemos trabajado para la organización de Correos de Suráfrica. Se nos pidió la creación de un plan director de seguridad con marco referencial en la ISO 17799, en la que se tuvieron en cuenta los análisis de riesgos, las políticas, las normativas y el plan de contingencias y continuidad de negocio. Se hizo en combinación con algunas empresas locales para la realización de determinados análisis detallados de vulnerabilidades en las distintas oficinas de correos del país. En este proyecto también tuvimos que ‘securizar’ toda la arquitectura de interconexión de sucursales.

– Usted, en tanto que profesional de la consultoría de seguridad TIC, conoce a la perfección normas como la ISO UNE 17799. Pese al ruido que ésta ha hecho, quizás las compañías no estén respondiendo a la certificación como era de esperar.

– El seguimiento de estándares es un principio generalmente admitido en muchas disciplinas, seguridad incluida. Los británicos se han tomado su BS 7799 muy en serio, de tal manera que hay numerosas organizaciones embarcadas actualmente en el proceso metódico de certificación de conformidad con la norma. En otros países europeos y en países asiáticos ya empieza a notarse lo propio en relación con la ISO 17799. Como suele suceder, en España vamos con cierto retraso. En la última edición de Infosecurity, celebrada en UK, se hizo énfasis en que dentro del modelo de negocio de proveedores de tecnología, en los SLAs se estaba exigiendo disponer de la certificación BS 7799 para poder participar en concursos. Aquí, en España, no se le ha dado este enfoque a la ISO UNE 17799; más bien se tiende a concebir como un marco de referencia para el planeamiento de la gestión de la seguridad.

– Seguir la norma pero no certificarse. ¿Un problema de tiempo, de dinero, de prioridades, de cultura?

– Un poco de todo; no obstante, es un hecho que cuando vamos a realizar un servicio referente a seguridad de la información alusivo a la definición de una política, de normativas o de un plan de seguridad, se nos exige usar como marco de referencia la ISO UNE 17799. La razón es sencilla: muchas veces la compañía cliente –sobre todo si es multinacional, aunque no en exclusiva– está sometida a auditorías periódicas. Seguir la norma –que no certificarse– facilita la realización de tales auditorías.

De todos modos, insisto: el no seguir formalmente el cumplimiento de normas es una característica del mercado español.

– ¿Qué opina de la certificación de la seguridad de productos TIC? ¿Le parece viable el modelo existente?

– Las organizaciones dedicadas a la creación y publicación de estándares han hecho un gran esfuerzo en lo

que se refiere a la evaluación y certificación de la seguridad de productos TIC para que no se impongan en los mismos las especificaciones técnicas de los fabricantes, sino más bien las necesidades de los clientes. Creo por tanto que los Criterios Comunes y la puesta en funcionamiento del concepto de Perfil de Protección redundan en este aspecto capital. Obviamente, la aplicación de este modelo resulta todavía muy costosa en términos económicos.

– **¿Qué áreas del mercado de servicios de seguridad de la información le parecen más prometedoras a largo plazo?**

– Todos tienen un excelente futuro por delante, tanto los de consultoría y prescripción como los de tecnología/soluciones, integración de sistemas y externalización de la gestión. Cualquier proveedor que quiera mantenerse como jugador de peso en este mercado deberá contar en su portafolio con una oferta global, incluyendo el epígrafe del cumplimiento de la legislación que sea de aplicación, ya que hoy por hoy, la tendencia de los usuarios que invierten en seguridad es a demandar a sus proveedores los servicios necesarios para el desarrollo de planes globales de arriba a abajo.

– **¿De dónde debería depender jerárquicamente la función de seguridad en una entidad típica?**

– La seguridad TIC debe de depender del órgano de mayor rango en materia de aplicación de tecnologías de información en una empresa. La función de seguridad de la información, por su parte, conviene encuadrarla en un nivel de *staff* de la dirección. Parece incontrovertible que son las áreas de negocio de una entidad las que deben solicitar que la seguridad se integre en los procesos TIC que dan soporte a las actividades. Esta es la clave para resolver el siempre polémico contexto organizativo y jerárquico de la seguridad.

– **¿No le parece que los mercados de consultoría y asesoría acerca de la protección de datos personales está algo ralentizado?**

– En lo que concierne al Reglamento de medidas, y debido al cumplimiento de plazos de adaptación, hubo en su momento un gran crecimiento de la demanda, sobre todo en el ámbito privado. Y ese ritmo no puede mantenerse hoy. Lo que sí noto es la apertura de proyectos más globales y de mayor volumen en la materia, especialmente originados en el sector público.

– **Entre los servicios que ofrece su compañía, se encuentran los de consultoría tecnológica y prescripción. ¿Están los desarrollos de las casas comerciales de herramientas a la altura de las necesidades de los usuarios corporativos en materia de protección de la información?**

– En líneas generales, las tecnologías de protección o que pueden utilizarse para fines de protección, están razonablemente maduras para que el usuario se base en ellas para configurar sus soluciones corporativas de seguridad. La única línea tecnológica que está en proceso de mejora y refinamiento es la relativa a los IDS, que está virando hacia una concepción más cercana a la previsión de intrusiones que a la detección. Otras herramientas, como las orientadas a la gestión de identidades y aprovisionamiento, las de análisis y gestión de *logs*, y las diseñadas para prestar servicios de confidencialidad, integridad y disponibilidad, están en una fase de madurez tecnológica más que aceptable. Asunto distinto es que para su implantación y despliegue sea prudente recurrir al mercado de integradores con experiencia.

– **¿Qué opina del ROI como justificación de proyec-**

tos de gestión de identidades y aprovisionamiento?

– Hace unos años, cuando la seguridad estaba muy imbricada con la gestión de sistemas, hubo un repunte de *frameworks* en los que se integraba la administración de seguridad de usuarios. Aquello no cuajó. Cada usuario tuvo que buscarse la vida para intentar de alguna manera automatizar al máximo este proceso de administración. Hoy, la llamada gestión de identidades y aprovisionamiento está bien sustentada en soluciones de fabricante, con lo que el emprendimiento de estos proyectos, a partir de cierta dimensión de heterogeneidad tecnológica y número de usuarios, suele tener una justificación clara también por ROI, y no sólo por la mejora de la calidad de servicio al usuario y el fortalecimiento de la seguridad



“Son las áreas de negocio de una organización las que deben solicitar que la seguridad se integre en los procesos TIC que dan soporte a sus actividades”

global en la organización. En este año es rara la compañía que no ha emprendido iniciativas para crear su directorio corporativo, algo esencial.

– **¿Le parece interesante el proyecto de DNI electrónico de la Dirección General de la Policía?**

– Es el paradigma en lo referente al despliegue de una PKI y certificados electrónicos para autenticación y firma almacenados en tarjeta inteligente. Tenemos un gran interés profesional en tener la oportunidad de colaborar con la DGP, ya sea en los ámbitos de consultoría como en los de servicios.

– **¿Cuál ha sido el proyecto de consultoría de seguridad de la información más estimulante en el que ha participado?**

– Me decanto por nuestra contribución al desarrollo del Plan Director CIS de Defensa, en el que estamos participando a efectos globales, y no solo en seguridad TIC. Era un reto desde el punto de vista tecnológico, desde el punto de vista de la concepción de una nueva organización y desde el punto de vista de la coordinación e integración de distintos proyectos sometidos a compromisos contractuales en su con-

secución y entrega. Nuestro trabajo ha consistido básicamente en asesorar al respecto de cómo organizar la seguridad, de cómo desplegarla, crear políticas y normas. Igualmente se nos ha requerido nuestra opinión profesional sobre distintas alternativas tecnológicas y herramientas técnicas.

– **¿Se aprende mucho sobre seguridad TIC en la organización de unos acontecimientos tan especiales como son los Juegos Olímpicos?**

– Nuestra responsabilidad en los JJ.OO. atañe a los sistemas soporte y a la seguridad de dichos sistemas, a efectos organizativos y tecnológicos. En Salt Lake City desarrollamos a medida muchos de los sistemas de seguridad: gestión, intrusiones... A partir de ahí creamos productos paquetizados que han funcionado en Atenas. Uno de los más importantes ha sido el denominado Cuadro de Mando, que permite hacer informes de situación a medida, quincenales, semanales, diarios y en ocasiones en línea, para los distintos responsables con acceso permitido a la información. En realidad, hemos desarrollado toda una infraestructura de herramientas alrededor de la gestión de la seguridad, la detección de intrusiones y la monitorización, que refinaremos para los siguientes Juegos Olímpicos. Por cierto, el responsable de seguridad de los JJ.OO. es un profesional de nuestra compañía.

– **¿Y es muy difícil diseñar y probar en cada edición de los JJ.OO. un plan de contingencias informático y de comunicaciones?**

– Tiene su complejidad por razón de la gran concentración de medios materiales, activos de información y personas en un corto periodo de tiempo, lo que obliga a realizar pruebas en unas condiciones muy especiales, contempladas en el análisis de riesgos. No obstante, tenemos experiencia y disponemos además de una estrategia a efectos de necesidades de respaldo en caliente y frente a contingencias muy severas. Para ello utilizamos los más de 40 centros de respaldo que Schlumberger tiene distribuidos por el mundo en su área de *Recovery*. Además, la infraestructura tecnológica de los Juegos está diseñada en alta disponibilidad desde Salt Lake City. La interconexión de redes para la divulgación casi en tiempo real de los resultados de las pruebas obliga a extremar los controles en este aspecto crítico de la seguridad informática.

– **Cabe suponer que en los análisis de riesgos que realizan para sus clientes, contemplan ustedes los posible apagones de luz, hecho que inhabilita prácticamente cualquier servicio basado en medios electrónicos e informáticos...**

– Este es un asunto muy crítico. El corte generalizado de fluido eléctrico padecido por Italia tras el verano, ha llevado al Banco de Italia a dictar una norma que obliga a todos los bancos del país a tener un plan de contingencia en el que se incluya la disposición de un centro de respaldo. Este es un paso importante que puede extenderse a otros estados de la UE. Obviamente, y como es sabido, las entidades financieras se mueven ya en el escenario de los denominados riesgos operacionales definidos en Basilea 2.

En España venimos notando en 2003 un incremento en la demanda de primeras fases de análisis de riesgos y de planes de contingencia informáticos, y no sólo en la banca y las finanzas, sino además en la industria y en el sector público. ■

Texto: José de la Peña Muñoz

Fotografía: Jesús A. de Lucas