C. Boletín del Grupo Internacional de Trabajo "Nuevas Tecnologías, Prevención y Seguro" Nº 8-2011*

I. PRESENTACIÓN

Dr. Joaquín Alarcón Fidalgo

II. INTERNET

1. Las nuevas responsabilidades electrónicas legales: disciplina y aseguramiento. Rafael Illescas

2. Ciberperiodismo, periodismo3.0, pseudoperiodismo y tráfico de información en la Web 2.1. Pepe Rodríguez

3. Internet y su efecto en la suscripción en el seguro de Automóviles. Eduardo Sánchez Delgado

4. Seguridad en redes y protección criptográfica de la información. Sergi Robles

5. Vulnerabilidades del sistema operativo y software malicioso. Sergio Castillo

6. Internet y coberturas del seguro: especial incidencia en el análisis del riesgo y en la tramitación de los siniestros. Félix Benito Osma

III. BIOTECNOLOGÍA

1. Los nuevos paradigmas en la medicina: medicina regenerativa y medicina personalizada. Josep Santaló

2. Genomas y modificaciones genéticas. Pere Puigdoménec

---

* Publicación parcial del Boletín del Grupo Internacional de Trabajo "*Nuevas tecnologías, prevención y seguro*". Depósito Legal: M-15219-93. Redactores: Joaquín Alarcón Fidalgo, Félix Benito Osma, Rosario Romero Alarcón. Enviado por el Centro de Documentación de SEAIDA.

3. Régimen jurídico de los biobancos: riesgos, responsabilidad y seguro. María José Morillas

4. Responsabilidad medioambiental y los OGMs. Teresa Rodríguez de las Heras Ballell

5. Prevención de riesgos presentes y futuros: directrices nacionales y comunitarias. Como se hace la prevención en la práctica. Manuel Pérez- Alonso

6. Genética y seguro: coberturas e incidencia en el análisis de riesgo y en la tramitación de los siniestros. Luis Almajano de Pablos

7. Implicaciones jurídicas de las pruebas genéticas y de otros datos de salud predictivos para los contratos de seguro. Carlos María Romeo-Casabona

IV. NANOTECNOLOGÍA

1. ¿Qué es la nanotecnología? ¿Cómo nos puede afectar? Jordi Pascual

2. Peligro de, y exposición a, la nanotecnología. Víctor Puntes

3. Cambios legislativos relacionados con la seguridad de los nanomateriales. Blanca Serrano

4. La gerencia de riesgos en la nanotecnología. Gonzalo Iturmendi

5. La nanotecnología y las normas: un auténtico reto. Emilio Prieto Esteban

6. El aseguramiento de los productos nanotecnológicos. Joaquín Alarcón Fidalgo

I. PRESENTACIÓN

Las nuevas tecnologías (Internet, biotecnología y nanotecnología) tienen, como áreas multidisciplinares, diversas repercusiones en todos los ramos del seguro. En la práctica se dan sorprendentes escenarios de riesgos, presentes y futuros.

Existe una cierta laguna de estudios doctrinales en nuestro país. Tampoco existe una intercomunicación entre científicos y juristas. Los primeros diciendo, desde su perspectiva, qué riesgos hay o puede haber y los segundos tratando de enmarcar esas observaciones en un marco jurídico operativo. Esta falta de comunicación origina una cierta inseguridad en los expertos del seguro a la hora de evaluar los riesgos y fijar las primas y condiciones.

El origen de las ponencias y comunicaciones tiene su base en las investigaciones que, desde hace años, viene realizando el Grupo Internacional de Trabajo *Nuevas*

Tecnologías, Prevención y Seguro de AIDA. El Grupo, a través de la Sección Española de la Asociación Internacional de Derecho de Seguros, ha organizado, con la colaboración de la Fundación MAPFRE y de diversas universidades, dos congresos, el de Madrid celebrado en 2010 y el de Barcelona, en 2011.

Las ponencias y comunicaciones del I Congreso de Madrid están recogidas en el Cuaderno 162 de la Fundación MAPFRE. La documentación del II Congreso aparecerá íntegra en el mes de enero del próximo año. Este boletín es un avance de la misma.

El II Congreso supuso, por un lado, una profundización en los temas abordados en el primero y, por otro, la aportación de novedades en el trinomio "riesgos-responsabilidad-seguro" a cargo de científicos, juristas y expertos aseguradores.

La primera mesa redonda, dedicada **Internet**, se centró en diversos escenarios:

- Los riesgos financieros (sistema de liquidación y compensación europeo), la intangibilidad y custodia del dinero recibido (riesgo de salvaguardia de los fondos del cliente) y los diversos sistemas de garantía. La ley del Juego y del Dinero electrónico fueron otros aspectos considerados.

- En la actualidad se están produciendo cambios considerables en los canales de suscripción con la introducción de Internet como nuevo canal, lo que tiene consecuencias de tipo económico para las compañías de seguros. Internet tiene un efecto inductor de compra, ofreciendo la posibilidad de poder comparar más rápidamente los precios.

- El ciberperiodismo, periodismo 3.0, pseudoperiodismo y tráfico de información en la Web 2.1, en la vertiente más clásica del periodismo *on line* y el periodismo ciudadano, el participativo, el colaborativo… que se ejerce al margen de los medios de comunicación *on line* y de las empresas de colaboración tradicionales y las prácticas pseudoperiodísticas.

- La seguridad en redes y protección criptográfica de la información y el análisis de aspectos tales como ataques distribuidos, denegación de servicio, firewalls, protección de la información e ingeniería social así como las vulnerabilidades del sistema operativo y software malicioso (spyware, virus, keyloggers, troyanos, botnets, spam, phishing) lleva a la conclusión de que no existe una solución definitiva para la seguridad de una red de ordenadores, dada la complejidad de estos sistemas. Por otro lado, la industria del malware focaliza sus esfuerzos en explotar las deficiencias de seguridad como una posible vía de infección de los sistemas, siendo una tarea ardua establecer una taxonomía genérica que permita clasificar el código malicioso en base a ciertas características.

- Los riesgos asegurables no son alterados por el cambio de medio o el comportamiento de las personas derivados de la revolución tecnológica, sino que son los mismos conforme al principio de neutralidad tecnológica. Existen nuevos

seguros con coberturas específicas, y nuevas responsabilidades electrónicas para profesiones jurídico-contables, etc. a las cuales el seguro no puede permanecer ajeno.

La segunda mesa redonda, dedicada a la biotecnología-ingeniería genética, ofreció un cuadro expositivo actualizado con diversas repercusiones en el seguro:

- Los nuevos paradigmas en la medicina se fundamentan en enfoques radicalmente distintos de la medicina tradicional y están centrados en la medicina regenerativa y medicina personalizada. La regenerativa parte del principio de regenerar los tejidos y órganos dañados utilizando células pluripotentes o multipotentes capaces de ser convertidas en cualquier tipo de estirpe celular del organismo, si bien presenta varios problemas (rechazo, etc.). La medicina personalizada tiene también sus riesgos que se derivan del conocimiento exhaustivo del genoma del paciente, aplicando a partir de él un tratamiento individualizado para cada paciente en función de las características genéticas. El riesgo está en la interpretación y la comprensión de dicha información genética.

- Las modificaciones genéticas en bacterias, en animales, en las plantas presentan problemas relacionados con la seguridad, los métodos de análisis de riesgo, los de tipo medioambiental junto a la necesidad de un código de conducta. Las modificaciones genéticas en humanos (clonación) están prohibidas por ser impredecible su resultado.

- Los biobancos tienen destacada importancia en la industria biotecnológica, farmacogenética y farmacogenómica, pero dan lugar a una serie de interrogantes jurídicos que afectan a materias muy diversas como protección de datos, derechos fundamentales, etc. Regulación de los biobancos sometida a normativa internacional de diverso tipo así como a diversos tipos de contratos. Posibilidad de causar daños a las personas involucradas en la investigación o a terceros y dar lugar a responsabilidad contractual o extracontractual.

- Los riesgos de los cultivos modificados genéticamente implican el identificar los posibles escenarios de responsabilidad asociados a los cultivos transgénicos y analizar las reglas aplicables en el marco normativo vigente. Existen cuatro posibles escenarios de responsabilidad (responsabilidad medioambiental, daños a cultivos colindantes convencionales, daños al ser humano por su toxicidad y alergenicidad e infracción de derechos de patente). La aplicación de la responsabilidad ambiental tiene un alcance limitado en las diversas situaciones estudiadas.

- Existen múltiples técnicas de diagnóstico genético (citogenética, genético molecular y genético preimplantacional). De las seis mil enfermedades genéticas, unas dos mil se puedan ya diagnosticar mediante el análisis de los genes individuales. El proceso de análisis genético consta de unas 12 fases, en las cuales hay un trasiego de muestras entre laboratorio y clínica que genera diversos riesgos

debidos a errores humanos, cruzamiento de muestras, errores de interpretación, etc. No obstante, los errores pueden ser los mismos que en cualquier tipo de análisis.

- El legislador debe hacer un esfuerzo integral para que el conocimiento del genoma humano despliegue ante la ley del contrato de seguro todas sus consecuencias, pero sin detrimento de la posibilidad real y efectiva de concertar seguros personales prescindiendo del conocimiento y aplicación contractual de dicho genoma, si esa es la voluntad del asegurado.

- La libertad de las aseguradoras para utilizar la información genética predictiva en la evaluación del riesgo está siendo cada vez más puesta en duda, apoyándose en razones éticas y en los derechos fundamentales de los clientes y de terceras personas.

- Existe una problemática distinta en los centros hospitalarios y centros de investigación en el cumplimiento de las obligaciones legales tanto en la vertiente asistencial como de producción científica. Esta problemática enlaza directamente con los derechos de los titulares tanto del material biológico como de la información clínica.

La tercera mesa redonda versó sobre diversos aspectos relacionados con la nanotecnología y el seguro. Se apuntaron diversas consideraciones sobre:

- ¿Qué es la nanotecnología? ¿Cómo nos puede afectar? (repaso de las ideas básicas de la nanotecnología para saber qué es y comprender mejor cómo nos puede afectar, indicando los principales campos de aplicación y los riesgos que comportan), el peligro de la nanotecnología y exposición a la misma. Las diferentes propiedades fisicoquímicas de las nanopartículas más comunes junto con su persistencia, dispersión y distribución han sido analizadas en la última década posibilitando el inicio de la determinación de las prácticas seguras y responsables de la nanotecnología, los cambios legislativos relacionados con la seguridad de los nanomateriales; tutela de productos mediante la gestión del uso de productos nanotecnológicos a lo largo de su ciclo de vida y en cada uno de los eslabones de la cadena productiva, las implicaciones medioambientales, de salud y seguridad de la nanotecnología.

- La nanotecnología, más que una invención es un descubrimiento. Su rápido crecimiento conlleva preocupaciones sobre el potencial impacto negativo en la salud y el medioambiente. Una cuestión planteada es si la nanoforma de una sustancia implica un aumento de su toxicidad o si, por ejemplo, hay nanopartículas tóxicas formadas de materiales no tóxicos. Es preciso conocer la interacción entre nanopartículas y sistemas biológicos, siendo precisa la evaluación del ciclo completo de vida de la nanopartícula.

- Se sabe poco de las propiedades específicas de las nanopartículas lo que produce alarma social. El nanomaterial no es más peligroso que el resto de sustancias químicas, pero el problema consiste en la dificultad de identificar sus propiedades y avaluar su riesgo en el uso, faltan métodos estandarizados. Con el fin de adaptar la legislación existente a los nanomateriales la Comisión ha iniciado un proyecto RIP (REACH Implementation Proyect) para los nanomateriales, RIPON, que se desarrolla paralelo a la necesidad de una legislación específica para nano.

- La normalización internacional de las normas juega un papel crítico en cuanto a poder garantizar todo el potencial de la nanotecnología y su integración segura en la sociedad. El desarrollo normativo se centra en terminología y nomenclatura, medición y caracterización, salud, seguridad y medioambiente y especificaciones de materiales.

- La gestión de riesgos es otro escenario incompleto sobre el cual es necesario actuar.

  Necesidad de constituir comités científicos para identificar, analizar y evaluar los nanorriesgos. El difícil control de los nanomateriales choca con marcos regulatorios insuficientes, pese a la enorme producción normativa directa o indirecta.

- El sector asegurador se ve ante varios dilemas: los nanoproductos están incluidos al no estar expresamente excluidos. Algunas voces hablan de una catástrofe similar a la del amianto. El sector no dispone de las herramientas necesarias como es la experiencia siniestral o dispositivos de la gerencia de riesgos. La legislación tampoco ayuda. No existen hasta ahora estudios sistemáticos sobre eventuales efectos negativos de los nanoproductos, si bien incendio y explosión, cosméticos, nanoproductos en la construcción, en la alimentación, en los embalajes o agricultura (toxicidad de las nanopartículas de plata o de carbono) indican claramente el riesgo latente. Existencia de pólizas en USA como la "Lex-NanoiSchield"", la "Nanotech Product Liability Insurance" o bien la ofrecida por la "Calco Comercial Insurance".

Joaquín Alarcón Fidalgo
Director del Congreso. Presidente del Grupo Internacional de Trabajo
"Nuevas Tecnologías, Prevención y Seguro".

II. INTERNET

1. LAS NUEVAS RESPONSABILIDADES ELECTRÓNICAS LEGALES: DISCIPLINA Y SU ASEGURAMIENTO.

Ponente: Dr. Rafael Illescas

Presidente de la Sección Española de la Asociación Internacional de Derecho de Seguros (SEAIDA). Catedrático de Derecho Mercantil en la Universidad Carlos III de Madrid. Vocal Permanente de la Comisión General de Codificación, España (2006). Delegado de España en la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL), Viena-Nueva York, desde 1984; en ella ha sido Presidente (2008-2009), Vicepresidente, "Rapporteur" y Presidente de Grupo de Trabajo Consejero y Fundador del "European Law Institute", Viena (Austria) (2011). Miembro permanente del Comité Maritime International, Amberes (Bélgica) y de la International Academy of Commercial and Consumer Law, Pittsburg, USA. Director de "Derecho de los Negocios", La Ley.

Resumen de la intervención:

Expresó la volatilidad legislativa del último año con una enumeración de disposiciones legales nuevas hasta un número total de 66, incluida una reforma constitucional y la Ley de economía sostenible que afecta hasta 59 leyes e incorpora una Ley Orgánica, lo que supone un total de 125 leyes. Puso en evidencia los riesgos nucleares, de auditoría, del naviero y medioambiental incluso de producción alimentaria con la reciente Ley de seguridad alimentaria, que no determina ni los riesgos ni su aseguramiento. Tampoco la Ley de ciencia identifica los riesgos y el seguro.

Mostró especial atención a los riesgos financieros (sistema de liquidación y compensación europeo), la intangibilidad y custodia del dinero recibido (riesgo de salvaguardia de los fondos de los clientes) ofreciéndose con ellos sistemas de garantías de diversa índole (aval, seguro, depósito, cuenta separada). También, mencionó la Ley del juego que aunque no se refiera expresamente al seguro sí lo hace su reglamento publicado hace apenas dos días en el BOE, pero no determina la cuantía del mismo. Igualmente, la Ley de dinero electrónico recoge el seguro (art. 10) en el que el riesgo es la declaración de concurso de la entidad de servicio de pago, así como la Ley de crédito al consumo. Son seguros poco claros, que se aproximan al seguro de crédito. Se demuestra la falta de claridad en la aplicabilidad de la ley respecto a los nuevos seguros.

2. CIBERPERIODISMO, PERIODISMO 3.0, PSEUDOPERIODISMO Y TRÁFICO DE INFORMACIÓN EN LA WEB 2.1.

Ponente: Dr. Pepe Rodríguez

Doctor en Psicología por la Universidad de Barcelona. Licenciado en Publicidad y Relaciones Públicas por la Universidad Autónoma de Barcelona. Profesor de las asignaturas de "Métodos, técnicas, fuentes y organización del trabajo periodístico", "Taller de redacción de prensa" y "Periodismo de investigación" en la Facultat de Ciències de la Comunicació (Departament de Periodisme i de Ciències de la Comunicació) de la UAB. Ha ejercido como periodista profesional desde 1976 y ha publicado 25 libros.

Resumen de la intervención:

El objetivo básico de la ponencia fue describir sucintamente la situación en la que se encuentra la producción y consumo de información dentro del modelo de comunicación Web 2.0, señalar los cambios drásticos que ha supuesto para medios y periodistas la implantación de herramientas colaborativas e interactivas que convierten a los antes pasivos lectores en activos autores o coautores productores de información, y apuntar algunas de las áreas y conductas que pueden conducir a posibles vulneraciones de derechos de terceros.

El modelo predominante en la actual arquitectura de Internet es bidireccional y simétrico, la Web 2.0 se centra en el usuario –con servicios como blogs, webs colaborativas o wikis, mashups, alojamiento de vídeos y fotografías, etc.– y es un entorno de lectura-escritura interactivo en el que los usuarios crean, amplían, varían o actualizan datos y contenidos. En esta Web social cualquier ciudadano puede publicar noticias, aunque desconozca completamente los requisitos formales, profesionales, éticos y jurídicos que se precisan para ello.

Los cambios de la Web 2.0 han transformado el campo periodístico y difuminado la barrera de la profesionalización. El amateurismo de los ciudadanos metidos a *periodistas* en funciones, que conlleva una falta de compromiso con la veracidad, la ética y la diligencia para elaborar "informaciones", puede desembocar en serios problemas de vulneración de derechos personales.

La implantación del modelo Web 2.0 ha transformado radicalmente los hábitos de consumo de información y obligado a los medios de comunicación a implementar herramientas de software "colaborativas" (comentarios a las noticias, blogs, periodismo ciudadano, foros, chats, encuestas, enlaces a alojadores de video e intercambio de contenidos a través de redes sociales) y ponerlas a disposición de sus audiencias.

Esas modificaciones en la arquitectura de los medios digitales van unidas a la creación de nuevas rutinas de trabajo, al nacimiento de nuevos perfiles periodísticos aunque también pseudoperiodísticos, y comportan una progresiva dilución de la au-

toría y de la responsabilidad ante lo que se publica, al producirse interacciones muy estrechas entre los periodistas y sus lectores anónimos, que pasan a ser autores o coautores y prescriptores de un sinnúmero de informaciones. Entre las características y ventajas del ciberperiodismo que pueden llevar a vulnerar derechos de terceros, podemos destacar los siguientes aspectos:

- La escritura hipertextual puede lesionar derechos en materia de propiedad intelectual y/o relativos a la protección de datos personales.

- La digitalización de ficheros facilita la vulneración de la propiedad intelectual y la protección de datos.

- La explotación de las bases de datos de las empresas periodísticas, dando acceso universal a sus usuarios, podría afectar a derechos intelectuales e incumplir aspectos de la legislación sobre protección de datos personales.

- La sindicación de contenidos de la prensa digital (redifusión por agentes ajenos al periodismo), podría vulnerar la legislación sobre protección de datos personales.

- La interactividad propia del Web 2.0 permite que los usuarios del periodismo digital participen activamente en la producción de las noticias, pero sin ningún control ni rigor. La interacción amparada en el anonimato no solo fomenta el insulto y la ofensa sino que permite la vulneración de derechos personales (honor, intimidad, propia imagen...).

- La facilidad para captar imágenes desde los aparatos móviles ha inundado la Red de pseudorreporteros y de videos y fotografías en webs y blogs, pero también en los medios digitales, que, aunque se editen, pueden vulnerar derechos personales (honor, intimidad, propia imagen, privacidad...).

- El informar e informarse a través de la Red, conlleva almacenar en ordenadores personales bases de datos y ficheros con datos personales que incumplen casi todo el articulado sobre protección de datos.

- Los ciudadanos que practican el periodismo ciudadano o el colaborativo, publicando gratis en medios digitales, pueden vulnerar los mismos derechos que los periodistas profesionales, pero sin tener su cobertura legal ni empresarial.

- La consideración de los sitios Web, por parte de la legislación sobre protección de datos, como meros ficheros automatizados, que NO son “fuentes accesibles al público”, coloca a todos los usuarios de Internet, sin excepción, en situación de sancionables permanentes.

3. INTERNET Y SU EFECTO EN LA SUSCRIPCIÓN EN EL SEGURO DE AUTOMÓVILES.

Ponente: Dr. Eduardo Sánchez Delgado

Doctor en Ciencias del Seguro, Universidad Pontificia de Salamanca y Diplomado en Estadística. Universidad Carlos III de Madrid. Actuario de Seguros, Universidad Complutense de Madrid. Licenciado en Ciencias Económicas y Empresariales. Rama Economía General. Universidad Complutense de Madrid. En la actualidad, Director del Área Actuarial de MAPFRE Familiar (MAPFRE Automóviles, MAPFRE Seguros Generales, MAPFRE Caja Salud y MAPFRE Agropecuaria).

Resumen de la intervención:

El objetivo de esta ponencia fue indicar que los cambios en los canales de suscripción que se están produciendo en la actualidad, con la introducción de Internet como nuevo canal, tienen también consecuencias de tipo económico en las compañías que operan en los ramos afectados. Estas consecuencias no son únicas para las entidades que comercializan exclusivamente seguros por canales directos sino que afectan a todo el mercado. En este trabajo se cuantifica algunas de las consecuencias económicas que está teniendo Internet para la industria aseguradora.

Autos es lo que más se comercializa por esta vía de contratación *on line*, pero se busca la prima más barata, sin informarse del contenido; lo que origina problemas en caso de siniestro. El internauta busca accesibilidad, rapidez e intimidad. Internet ofrece la posibilidad de poder comparar más rápidamente.

Internet no se ha desarrollado de modo significativo, hasta la fecha, como canal de suscripción en nuestro país. No obstante existe un potencial importante de crecimiento basado en el comportamiento de las cohortes de edad de los tomadores de seguro.

Internet sí tiene un efecto inductor de compra que afecta a otros canales de distribución y que está afectando a una reducción del resultado técnico de las entidades aseguradoras.

Los resultados técnicos de las entidades que comercializan sus seguros a través de canales directos presentan ratios de siniestralidad más elevados y gastos de gestión ligeramente más reducidos frente a las entidades multicanal.

El valor de un cliente para una compañía de seguros de automóviles varía de forma muy sustancial si se contrata por un canal agencial o si se contrata por Internet. Dentro de la Web también el valor difiere de modo muy importante si la suscripción es a través de la Web de la entidad o a través de un agregador.

4. SEGURIDAD EN REDES Y PROTECCIÓN CRIPTOGRÁFICA DE LA INFORMACIÓN

Ponente: Dr. Sergi Robles

Doctor Ingeniero en Informática, por la Universidad Autónoma de Barcelona. Profesor Titular en la Universidad Autónoma de Barcelona, donde combina tareas de investigación y docencia en el Departamento de Ingeniería de la Información y de las Comunicaciones. Actualmente dirige el grupo de investigación SENDA (Security in Networks and Distributed Applications) de la UAB, integrado por 15 investigadores entre personal permanente y temporal. Su actividad científica incluye publicaciones en revistas de prestigio, patentes, y dirección de proyectos de investigación nacionales e internacionales. Las líneas de investigación del Doctor Robles incluyen en estos momentos el encaminamiento y seguridad en redes DTN, las aplicaciones seguras de Agentes Móviles, y la protección de sistemas distribuidos.

Resumen de la intervención:

El objetivo principal de su ponencia fue introducir los conceptos fundamentales de la seguridad en las redes de ordenadores y de la protección criptográfica de la información, aportando ejemplos para ilustrarlos, para resaltar los riesgos asociados.

Se abordaron entre otros temas, la protección de la información (documentación, información sencilla, dispositivos de almacenaje, comunicaciones). Amenazas: privacidad, autenticidad, integridad, repudio. Clave simétrica y asimétrica. Herramientas: Hay muchas (watermarking, fingerprint, TLS, S/M, IME. Responsabilidad por utilización del correo sin cifrar. Sistema pericial. Problemas: técnicas de protección criptográfica (caso Diginotar julio 2011 en Holanda respecto a la autoridad de certificación), uso de RKI que no siempre se encuentra, complejidad de los esquemas criptográficos, no agilidad del sistema de revocación de certificados. Hay herramientas pero no son del todo operativas. Redes: protocolos de comunicación (red, transporte, aplicación). Tienen vulnerabilidades congénitas (diseño) y adquiridas (implantación). Ataques: impersonación (IP, MAC, Router, DNS). Denegación de servicio (Dos, monitorización local), intrusión (fallos de configuración, vulnerabilidad del www, parametrización no controlada), correo electrónico SPAM, impersonación). Mecanismos de protección. La ingeniería social (phising, hoaxes, scareware). Soluciones: tener política de seguridad, auditorías específicas, formación, sensibilización y concienciación. La ingeniería social es el problema más grave.

Como principal conclusión se indicó que así como la protección criptográfica de la información es fácilmente alcanzable haciendo uso de una metodología estricta, no existe una solución definitiva para la seguridad de una red de ordenadores. La complejidad de estos sistemas, basados en una multitud de protocolos y de sistemas operativos, hace difícil afrontar el reto de la securización total de las redes. No obstante, haciendo uso de algunas herramientas básicas y siguiendo unas pautas de comportamiento específicas, es posible reducir la probabilidad de éxito de los atacantes.

5. VULNERABILIDADES DEL SISTEMA OPERATIVO Y SOFTWARE MALICIOSO

Ponente: Dr. Sergio Castillo

Ingeniero en Informática por la Universidad Autónoma de Barcelona (UAB). Actualmente realiza su tesis doctoral en la misma universidad en el ámbito de las redes de comunicación y la seguridad computacional, dentro del grupo de investigación SENDA (Security of Networks and Distributed Applications). Desde el año 2005, es profesor asociado de la UAB en el departamento de Ingeniería de la Información y de las Comunicaciones (dEIC), impartiendo diversas asignaturas. También ha trabajado en el ámbito empresarial como asesor y responsable de la seguridad de redes y sistemas en diferentes plataformas.

Resumen de la intervención:

La industria del malware ha focalizado sus esfuerzos en explotar las deficiencias de seguridad como una posible vía de infección de los sistemas. Asimismo, dicha industria se ha profesionalizado en los últimos tiempos al ser su motivación |principalmente| la económica. Medir el riesgo en este ámbito no resulta una tarea sencilla, ya que la infección de un sistema no depende exclusivamente de la cantidad de amenazas (atacantes) y de vulnerabilidades que le afectan, sino que existen otros factores adicionales difícilmente cuantificables como son la complejidad de explotar una vulnerabilidad, el interés y la motivación del atacante, o las contramedidas implementadas entre otros.

Del mismo modo, establecer una taxonomía genérica que permita clasificar el código malicioso en base a ciertas características se hace una tarea ardua. Cada día se hace más patente que las nuevas formas de malware exhiben comportamientos que dan lugar a que puedan clasificarse según diversas categorías. Esto pone de manifiesto la constante evolución que está sufriendo el código malicioso, y la necesidad de tener que extremar las medidas de seguridad para proteger a los sistemas de información. En este sentido, el software de detección de malware es una herramienta proactiva que debe ser combinada junto a otras estrategias, como son las buenas prácticas llevadas a cabo por los usuarios, los diseños de software basados en patrones de protección, o el uso de las armas digitales.

El software de detección de código malicioso se sustenta en dos grandes pilares para la localización de objetos dañinos. La forma más básica es la detección basada en la sintaxis del código, siendo esta estrategia un método fácilmente eludible por el código malicioso a través de técnicas de ofuscación. Por otro lado, la detección semántica se presenta como una forma de superar las deficiencias de la detección sintáctica, siendo incluso capaz de detectar malware desconocido. A pesar de la indiscutible utilidad del software de detección, es importante remarcar el hecho de que la detección perfecta no existe, tal y como ya postuló Cohen en sus trabajos

en el campo de los virus informáticos. Como consecuencia, nuestros sistemas siempre deben ser considerados como potencialmente vulnerables al malware, ya que no existe ninguna garantía plena de que las herramientas de detección contrarresten un nuevo malware, y ya que no existe la certeza de que los sistemas estén libres en su totalidad de vulnerabilidad.

6. INTERNET Y COBERTURAS DEL SEGURO: ESPECIAL INCIDENCIA EN EL ANÁLISIS DEL RIESGO Y EN LA TRAMITACIÓN DE LOS SINIESTROS

Ponente: Dr. Félix Benito Osma

Doctor en Derecho por la Universidad Carlos III de Madrid. Profesor Asociado de Derecho Mercantil en la Universidad Carlos III de Madrid. Asesor Científico de SEAIDA. Secretario General del Grupo de Trabajo Internacional AIDA "Nuevas Tecnologías, Prevención y Seguro". Secretario y miembro del Consejo de Redacción de la Revista Española de Seguros. Abogado ejerciente del Ilustre Colegio de Abogados de Madrid. Colaborador permanente en la Sección "Seguros" de la Revista de Derecho del Transporte. Miembro del Proyecto de Investigación "Avances e innovaciones biotecnológicas: aspectos jurídicos".

Resumen de la intervención:

Enumeró los datos estadísticos sobre la evolución del equipamiento TIC y el acceso a conexión de banda ancha en el año 2011 en los hogares españoles. La implantación de las TIC es toda una realidad en todos los sectores económicos, incluido el asegurador (con multiplicidad de canales, aceptación de coberturas por las entidades aseguradoras a través de su página Web u otras creadas "*ad hoc*", así como el establecimiento de canales de comunicación con la clientela, multitarificador unida a la página Web del intermediario de seguros) y en la autoridad supervisora (portal del asegurado que ofrece información a los ciudadanos sobre sus derechos, los mecanismos de defensa y el servicio de reclamaciones vía telemática). Los riesgos no son alterados por el cambio de medio o el comportamiento de las personas que supone esta revolución tecnológica. Son los mismos conforme al principio de neutralidad tecnológica, pero hay que evaluar la medida de riesgo y la probabilidad de ocurrencia. Para ello, la gestión de riesgos ha de ser administrada como un negocio dentro de la empresa, como una parte integral de la estrategia empresarial, profesional e institucional que contribuye a la satisfacción de los objetivos marcados por aquellas. Estamos, pues, en un proceso de transformación en el que todavía es pronto su evaluación. Expresó los riesgos asegurables relacionados con el uso de las TIC o del entorno electrónico clasificados en daños en las cosas o en el patrimonio, responsabilidad civil, asistencia y otros referidos a la salud, accidentes y medioambiental. Detalló los nuevos seguros con coberturas específicas: seguros de equipos informáticos, seguros de consultoría y asistencia informática, seguros de pérdidas de datos, seguro de protección de datos, seguros de redes sociales, además de las pólizas que quedan afectadas.

También, las responsabilidades electrónicas y el seguro de los administradores de las sociedades de capital por la introducción del artículo 11 bis –sede electrónica– en la Ley de sociedades de capital; que atribuye al administrador la certeza del hecho de la inserción de contenidos en la Web y de la fecha en que se hicieron. También, las responsabilidades de las profesiones jurídicas (secretario judicial, procurador, abogado y notario) en las comunicaciones y notificaciones electrónicas y la suplantación de identidad y, especialmente, la responsabilidad y el seguro de RC obligatorio del notario en la constitución telemática de las sociedades de capital tras las leyes de reforma de la Ley de sociedades de capital de 2010 y 2011 y, por otro lado, en el acceso telemático al Registro de condiciones generales de la contratación.

El sector asegurador se encuentra en pleno proceso estructural como consecuencia del entorno competitivo y sus esfuerzos van encaminados a mejorar la competitividad desde el punto de vista técnico y operativo, con la creación y lanzamiento de nuevos productos de manera ágil y eficaz. De ahí surge la necesidad de su implantación generalizada con el acceso a los nuevos canales de comunicación y de distribución.

El seguro no puede ni debe permanecer ajeno a esta revolución tecnológica. La implantación de nuevos seguros y la adaptación de las pólizas vigentes a los nuevos riesgos electrónicos generados por el desarrollo económico y social debe ser una prioridad para el sector asegurador, pues el cambio estratégico, comercial y cultural pasa ineludiblemente por el contrato de seguro. Debe servir y sirve como elemento de auxilio y complemento a este proceso de transformación en las comunicaciones, operaciones y responsabilidades electrónicas que está demandando la sociedad civil y económica.

El adelanto o su preparación vendrá determinado por el análisis y gestión de los riesgos por las propias compañías dentro de su gobierno corporativo con la participación inexcusable de las aseguradoras y de los intermediarios o asesores de seguros. Estamos, pues, ante un campo de actuación y de negocio abierto generado precisamente por la revolución técnica y tecnológica a la que estamos inmersos en el que el contrato de seguro ha de jugar un papel importante.

El sector asegurador en su sentido más amplio ha de ser la figura coadyuvante en este proceso de cambio y de desarrollo y el seguro el complemento a toda estrategia o plan integral de gestión de riesgos de la actividad necesariamente interdependiente.