# Conclusiones de la XVII Jornada Internacional de Seguridad de la Información de ISMS Forum Spain

La **XVII Jornada Internacional de Seguridad de la Información: "Blurring Privacy and Security Boundaries: A Few Market Shaking Ideas",** se celebró el pasado **MIÉRCOLES 20 DE MAYO DE 2015 EN MADRID**, en la Cineteca de El Matadero (Plaza de Legazpi, 8, 28045, Madrid).

A la decimoséptima edición titulada "**Blurring Privacy and Security Boundaries: A Few Market Shaking Ideas"**, que tuvo lugar el miércoles 20 de mayo de 2015 en la Cineteca de El Matadero de Madrid, **acudieron 325 profesionales del Sector** que pudieron conocer de primera mano las últimas novedades de la industria de la ciberseguridad, además de informarse y conocer a importantes expertos nacionales e internacionales de seguridad de la información.

En su discurso de bienvenida, **Gianluca D'Antonio, presidente de ISMS Forum Spain**, anunció los temas a tratar en esta edición, en la que pudimos examinar el mercado de la ciberseguridad y ahondar en los problemas y soluciones que se pueden ofrecer, así como las tendencias y los trabajos que actualmente se están realizando. También **se incidió en la consumerización de las nuevas tecnologías de la información**, las consecuencias legales de un ciberataque y **el papel de los gobiernos a la hora de incentivar la ciberseguridad en las empresas.**

"**Confianza y seguridad sabemos que van asociadas, por eso hay que conocer el entorno y apostar por la movilidad y el Internet de las cosas".** Así presentó **Francisco Lázaro**, CISO de Renfe, el **Centro de Estudios en Movilidad**, una iniciativa pionera de ISMS Forum Spain. Le acompañó **David Alonso**, director de 'business to business' de Samsung, y ambos desgranaron los objetivos de este Centro dirigido a profesionales de la seguridad, expertos legales, C-level, ingenieros y tecnólogos, usuarios e inmigrantes y nativos digitales. Por su parte, David Alonso

nos recordó **que existe una preocupación especial por los dispositivos que pasan del mercado de consumo al uso empresarial**, ya que en estos entornos se pueden plantear múltiples agujeros de seguridad, del mismo modo insistió en la firme apuesta de su compañía por dotar a sus dispositivos móviles de seguridad.

La ponencia que abría la sesión era casualmente las más esperada por el público y los fuertes aplausos del final indicaron que no defraudó. **Richard Bach**, subdirector de ciberseguridad del Ministerio de Negocios, Innovación y Capacitación Empresarial del Reino Unido, nos contó sin tapujos **la labor de su país para ayudar al sector de la ciberseguridad**. Dijo que es un elemento facilitador del crecimiento económico y que requiere un fuerte nivel de trabajo y compromiso. Asimismo, enumeró los objetivos de la ciberseguridad: **"lucha contra el cibercrimen y el ciberdelito, refuerzo de fronteras, investigación y desarrollo".**

También sacó a relucir que para vigilar y controlar el cibercrimen es fundamental un **partenariado público-privado en el que el diálogo y la participación sean la pieza fundamental en las labores de seguridad** que se llevan a cabo en el ciberespacio a la hora de frenar las amenazas cibernéticas. Esto facilitará que las empresas tengan más recursos para hacer frente a las amenazas existentes.

Richard Bach afirmó que el mayor reto es ponernos todos de acuerdo y que todas las estrategias y prevenciones se deben incorporar a los productos que ofrecen las empresas. **No sólo es suficiente con que los gobiernos inyecten dinero, sino que deben colaborar conjuntamente con la industria de la ciberseguridad para combatir los ciberdelitos** y a la vez trabajar para innovar, buscando un desarrollo, una estabilidad y un liderazgo de la industria.

Otro aspecto destacable de su intervención fueron las importantes iniciativas que fue apuntando para la defensa y el fortalecimiento de la ciberseguridad: **actividades de formación, cursos en línea abierta (MOOC) para educar a los universitarios y un Servicio Cibernético de Respuestas a Incidentes (CIRS)** para hacer del Reino Unido uno de los países más resistentes frente a los peligrosos ciberataques.

Para finalizar su discurso nos indicó la necesidad de **buscar un denominador común entre privacidad y seguridad**, lograr una visión global eliminando las fronteras y buscar una fusión, **empezando por utilizar un mismo vocabulario en el contexto cibernético**. Se despidió del

auditorio con una afirmación ilusionante: **"Estamos listos para los cambios que están a punto de llegar".**

La primera mesa redonda, **"*The End of the Security Perimeter: Mobility, Interoperability and Other Challenges*",** fue moderada por **Raffaele Di Giovanni-Bezzi,** responsable de la DG Connect de la Comisión Europea, que comenzó diciendo que en el ámbito de la ciberseguridad no es posible reducir el riesgo al cien por cien, pero que sí podemos mitigar las consecuencias de las amenazas cibernéticas, a la par que destacó **la necesidad de apostar por el I+D para dar mayor impulso a la industria.**

Los integrantes de esta mesa fueron **James Kretchmar**, Chief Technology Officer EMEA de Akamai, quien aseguró que hay una clara tendencia a que los ciberataques se alarguen en el tiempo, y nos habló del peligro de **los ataques DDoS (Denegación de Servicio Distribuido) que son más sofisticados gracias a que utilizan el protocolo SSDP (Simple Service Discovery Protocol).** Subrayó también que las bases de datos, donde se guardan informaciones muy valiosas, son muy vulnerables a los ataques a través de la inyección directa de comandos SQL. **Laurent Heslault**, Chief Security Strategist de Symantec, indicó que lo importante es **tener indicadores que nos permitan prevenir el riesgo, detectarlo a tiempo y saber controlarlo.**

Por su parte, **David Francis**, UK Chief Security Officer de Huawei, agregó que es esencial educar a la opinión pública para que conozca la regularización y las normas existentes en cuanto a seguridad y privacidad y resaltó que es básico **tener primero el control y la seguridad sobre la tecnología y los productos antes de que salgan al mercado y no después** de que ya estén en manos del consumidor. **Ram Motipally**, Senior Director and Global Knox Business Team de Samsung, manifestó la creciente tendencia hacia la consumerización, con este panorama dijo que lo ideal es **buscar un equilibrio entre seguridad y privacidad**, un reto complejo por la conectividad universal existente hoy en día.

Al mismo tiempo que esta atrayente mesa, se celebró un taller práctico donde se detalló en qué consiste el **malware CryptoLocker**. **Almudena Alcaide**, responsable de CyberSOC Academy de Deloitte, y **Pedro Marco**, Presales Manager de Kaspersky, nos pusieron un gran ejemplo práctico para comprender mejor este malicioso software.

El segundo panel de expertos, **"*Crisis Management: Defence, Resilience and Effective Communication*",** estuvo dirigido por **Marcos Gómez,** subdirector del Instituto Nacional de

Ciberseguridad (INCIBE), y en él se trataron temas como los conflictos que lleva asociados el sector de la ciberseguridad y la manera de gestionarlos ante una situación de crisis.

**Vicente Pastor**, jefe de Servicios de Seguridad Empresariales Capacidad de Respuesta a Incidentes de Seguridad Informática de la OTAN, nos desveló las iniciativas que su organización tiene en marcha, como son la **Incubadora de Seguridad Cibernética** y el **proyecto Smart Defence**. **Eutimio Fernández**, Security Account Manager de Cisco, defendió que hay que **tener sí o sí una respuesta efectiva en caso de incidentes**, saber reaccionar ante ellos y gestionarlos de un modo correcto para erradicar todo el malware y posteriormente reestablecer los servicios y aprender de los resultados. **Richard Curran**, Security Officer EMEA de Intel Security, se refirió al **Ley de Moore, al año 2025 y la Cloud Revolution** para situarnos en un escenario y en un tiempo donde habrá mayores oportunidades de negocio y una transformación de las ciudades inteligentes, y anunció que para enfrentarnos a todos estos avances con seguridad deberemos apoyarnos en la **Privacy by Design**. **"La seguridad estará en cada pieza de silicio"**, concluyó Richard Curran. El último integrante, **Fernando Picatoste**, Partner de Deloitte, habló sobre la importancia de contar con un equipo multidisciplinar para afrontar las crisis y que exista una comunicación efectiva para que el **CISO reciba la información necesaria y pueda actuar en consecuencia.**

Paralelamente a esta segunda mesa se impartió otra en la sala contigua, **Noemí Brito**, Miembro del Data Privacy Institute, encabezó la mesa en la que se conversó sobre ***"Los límites de la privacidad ante la gestión de crisis y la investigación de incidentes".*** Estuvieron presentes **Óscar de la Cruz**, Comandante Jefe del Grupo de Delitos Telemáticos de la Guardia Civil, **Joan Camps**, Director de la Unidad Tecnológica del Consejo General de Colegios de Médicos y **Roberto Baratta**, Director of Prevention, Business Continuity and Security de Abanca, los cuales promovieron un debate fructífero y provechoso para los asistentes.

En el tercer encuentro de expertos, ***"Under Constant Attack: Trends and Solutions",*** se departió sobre las **amenazas cibernéticas a las que constantemente estamos sometidos.** Presidió la reunión la **Dr. Nicole van der Meulen,** analista del equipo de Seguridad y Defensa de RAND Europe, que insistió en la **armonización de todos los actores, organizaciones y empresas** para conseguir una madurez de la industria de la ciberseguridad. **Johan Arts**, Director of Security Systems Europe de IBM, enfocó su charla sobre el **reto de la integración para desarrollar estrategias de seguridad integrales** y reclamó que el CISO y los miembros de la junta directiva deben entenderse para colaborar de forma conjunta. **Neil Thacker**, Information Security &

Strategy Officer EMEA de Websense, dijo que hay que **aplicar medidas efectivas** para evitar que las empresas se vean atacadas y comprometidas, y añadió que hay que utilizar más la métrica para educar a los empleados en la seguridad de la información. **Simon Young**, VP Strategic Alliances & Partnerships Europe de Trend Micro, no tiene duda de que hace falta que la **capa de defensa sea cada vez más moderna, más actual y más sofisticada para batallar con los importantes ataques que sufre la ciberseguridad**. **Richard McCluney**, Senior Vice President of Business Operations de Blue Coat, abogó por un **enfoque híbrido** prestando atención a las alertas y buscando respuestas para hacer frente a las amenazas.

La última mesa, ***"Security Analytics and Incidents Investigation"*,** estuvo moderada por **Jan Ellermann**, Senior Specialist Europol Data Protection Office de Europol. Abrió el debate **Jaap-Henk Hoepman**, Scientific Director, Privacy & Identity Lab de Radboud University, quien rápidamente nos relató como la **Privacy by Design puede ayudar a los indicadores de la organización** a tratar la privacidad de una manera responsable y comprometida. **Francesco Vitali**, Communication and Media Officer de Italian Data Protection Authority, nos dijo que hay que **pensar en la seguridad y la privacidad no sólo en términos legales sino también políticos, como las claves que conforman las relaciones internacionales de los países** y nos informó de la gran cantidad de recursos que los gobiernos dedican al espionaje. **Anas Hadidi**, Solution Architect Enterprise Products EMEA de HP Enterprise Security Products, **demandó proactividad**, diciendo que debemos adelantarnos y protegernos antes de que nuestro entorno se vea comprometido. **Darren Gale**, EMEA Lead, Network and Endpoint Forensics and Mandiant Consulting Services de FireEye, nos dio la llave para cuando se analizan y consumen datos de forma masiva, dijo que **un buen control y solución de los incidentes pasa por dar valor a la calidad frente a la cantidad**, esto nos permitirá ser más seguros y eficaces y que no pasen meses antes de que pueda ser detectada una amenaza.

**Miguel Portillo**, Associate Director de Michael Page Executive Search, cerró la mañana en la Cineteca de El Matadero de Madrid con una presentación sobre las oportunidades que nos ofrece el mercado laboral, puso ejemplos, desmenuzó el escenario en el que estamos inmersos e hizo una clara **apuesta por el talento y por la mezcla de generaciones para trabajar juntos, no sólo en la industria de la ciberseguridad, sino en todos los terrenos profesionales**.

Tras el almuerzo se llevó a cabo un **Role Play**, en el cual se simuló una situación real de crisis que venía dada por un ciberataque, dirigió el acto **Patricia Morales**, Trainer & Motivational speaker de The Box Innovation, el papel lo interpretaron **Antonio Fontiveros**, responsable de Seguridad

Tecnológica de Abertis Autopistas y **Rodrigo Jiménez del Val**, Security Advisor de Necsia. Las conclusiones sacadas de esta representación las apuntaron los propios asistentes; algunos señalaron como básicas la **comunicación** y la **calma**, otros comentaron que **no hay que quedarse aislado** y que se debe **responder de acuerdo al protocolo** para evitar males mayores y así reparar la crisis de una manera rápida y resolutiva. Pero el factor común de todas las aportaciones, apuntaba Rodrigo Jiménez, supone la **adopción de un plan de continuidad de negocio que permita prever y actuar ante cualquier situación de crisis**.

La jornada terminó con la **entrega de diplomas** de la VIII Edición del Máster en Gobierno de la Ciberseguridad de la Universidad Politécnica de Madrid y con el **sorteo de los premios** ofrecidos por los patrocinadores del evento y organizado por ISMS Forum Spain.

**Patrocinadores**


**Más información**
Departamento de comunicación de ISMS Forum Spain
**Tfno:** +34 911 861 350 / 677 684 534
**Web:** www.ismsforum.es
**Email:** comunicacion@ismsforum.es