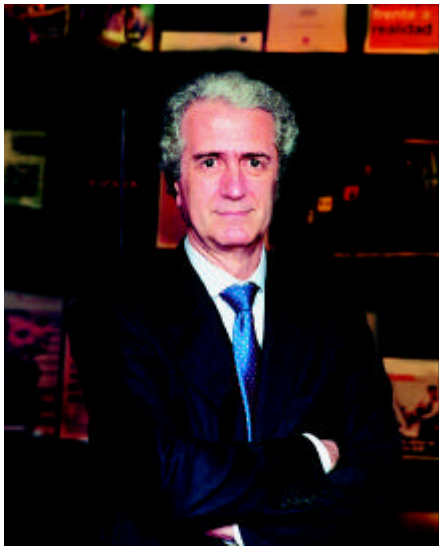
Juan Miguel Ramos Escobosa, Socio responsable en España de la Unidad de Gestión de Riesgos Informáticos -Technology Risk Consulting- de Arthur Andersen

"Las empresas han de convertir la necesidad de la seguridad informática en ventaja competitiva y atreverse a divulgar el cumplimiento de normas"

Doctor Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, y CISA (*Certified Information Systems Auditor*), Juan Miguel Ramos Escobosa es, sin duda, uno de los profesionales de nuestro país con más dilatada trayectoria en las actividades de auditoría informática, evaluación de seguridad y riesgos informáticos en los negocios. Al frente de una de las unidades especializadas de más larga historia en España, este experto de Arthur Andersen ha sido siempre fiel a sus ideas, forjadas en el campo de batalla de nuestro no precisamente fácil mercado.



– ¿Qué se entiende en Arthur Andersen por seguridad en tecnologías y en sistemas de información y comunicaciones?

– La seguridad no es un estado, sino un proceso, y como tal proceso requiere organización, personas, procedimientos... La seguridad, es decir, el proceso de seguridad, debe ser acorde con normas de amplio reconocimiento, como por ejemplo el Código de buenas prácticas para la gestión de la seguridad de la información, BS 7799, que como sabe ha sido aceptado por ISO. Si se estudia detenidamente este estándar, muy estructurado y sistemático, no por ser breve deja de contener verdades como puños.

– ¿Considera que la realidad actual ha introducido algún cambio cualitativo en la seguridad TIC que realmente la diferencie de la imperante en otras épocas?

– Las necesidades de la seguridad han ido cambiando a lo largo del tiempo. Hoy, por ejemplo, es necesario dotar a los servicios de una disponibilidad 24x7, cosa que hace años no sucedía, puesto que se trabajaba en un escenario muy diferente. Considero, también, que en España la aparición de la legislación sobre tratamiento de datos de carácter personal, permite establecer un antes y un después en el mundo de la seguridad.

Por otra parte, las comunicaciones avanzadas, y en especial las redes IP, están protagonizando una de las revoluciones más significativas en el escenario de la seguridad técnica. Mucha gente habla de servicios de confidencialidad e integridad de mensajes, o de identificación y autenticación de usuarios, antaño circunscritos estrictamente al entorno profesional de las TIC.

– De los riesgos en los negocios, ¿cuáles específicamente están conceptuados en Arthur Andersen como de seguridad TIC?

– Arthur Andersen dispone desde hace años de un modelo evolutivo de riesgos de negocio muy exhaustivo. Los tres grandes grupos de riesgo recogidos son los de entorno, los operativos y los de la información para la toma de decisiones, y en el corazón de todos ellos se identifican cinco riesgos tecnológicos: los tres tradicionales de integridad, disponibilidad y confidencialidad, uno de infraestructura y uno de relevancia. La relevancia en un concepto esencial. Significa que la que información que debe protegerse es aquella importante para el negocio.

– ¿Se aplica correctamente este concepto en las entidades?

– Se aplica poco.

– De los riesgos de seguridad antedichos, ¿cuáles le parecen más críticos?

– Personalmente opino que los que afectan a la integridad de la información. Por serle sucinto: si la información no es íntegra, todo lo demás sirve de bien poco. De lo que se trata en última instancia es de que la información tenga garantías de integridad y, por extensión, sea fiable.

– ¿Cuántos expertos prestan sus servicios actualmente en la Unidad de Gestión de Riesgos Informáticos de Arthur Andersen, y cuántos lo hacen específicamente en el epígrafe de seguridad TIC?

– Somos cerca de cien profesionales trabajando en la gestión de riesgos tecnológicos, la mayor parte de ellos en seguridad.

– ¿Han experimentado en la Unidad un crecimiento de actividad en el ejercicio de 2000?

– Sí, de entre un 35% y un 40% en relación con lo registrado en el ejercicio de 1999, y si no hemos crecido más es porque no encontramos suficientes profesionales en el mercado.

– ¿Estaría de acuerdo con la siguiente afirmación: los fabricantes de herramientas y productos tecnológicos ponen a la venta soluciones poco probadas en materia de seguridad técnica, o que no disponen de las funcionalidades y mecanismos de seguridad que se necesitan hoy en los negocios?

– Hace unos años, el mercado no demandaba determinadas capacidades y servicios de seguridad en productos de TIC, y sí funcionalidad. La seguridad, por tanto, era algo marginal y añadido. Últimamente esto está cambiado, pero hasta que los procesos de calidad en el desarrollo de software adquieran la madurez necesaria para controlar adecuadamente el desarrollo de las funcionalidades de seguridad pasará un cierto tiempo. Digamos que los fabricantes de TIC están precisamente ahora adaptándose a las demandas de los usuarios.

Por otra parte, quizá la rápida velocidad de los acontecimientos puede estar propiciando un cierto apresuramiento en el lanzamiento de algunas herramientas tecnológicas.

– A grandes rasgos, ¿en qué debería consistir el trabajo de un director de seguridad TIC en una organización?

– Depende mucho del tamaño de la organización. Las pequeñas tendrán a la seguridad en el último puesto de sus prioridades. A medida que la organización crece, empieza a haber especialización y segregación de funciones, hasta que se llega a las grandes organizaciones, en las que sí existe la figura de responsable de seguridad TIC. Su misión es la de gestionar y marcar las políticas, pero no debería ser la de administrar. Gestionar consiste en recoger información lo más automatizadamente posible de los distintos registros, compilarla, y estudiarla y analizarla. La seguridad, sin duda, debe formar parte de la gestión empresarial. La otra labor, la de la administración del día a día de la seguridad, debe automatizarse con la ayuda de herramientas adecuadas y/o descentralizarse por áreas, departamentos... etc.

– ¿Cómo estratificaría las distintas áreas de trabajo de un departamento de seguridad TIC en una organización típica?

– Así, sin más, creo que sería procedente una primera división obvia por tecnologías y plataformas: red, *ebusiness*, *mainframe*, Unix, NT, Windows 2000... En todo caso, una de las funciones básicas que debe tener ese departamento de seguridad, ya se incardine en su director ya se comparta, es la de conseguir la uniformidad de las políticas, de los procedimientos y de las normas de aplicación en los distintos entornos tecnológicos. Ocurre, sin embargo, que la respuesta de los fabricantes en las diversas plataformas en lo concerniente a funcionalidades de seguridad, es bastante diferente.

– ¿Qué argumentos puede utilizar un Director de seguridad TIC para convencer a los directivos de departamentos de su organización con responsabilidades de pérdidas y ganancias de que han de invertir en seguridad? ¿Asustar?

– Es uno de ellos, y que conste que lo ha menciona-

do usted. Más en serio le diré que 'vender' internamente la seguridad con argumentos de ahorro de coste no me parece procedente en todos los casos. En la gestión centralizada de usuarios, la sincronización de contraseñas y la entrada única, por ejemplo, sí se puede argumentar; en la implantación de una PKI, no. La PKI no genera ahorro de costes, sino que facilita nuevos negocios.

En ocasiones yo he utilizado el argumento del coste de la 'no–seguridad', que se concreta en los daños económicos y en los daños de imagen. No obstante, en mi experiencia no he tenido nunca que justificar un proyecto de seguridad en base a conceptos como el ahorro de costes o similares. La seguridad es una inversión, y dicha inversión debe hacerse con 'luz y taquígrafos'.

– Hablemos de mercado. ¿Qué ofrece Arthur Andersen a sus clientes o posibles clientes en el epígrafe de seguridad TIC?

– Tres valores: primero, conocimiento –hace algunos años a esto se le llamaba experiencia–; segundo, método, en decir la aplicación de ese conocimiento siguiendo unas pautas, una estructura y una sistematización, y tercero, independencia frente a cualquier fabricante. Arthur Andersen quiere mantenerse independiente, aunque admito y me parece defendible que otras compañías opten por 'casarse' con una buena tecnología. Pero son modelos de negocio distintos. Arthur Andersen apuesta por la independencia.

Bajo estas premisas, le puedo indicar, más específicamente, que nuestra oferta en seguridad TIC se centra en tres grandes áreas: revisión y diagnóstico con emisión de informes de estado y recomendaciones, diseño de sistemas de seguridad, e implantación de herramientas e integración de sistemas de seguridad.

– ¿Cuáles son las líneas de trabajo en seguridad TIC que más les están demandando sus clientes?

– Aunque seguimos teniendo trabajos en el mundo *mainframe*, he de reconocer que hoy *ebusiness* es la palabra para todo. Descendiendo a aspectos más concretos, ciertamente hemos registrado entradas en la creación de sistemas centralizados de recogida de datos sobre la actividad de la seguridad. Con esos datos se puede obtener una información de incalculable valor sobre los estados de seguridad en las redes y sistemas heterogéneos de una empresa. También tenemos demandas en la prescripción de herramientas tecnológicas, ya por necesidades puntuales de clientes, ya en el contexto de proyectos más amplios.

Por otra parte, estamos notando un cierto despertar en el planteamiento de proyectos de administración centralizada de usuarios, y una muy importante actividad en la revisión y diagnóstico de la seguridad de las redes corporativas.

– En su opinión, ¿qué distingue a su compañía de otras que podrían considerarse como 'la competencia?

– Como actitud general, en todo proyecto, además de aplicar el conocimiento, el método y la independencia que creo nos definen, procuramos entender lo que en realidad es importante para el negocio del cliente. Hay otro aspecto esencial en nuestra forma de abordar el mercado: la focalización. Nuestra Unidad lleva ya muchos años dedicándose en exclusiva a la gestión de los riesgos tecnológicos. No somos, precisamente, unos recién llegados.

También es cierto que en la Unidad, desde hace muchos años, apoyamos y financiamos el estar en posesión del título CISA y mantenerlo vivo. Es un requisito indispensable para 'hacer carrera' interna.

– ¿Cuál es el proyecto de seguridad más ilusionante en el que ha participado Arthur Andersen en España en los últimos tiempos?

– Hay varios. En algunos nuestra misión consiste en diseñar la seguridad de negocio desde cero; me estoy refiriendo a *star-ups* B2B centradas en mercados digitales orientados a los sectores de finanzas, construcción e industrial...; en otros, nos encargamos de renovar la seguridad de una gran organización que aunque ya dispone de sistemas de seguridad, quiere modernizarse. En este último caso disponemos de referencias en el sector bancario y en el de telecomunicaciones. Hay otros proyectos, quizá menos ilusionantes pero, sin duda, más numerosos, que tienen por finalidad retocar áreas de la seguridad ya existente en una organización para mejorarla.

"La concienciación de todos los usuarios de una organización es capital para el éxito en todos los niveles de la gestión del riesgo tecnológico"

– ¿Cómo cree que conciben o entienden la seguridad TIC los directivos de áreas económico–financieras, jurídicas, comerciales, de marketing, de auditoría y de TIC..., en una organización española típica?

– Hay actitudes de todo tipo: el que piensa que no le va a pasar nada porque, básicamente, nunca le ha pasado; el que está honradamente preocupado e invierte lo adecuado, sin pasarse; el que cree que está libre de peligro porque dispone, sin más, de herramientas y tiene una falsa sensación de seguridad; y finalmente el más peligroso, aquel que cree que está fuera de peligro porque no entiende de los problemas que lleva aparejados la falta de seguridad, y piensa que hay otros en la compañía que ya lidian con ese toro. En el momento en que pasa algo, se suele llevar las manos a la cabeza y se pregunta: "¿Cómo es posible que haya sucedido esto?"..., cuando a lo mejor él fue quien en el pasado cortó el presupuesto de inversión en seguridad.

No hay duda: la concienciación de todos los usuarios de una organización es un aspecto capital para el éxito en todos los niveles de la gestión del riesgo tecnológico. Al respecto tengo que romper una lanza a favor de los directivos informáticos, ya que, en mi experiencia, constituyen el colectivo profesional que suele estar más concienciado en la materia que nos ocupa, independientemente de que aborden o no proyectos.

– En los tiempos que corren, las actividades mercantiles (productos y servicios) relacionadas con la seguridad TIC van muy bien. Algunos opinan que como nunca. ¿Cree usted, al margen de los datos estadísticos al uso sobre crecimientos, que este es un fenómeno pasajero?

– La seguridad no es una moda: está para quedarse. Hay dos factores detonantes, uno global, que es el *ebusiness*, y otro local, la existencia de la Ley de protección de datos personales y del Reglamento de medidas de seguridad. He de añadir que la protección de datos personales está calando no sólo en Europa, sino también en el mundo americano. Canadá ha dado unos pasos muy significativos al respecto, al igual que Argentina. En EE.UU. está costando más, pero es una cuestión de tiempo.

– ¿Le parece muy difícil de cumplir, cuando no imposible, algún mandato del Reglamento de medidas de seguridad para algunos Responsables de Ficheros de titularidad privada que operan en España?

– La seguridad TIC, antes de la publicación del Reglamento, era un páramo, con excepción de algunas grandes entidades que ya tenían una organización relativamente bien montada. El Reglamento es un texto de exigencia media y genérico, a fin de que el paso del tiempo no lo deje obsoleto. ¿Hay algunos mandatos más difíciles de cumplir que otros? Sí. ¿Hay mandatos difíciles de cumplir? Sí, en función de la tecnología, del estado de la tecnología y de las organizaciones. Las grandes tienen dificultades debido a la gran cantidad de ficheros que han de proteger y de los datos personales que tratan.

– ¿Qué opinión le merece el papel de la auditoría obligatoria en el contexto del Reglamento de medidas?

– No hace sino extender también a este ámbito la filosofía tradicional de revisión independiente para mejorar. En lo referente al plazo máximo, dos años no me parece mal. Sí conviene planificar a conciencia el momento en el que se va a afrontar esta auditoría específica. Esta decisión no es trivial.

– Una última pregunta: si un responsable de fichero de titularidad privada decide encargar la auditoría reglamentaria a profesionales externos, ¿cree que es más adecuado que en cada ocasión la contrate a compañías especializadas distintas?

– Creo que es correcto que la encargue a compañías especializadas. Se gana en independencia, actualización tecnológica, etc. Sin embargo, no tengo tan claro que el cambiar de compañía especializada cada vez aporte algo. Si trazamos un paralelismo con la auditoría financiera, las compañías no cambian de auditor todos los años, más bien, justamente, todo lo contrario. ■

Texto: **José de la Peña Muñoz**
Fotografía: **Jesús A. de Lucas**