


**FORO FAST DE DINTEL**

# Indicadores y Métricas de Seguridad. Gestión de la Continuidad del Negocio

EL PASADO DÍA 9 DE ABRIL TUVO LUGAR LA SESIÓN INAUGURAL DEL FORO FAST DEL AÑO 2008. LA SESIÓN CONTÓ CON GMV, NCS, SOPHOS Y STERIA COMO PATROCINADORES Y CON IBM COMO COLABORADOR DEL EVENTO

TEXTO: **Carlos Useros**

La primera sesión técnica del día, dedicada a Indicadores y Métricas de Seguridad, comenzó con la introducción de **D. Gianluca D'Antonio**, Presidente de ISMS Forum, quien expuso una breve disertación a todos los presentes de lo que es ISMS Forum.

Seguidamente inició su exposición **D. Alejandro Corletti**, realizando su presentación acerca de tendencias y perspectivas en España de la ISO-27001. Explicó que la Norma tiene sus orígenes en los años 90 en el BS-7799, y que ha pasado por un proceso de modificaciones hasta la situación actual (Familia 27000). La Norma marca un antes y un después en la Industria ya que la Seguridad deja de ser sólo una cuestión técnica e implica a todos los niveles de la organización.

Además, Introduce el Análisis de Riesgo y el SGSI, sin dejar nada librado al azar. Esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es: "Organizar la seguridad de la información". Además, propone secuencias de acciones tendentes al establecimiento, la implementación, la operación, la monitorización, la revisión, el mantenimiento y la mejora de un Sistema de Gestión de la Seguridad de la Información. Los detalles que conforman el cuerpo de esta norma se podrían agrupar en tres grandes líneas: Análisis de riesgo (puede ser desarrollado con cualquier tipo de metodología, ya sea pública o particular, siempre y cuando sea completa y metódica), SGSI (en el punto cuatro de la norma, se establecen

los conceptos rectores del SGSI) y Controles (que son enumerados en el Anexo A de la Norma).

Europa se encuentra en una necesidad de demostrar, garantizar y justificar su "Calidad". Con respecto a España, no hay pautas claras que le sitúen como un País confiable para intercambiar información "On Line", para abrir y compartir bases de datos privadas y públicas, para confiar el bien más preciado, para comunicarse de forma segura, etc. En seguridad, internacionalmente no demostramos ninguna preocupación. Esto tal vez pueda no ser significativo para ciertos nichos de mercado pero cualquier empresa que trabaje con información confidencial, privada, crítica, que tenga alta dependencia de la disponibilidad de sus datos, de I+D, etc., ya no puede dejar pasar más tiempo.

**PATROCINADORES**

**SOPHOS**

**COLABORADOR**




Mesa presidencial de la primera sesión técnica de la jornada. De izquierda a derecha: D. Eduardo Martín, Business Developer de Steria; D. Gianluca D'Antonio, Presidente de ISMS Forum; D. Jesús Rivero, Presidente de DINTEL y Editor de *a+*; D. Alejandro Corletti, Director de la División de Seguridad de NCS; y, D. Ricardo Cañizares, Director de *a+*

El segundo de los ponentes, **D. Eduardo Martín Calleja** realizó su exposición acerca de los retos de una gestión corporativa de los riesgos de la información. Se trata de una de las áreas críticas de un ERM (Enterprise Risk Management), donde las TIC constituyen la infraestructura vital de la empresa moderna y donde se ha realizado una toma de conciencia creciente de los riesgos de las TIC y las potenciales pérdidas para el negocio que puede acarrear un fallo. Además, la empresa debe afrontar un cambio cultural en la gestión de los riesgos asociados a las TI, adoptando decisiones sobre los riesgos residuales basándose en criterios de negocio. El marco CobiT de objetivos de control de las TI, y la familia de estándares ISO 27000 proporcionan una base sólida para adoptar un enfoque de los riesgos de las TI consistente con una gestión de riesgos integrada a nivel corporativo.

Sobre cómo implantar una gestión de riesgos de la información, comentó que se debe adoptar un marco ERM, COBIT, y la ISO 2700x como referencias, y seleccionar una metodología de análisis de riesgos de la información que se adapte al marco global de gestión de riesgos de la empresa, adaptando la metodología al modelo de gestión de riesgos global. Además, se deben aprovechar las oportunidades que brindan los nuevos proyectos, implantación de soluciones ERP, etc., donde cada nuevo despliegue debe ir acompañado de una evaluación de los riesgos.

En la segunda sesión técnica del día, presidida por **D. Jesús Milán**, Director del Departamento de Seguridad Informática de Bankinter, y dedicada a la Gestión de la Continuidad de Negocio, **D. Martín Carvallo** comenzó con su exposición acerca de la necesidad del control como parte integrante de la

seguridad. Comentó que hoy en día los riesgos siguen aumentando, pero siempre el terminal de trabajo es el punto débil de la seguridad. Como consecuencia de esto se multiplican las soluciones para intentar mitigar dicha debilidad, lo que genera mayores costes de adquisición y de administración, conflictos entre diferentes soluciones, protección no sincronizada y rigidez en la arquitectura. Por lo tanto, a nivel de seguridad, podemos decir que se ha pasado de una protección reactiva (basada en firmas) a una protección proactiva (HIPS, análisis de comportamiento), y cada vez más vamos hacia una protección preventiva (englobando seguridad, conformidad y control).

Por tanto, la meta es la integración para simplificar la administración; dar más control y más medios para agilizar la administración de las soluciones. Además se debe controlar la versatilidad de las soluciones y el impacto sobre los sistemas, controlar las aplicaciones (bloquear el uso de aplicaciones no autorizadas, reducir los riesgos de seguridad y aumentar la productividad de los empleados). Por último, se debe mantener siempre un acceso sencillo e inmediato a la información y las políticas.

**Nathalie Dahan**, por su parte, centró su exposición alrededor de la externalización de los servicios de seguridad. Comentó que, la



Instantánea de parte de los asistentes a la Sesión Inaugural del Foro FAST



Mesa presidencial de la segunda sesión técnica de la jornada. De izquierda a derecha: D. Martín Carvallo, Responsable de Sophos Iberia para el Sur de Europa; D<sup>a</sup>. Nathalie Dahan, Responsable de Desarrollo de Negocio de Seguridad de GMV; D. Jesús Millán, Director del Departamento de Seguridad Informática de Bankinter; D. Jesús Rivero, Presidente de DINTEL y Editor de *a+*; D. Yago Cid, Consultor de Servicios de Continuidad de Negocio de IBM Global Technology Services; y, D. Ricardo Cañizares, Director de *a+*

externalización se debe realizar debido a varios factores, que son: factores financieros y contables (reducir costes, eliminar elementos del coste fijo transformándolos en variables y reducir la inversión para transformarla en gasto y dejar así la inversión para activos más críticos). Además, al externalizar se busca incrementar la eficiencia en procesos "no de negocio" aunque con repercusión en el servicio, disponer de conocimiento experto sin necesidad de desarrollarlo (conocimiento de mercado), exigir responsabilidades y garantizar la resolución de incidentes.

Explicó que, de las razones del éxito en un proceso de externalización, se pueden destacar dos que son la selección del proveedor, el cual debe ser

flexible, global en cuanto a servicios de seguridad y seguidor de un conjunto de buenas prácticas. Otra clave del éxito de un proceso de externalización es el contrato de servicio, el cual debe ser una herramienta para conseguir un buen servicio y no un freno ni una vía de continua amenaza.

Como conclusión, explicó que el proceso de externalización tiene ventajas pero también ciertos riesgos que deben conocerse para tratarse desde el principio.

Finalmente, **D. Yago Cid**, cerró la segunda sesión técnica de la mañana con su ponencia acerca de la gestión de la continuidad de negocio. Actualmente las entidades del mercado español, están actuando en la siguiente línea de

trabajo: gestionar la continuidad de negocio para garantizar la disponibilidad del servicio. Sí es cierto que en líneas generales, el nivel de gestión del proceso de continuidad de negocio detectado en las entidades del mercado español está por debajo de las mejores prácticas sectoriales. La situación ideal de la Continuidad de Negocio es seguir un **ciclo de vida activo**, alcanzando un nivel constante de disponibilidad, acorde con los requerimientos del negocio y su estrategia corporativa. Explicó que IBM, desde hace más de 25 años, aplica el ciclo de continuidad de negocio en los clientes por medio de soluciones de respaldo o servicios de consultoría, que dimensionan y analizan dichas soluciones. ♦

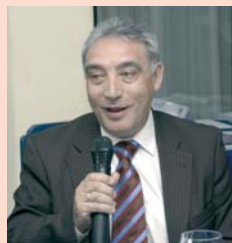
## INTERVINENTES



**D. Jesús Gómez Ruedas**  
Responsable de Seguridad del CCEA – MINISTERIO DE DEFENSA



**D. Ricardo Sanfeliz**  
Director de GETRONICS



**D. Tomás Arroyo**  
Gerente de Consultoría de Seguridad de la Información de NOVOTEC



**D. Pedro Pablo López Bernal**  
Gerente de Infraestructura de Seguridad de CAJA RURAL



## Conclusiones

TEXTO: **Ricardo Cañizares**

Durante el primer Foro FAST de este año 2008, se han debatido temas de gran interés para el sector de la seguridad: Indicadores y Métricas de Seguridad, los Sistemas de Gestión de la Seguridad de la Información y la Gestión de la Continuidad del Negocio. Los ponentes nos transmitieron su visión sobre dichos temas y se produjo un interesante debate en el que participaron activamente los asistentes. Las principales conclusiones que se pueden extraer de este primer Foro FAST son las que a continuación expondré.

La importancia de las métricas e indicadores de seguridad, cada vez es mayor, pero no tenemos que confundir ni mezclar las métricas y los indicadores, cada uno de ellos tienen unas características y objetivos diferentes. Como ejemplo de indicadores, citaremos: la capacidad de traducir los resultados al lenguaje del negocio y la capacidad de abstraer resultados ejecutivos.

La norma ISO-27001 va a suponer un antes y un después en el desarrollo de la Industria de la Seguridad de la Información en España, el apoyo que está recibiendo de las AA.PP. y la apuesta que está realizando por la misma el sector privado son factores determinantes. Disponer de un SGSI certificado es un valor competitivo, además no podemos olvidar que, las certificaciones son muy importantes a la hora de garantizar los cumplimientos legales.

La gestión de riesgos de la información debe contemplarse dentro de la gestión del riesgo empresarial. Nos encontramos en el momento de un cambio de paradigma en la gestión de riesgos, debemos gestionar el riesgo de una forma global con una estrategia global y un sistema de indicadores comunes.



Instantánea durante el almuerzo del Foro FAST

El “control” es una parte muy importante de la seguridad; es necesario evolucionar de la protección activa, pasando por la proactiva hasta llegar al control preventivo. Es necesario disponer de “Control” de lo que hace cada una de las aplicaciones de nuestros sistemas. Para ello es necesaria la integración en un único “agente” todas las soluciones de seguridad.

La Continuidad del Negocio es un tema importante al que no se le presta la atención adecuada en el día a día. Para garantizar la Continuidad del Negocio, hay que construir un proceso, gestionarlo y darle continuidad, en definitiva es necesaria una Gestión de la Continuidad del Negocio, que garantice la existencia de un ciclo de vida activo de los planes de continuidad.

La externalización es una decisión estratégica, independientemente del tipo y objetivo de la externalización. Si estamos hablando de externalizar la seguridad, al final lo que se busca es garantizar la Continuidad del Negocio en la Organización. Existen riesgos asociados a la externalización, pero es necesario y posible gestionarlos adecuadamente. La principal clave del éxito de un proceso de externalización es la existencia de un contrato de servicio completo y claro, que no deje nada al azar y que defina claramente los servicios que contempla la externalización.