

«La de seguridad en los sistemas de información es un área estratégica para nuestra firma»



Jesús Merino, socio director de Technology & Security Risk Services de Ernst & Young

Desde que hace tres años, Ernst & Young considerara estratégica su área Technology & Security Risk Services (TSRS), ésta ha cosechado importantes éxitos en los mercados. TSRS está dirigida en España por Jesús Merino, quien comenta en la presente entrevista algunos aspectos de la seguridad de la información, su control, auditoría y revisión, que ayudan a comprender el estilo de esta prestigiosa firma de servicios profesionales.

– ¿Cómo se entiende en Ernst & Young la seguridad de la información?

– Vista desde la óptica del área específica de Technology & Security Risk Services (TSRS), entendemos la seguridad de la información, a efectos de mercado, como un producto indispensable para cualquier compañía, principalmente de los sectores tradicionales: financiero, comunicaciones, media, energías... La consideramos, como digo, indispensable, entre otras razones porque nos hemos dado cuenta de que las empresas y sus directivos la están empezando a considerar así.

– ¿De dónde depende, en el marco de Ernst & Young, el área de Technology & Security Risk Services?

– Ernst & Young está actualmente en un proceso de globalización, como muchas otras organizaciones, y está dividida en zonas geográficas. Nosotros pertenecemos a la del oeste de Europa, en la que se encuentra Francia, España, Portugal, Bélgica, Luxemburgo y algunos países africanos de influencia francófona principalmente. La cabeza está actualmente en París. El de Francia es el departamento más grande, y después el de España. Ésta es nuestra organización a efectos funcionales. A efectos jerárquicos tenemos un presidente, directores generales..., y nos enmarcamos en el área de *Advisory*, desde donde prestamos servicios de asesoramiento a nuestros clientes. TSRS es desde hace tres años un área estratégica de Ernst & Young.

– ¿Cuántos profesionales trabajan actualmente en el área TSRS en España?

– En 2001 éramos veinticinco personas; hoy somos cuarenta, y con la idea de terminar el año con setenta y cinco, si es que somos capaces de contratar a expertos adecuados. Ya sabe: hay buenos profesionales en el mercado, pero escasos.

– A tenor de lo que dice, el negocio les va bien...

– Estamos contentos. Este año esperamos cerrar el ejercicio con un incremento en la facturación del 81% frente al ejercicio anterior.

– En el epígrafe específico de seguridad de la información, ¿que servicios ofrece Ernst & Young?

– Prácticamente todos, pero por comentar alguno más novedoso y demandado, le menciono el del análisis y la detección de intrusiones desde Internet, denominado *Attack & Penetration*. Lo damos, previo contrato, desde nuestro laboratorio en Madrid, y si es necesario en colaboración con el laboratorio central de Francia. El laboratorio está desconectado de nuestros propios sistemas, puesto que estos servicios tienen en ocasiones unas peculiares connotaciones legales con los clientes. Hay otro producto que va entrar en breve en nuestro mercado: me refiero al de los sellos *WebTrust* y *SysTrust*, de Aicpa y Cica. Hay, como sabe, muchos sellos, y algunos desprestigiados, puesto que se conceden por la simple contestación de una lista de chequeo. Ernst & Young tiene un sello propio, *Ciber Process Certification*, que unido a los de Aicpa y Cica pretende, realmente, constituirse en un signo de garantía razonable de que hay una seguridad adecuada en las transacciones que se hagan a través de Internet con ciertos sitios web. Hasta la fecha en el mundo no hay más de 60 sellos *WebTrust* y *SysTrust*, de los cuales un 50% han sido emitidos por Ernst & Young. Esa experiencia que tenemos fuera de España la queremos trasladar a nuestro país, en el que todavía este asunto es poco conocido entre empresas y personas.

No puedo dejar de mencionar otra línea de gran interés, la que alude a los planes de contingencia y de continuidad de negocio, aspecto que tras el 11-S se ha disparado en los mercados. Ernst & Young tiene en este punto una experiencia importante, ya que en TSRS de París, se encuentra el equipo de profesionales que elaboró y mantuvo el plan de contingencias del Credit Lyonnais cuando la entidad sufrió un incendio catastrófico hace

pocos años. Estos profesionales tienen una experiencia real y vivida, y no sólo en ese suceso, sino en lo que los franceses entienden por 600 misiones: desastres que han ocurrido y que han requerido su intervención.

Por supuesto ofrecemos servicios de apoyo a la auditoría interna, auditorías informáticas, desarrollo de políticas, normativas y procedimientos de seguridad, el estudio de los sistemas de información tecnológicos de empresas que van a ser compradas –aspecto que cada vez es más crítico en las operaciones de *Due Diligence*–, y la detección de fraude, epígrafe en el que podemos actuar, incluso, como peritos de parte.

– **¿Se está dejando notar en el mercado español la influencia del Reglamento de medidas de seguridad de los ficheros que contengan datos personales?**

– Estamos en una fase en la que se registra una gran demanda de auditorías del artículo 17 del Reglamento de medidas de seguridad. No obstante, todavía nos encontramos con que muchas empresas son desconocedoras de los requisitos legales en el tratamiento automatizado de datos personales, y somos nosotros muchas veces los que tenemos que informar de estos extremos a los responsables de ficheros. Puede estar dándose algún repunte de inquietud con esto de la auditoría del Reglamento, en parte generado por las compañías interesadas en informar y dar un buen servicio a nuestros clientes. La verdad es que se espera una avalancha de trabajo al respecto, y nosotros nos estamos reforzando con expertos en la materia.

– **¿Auditoría interna o externa?**

– En esta ocasión, y al ser una primera auditoría, muchas organizaciones están prefiriendo a un auditor externo. ¿Por qué? Pues por ver cómo trabajan profesionales externos, independientes y con más experiencia en el terreno auditor. En otras ocasiones, colaboramos con los auditores internos, y en unos casos el informe lo firma Ernst & Young y en otros el auditor interno de la entidad.

– **¿Qué opina del estado actual de falta de reconocimiento oficial de la actividad de auditoría informática? ¿Está usted de acuerdo en que una consultora que haya ayudado a un cliente a adaptarse al Reglamento de medidas, pueda después auditarle?**

– En Ernst & Young seguimos unas normas muy estrictas en este sentido, y las cumplimos a rajatabla: si implantamos o creamos procedimientos en una empresa, en ningún caso le hacemos la auditoría.

Hace un año y medio, hicimos en Ernst & Young una consulta a nuestro departamento de Risk Management, y llegamos a la conclusión de que consultoría y auditoría informática no son compatibles. Y no porque haya alguna norma que así lo indique, puesto que como bien dice, la auditoría informática no está regulada. Pero, ¿qué ocurriría si aparece un problema en este sentido? Pues que se acudiría a la legislación más análoga, que sería probablemente la de auditoría de cuentas, en la que se prohíbe que la misma persona ejecute la contabilidad y luego la audite.

No obstante lo dicho, creo que la razón más poderosa para no hacer esto es que te creas un problema de independencia complejo del que después resulta casi imposible salir. Nosotros tenemos clientes a quienes les habíamos realizado algún trabajo de desarrollo de procedimientos, y al pedirnos que les auditáramos, les contestamos que no podíamos ofrecerles este servicio por razones obvias.

– **¿Qué proyectos de seguridad y control en los que han participado en los últimos meses le parecen**

más interesantes?

– Lo más apasionante por novedoso en nuestros clientes ha sido el servicio de *Attack & Penetration*. Varios proyectos que hemos realizado en ese sentido muestran unos resultados espectaculares. El informático, que conoce los datos y sus sistemas, y los riesgos a los que están sometidos, se asombra de nuestros resultados, pero menos que un director general o un consejero, a quienes haces un *mapping* de su sistema de información y le presentas un gráfico en el cual, sin conocer nada de su informática, salvo una dirección IP (que es pública), aparecen servidores, cortafuegos, elementos de red y de sistemas vulnerables... La primera reacción es preguntar quién desde dentro ha facilitado la información. Inmediatamente se dan cuenta de lo vulnerables que son sus sistemas, de lo mal protegidos que están, y de que existen elementos y controles que pueden implantarse para 'securizarlos' debidamente.



«La dirección en las empresas está sensibilizada en lo que a seguridad se refiere; sin embargo, no concuerda dicha sensibilización con las medidas que después se ponen».

El siguiente paso de nuestro trabajo es explotar esas vulnerabilidades teóricas encontradas con herramientas y profesionales para alcanzar mayor exactitud y profundidad en nuestro análisis. Los mayores usuarios de este servicio provienen del sector financiero. Hay otra línea de trabajo, ya mencionada y menos espectacular que la anterior, que es la de apoyo al trabajo de los auditores internos informáticos.

– **¿Han realizado trabajos de desarrollo e implantación de controles de seguridad?**

– Implantamos controles de seguridad, y revisamos y asesoramos, pero siempre a clientes que no auditamos. En las labores de implantación, siempre hay determinado nivel en el que la propia empresa es quien conoce el detalle de ese control a implantar, y el último toque lo pone el cliente.

– **¿Ha venido la seguridad TIC para quedarse, o es un fenómeno pasajero?**

– Ha venido para quedarse. Si me lo pregunta por

España, le diré que el concepto de seguridad informática ya ha prendido, ya está instaurado. A ello ha contribuido notablemente la legislación sobre tratamiento automatizado de datos personales.

– **¿Valoran ustedes la certificación Cisa?**

– Mucho. Para ser gerente de Ernst & Young hay que ser Cisa. Nos parece que tiene un valor importante: obtenerlo no es fácil y mantenerlo requiere una formación continuada; además, estar en posesión de este certificado te permite conocer los sistemas informáticos hasta un cierto nivel, así como los métodos de enfoques de proyectos y metodologías de revisión.

– **¿Qué va primero, la confidencialidad, la integridad o la disponibilidad?**

– Depende del escenario, aunque hoy en día está de moda la confidencialidad entre los ciudadanos. En el mundo empresarial, creo que gana enteros la disponibilidad, y muy de cerca, la integridad.

– **Antes comentaba que la seguridad ya ha prendido en España. Sin embargo, quizá todavía no se esté invirtiendo lo suficiente...**

– La dirección de las empresas está sensibilizada en lo que a seguridad se refiere; sin embargo, no concuerda dicha sensibilización con las medidas que después se ponen.

– **¿Por qué, por complejidad, por precio...?**

– El tema económico, que duda cabe, es determinante. Y no porque la seguridad sea cara, sino porque el retorno de la inversión es cero. Las empresas se preguntan qué ganan con invertir determinados millones en seguridad. Y en muchos casos la respuesta se centra sólo en la tranquilidad del gerente en estar bien protegido. Pero ya no sólo es cuestión de que el gestor esté tranquilo, sino que detrás de la empresa están los accionistas, empleados, proveedores, acreedores, etc., que exigen esa confianza para mantener su apoyo.

– **¿Sigue Ernst & Young realizando la encuesta global de seguridad informática?**

– Acabamos de elaborar la última, que será publicada en junio de este año. La hemos realizado a los directores de sistemas de información de 500 empresas de 17 países.

– **¿Podría adelantar algunas conclusiones, siquiera generales?**

– Las principales conclusiones son que en caso de ataque a sus sistemas, sólo el 40% de los encuestados piensa que lo detectaría. Otro dato relevante es que el 40% de las organizaciones no investigan los incidentes de seguridad. En lo referente a los planes de contingencia y de continuidad de negocio, que tan de moda se están poniendo, tan sólo el 53% de las organizaciones encuestadas declara tener un plan de continuidad de negocio, entendiendo por el mismo un plan de emplazamiento alternativo y procedimientos, completo, probado y mantenido, que abarque las áreas críticas de negocio.

También podemos decir que sólo el 50% de las organizaciones tienen programas de entrenamiento en seguridad, y programas de concienciación sobre seguridad. Uno de los servicios que ofrece Ernst & Young es la realización de planes de concienciación de usuarios, que son algo así como campañas publicitarias internas para divulgar y dar a conocer a los empleados de una entidad las normas y procedimientos de seguridad de aplicación en dicha entidad. Que lo realicen expertos externos parece que da más credibilidad. En otros países se hace mucho, pero en España casi le diría que hay que considerarlo como un producto de lujo. ■

Texto: José de la Peña Muñoz

Fotografía: Jesús A. De Lucas