IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

OMC
ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA
Consejo General de Colegios
Oficiales de Médicos de España

Curso de Experto en Ciberseguridad y Privacidad

CONCLUSIONES

Curso de Experto en
Ciberseguridad y Privacidad

CONCLUSIONES

El éxito empresarial pasa por formar a profesionales que tengan en cuenta la normativa, la tecnología y la gestión

Vivimos en un mundo globalizado, interconectado a la Red, repleto de vasos comunicantes entre la parte técnica, legal y de gestión empresarial en el que subyacen enormes ventajas pero también grandes peligros que han de tenerse en cuenta y prevenirlos para lograr generar confianza en nuestras estructuras, y, con ello, ganar la de nuestros socios y clientes, actuales y futuros, para mejorar la actividad empresarial. Son estos desafíos por los que las normativas y la concepción sobre protección de datos y ciberseguridad se están cambiando. Ahora, el reto es formar personales que sepan trabajar en este nuevo entorno.

Esta sería la principal conclusión del Curso de Experto en Ciberseguridad y Privacidad desarrollado del 28 al 30 de enero en Madrid, organizado por la IAITG y la Organización Médico Colegial (OMC). Un curso multidisciplinar (Derecho, tecnología y gestión de empresa) que ha servido para reunir a algunos de los máximos expertos del país en Ciberseguridad y Privacidad aplicadas a sus diferentes materias. Dirigido por **Antoni Bosch, director general de IAITG y director del Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC de la Universidad Autónoma de Madrid**, estas jornadas han servido para ofrecer un panorama del actual estado de la ciberseguridad y la privacidad en nuestro entorno empresarial, en las instituciones y, también en el ámbito personal.

Derecho, empresa y tecnología

La evolución del término Privacidad en el Derecho Internacional ha sido constante a lo largo de los últimos años y todavía varía de un país a otro, de hecho hay sitios donde este término no tiene una traducción directa. **Alejando Sousa Bravo, encargado de asuntos jurídicos de la Misión de México en Naciones Unidas**, mostró las diferentes acepciones que ha ido teniendo este concepto e hizo un análisis de la jurisprudencia al respecto de su aplicación. "No hay una norma común, se aplican diferentes criterios en función de lo público que sea esa persona y del ámbito (esfera privada o personal) en donde se hayan capturado esos datos o informaciones".

Eloy Velasco Núñez

"El concepto anglosajón de vivir para trabajar frente al español de trabajar para sobrevivir". Para **Eloy Velasco Núñez, magistrado del Juzgado Central de Instrucción 6 de la Audiencia Nacional**, esta diferencia en la apreciación de lo que podríamos denominar "cultura empresarial" es clave para comprender la importancia de la aplicación de Ley Orgánica 5/2010 sobre Responsabilidad Penal de las Personas Jurídicas. Una ley, casi sin jurisprudencia por su reciente promulgación (diciembre de 2010), que establece que si desde su empresa se comete alguno de los delitos tipificados por esta ley pueden imputar penalmente tanto al responsable directo del hecho como al administrador de la empresa.

Un concepto clave para comprender las reticencias que muestra la sociedad española a la hora de establecer mecanismos para vigilar la actuación interna de los empleados, sistemas de prevención que son habituales en Estados Unidos y los países anglosajones para impedir que una actuación aislada (revelación de secretos, vulnerar la intimidad, acceso sin autorización a datos o programas informáticos, dañar o alterar datos o programas informáticos, etc.) ponga en peligro la continuidad de la empresa y, por tanto, la del resto de los empleados.

Una norma que, para su correcta aplicación desde los tribunales, representa un auténtico reto para los juristas que deberán tener en cuenta la dificultad que entraña dilucidar si el acto delictivo se ha cometido por falta de control de la empresa, y que les lleva a replantearse una teoría del delito a través de la persona jurídica y las consecuencias de su correcta o incorrecta aplicación.

Una norma (la Responsabilidad Penal de las Personas Jurídicas) que, según **José Manuel Maza Martín, magistrado de la sala segunda del Tribunal Supremo**, "significa que hay que dirimir si el delito se ha cometido por

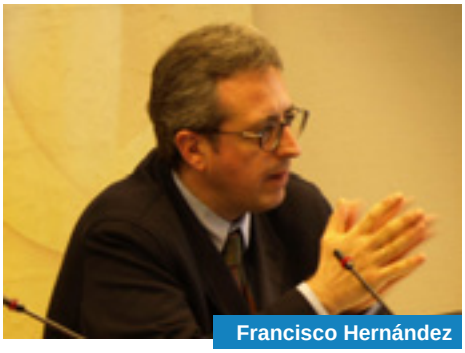
José Manuel Maza Martín

falta de control de la empresa y en el que su correcta aplicación desde los tribunales, representa un auténtico reto para los juristas que deberán tener en cuenta la dificultad que entraña dilucidar si el acto delictivo se ha cometido por falta de control de la empresa, y que les lleva a replantearse una teoría del delito a través de la persona jurídica y las consecuencias de su correcta o incorrecta aplicación".

> "La ley de enjuiciamiento criminal está totalmente desfasada en lo que respecta a la parte tecnológica"

Manuel Marchena Gómez

Según los tres jueces presentes en los cursos, la falta de normativa legislativa cuando se trata de temas en los que de alguna forma intervienen las nuevas tecnologías es evidente; lo que provoca la indefensión de los jueces de instrucción que tienen que actuar en función de su buen criterio o buscar referencias y símiles (muy lejanos) en el actual código penal. Para **Manuel Marchena Gómez, magistrado de la sala segunda del Tribunal Supremo**, "la ley de enjuiciamiento criminal está totalmente desfasada en lo que respecta a la parte tecnológica". Marchena preside actualmente la Comisión encargada por el Gobierno que está preparando un borrador de anteproyecto para, entre otras cosas, actualizarla y dar solución a buena parte de estos problemas.



Francisco Hernández

Por el lado de la Fiscalía, **Francisco Hernández, fiscal delegado del servicio de Criminalidad Informática**, también coincide en que el problema está en la aplicación del Derecho a los casos en los que interviene la informática y las nuevas tecnologías. Por ejemplo, el ciberacoso no está regulado en España, desde el punto de vista procesal no tenemos penas "informacionales" (privativas de derechos en el uso de instrumentos tecnológicos a aquellas personas que han resultado culpables de utilizarlos para realizar crímenes).

Para el fiscal Francisco Hernández, la respuesta legal contra el ciberterrorismo debe provenir de la seguridad nacional y de los ciudadanos; de la coordinación de los cuerpos de investigación militares y la policía; del intercambio de información (cumpliendo con las garantías). Desde el punto de vista procesal, hay que unificar las herramientas periciales, disponer de acceso a los medios informáticos de los sospechosos y vigilar escrupulosamente cómo se custodian las pruebas. "Somos fiscales cuánticos, tenemos que saber vivir con la incertidumbre de que lo que hemos aprendido hoy no nos servirá mañana".

Contexto político en Europa

En este contexto multidisciplinar, la intención de Bruselas es desarrollar el mercado interior, defender la Justicia, la libertad, la privacidad y favorecer la cooperación administrativa. Según **Francisco García Morán, director general de Informática de la Comisión Europea**, "para conseguirlo, la clave está en compartir información y la interoperabilidad en temas de seguridad".

La Agenda Digital Europea, aprobada en junio de 2010, surge por una falta de infraestructuras y de interoperabilidad, un aumento del cibercrimen; falta de confianza de los ciudadanos; carencia de profesionales; falta de inversión en seguridad lógica y muchas lagunas en lo de se denomina Gobierno Electrónico.

Francisco García Morán

Ante este panorama, las políticas de seguridad de la UE se basan en la prevención, la persecución del cibercrimen y del ciberterrorismo, y la protección. Los principios de la estrategia europea pasan por reforzar la seguridad (pública y privada); las acciones unificadas y coherentes

contra el cibercrimen; las propuestas legislativas; concienciar a las empresas e instituciones y apoyar en materia de seguridad a los países que lo necesiten para su transposición legal. ¿Cómo desarrollarla?: a través de sinergia, cooperación y colaboración para lograr al menos compromisos de normas de comportamiento.

Con respecto a las acciones concretas de Europa, tenemos la propuesta de Reglamento europeo para la Protección de datos, que muchos esperan su entrada en vigor para 2014, y una nueva Directiva contra el cibercrimen, más difícil de llevar a cabo próximamente y que tendría que transponerse a las distintas legislaciones de los Estados miembros.

Con el nuevo Reglamento europeo estamos ante una reforma horizontal que va a cambiar el paradigma de la protección de datos. Para **Jorge Carrera Domenech, consejero de Justicia en la Representación Permanente de España ante la UE**, "esta reforma se hacía imprescindible en aras a fortalecer el mercado único, consensuar criterios (ahora existen 27 directivas distintas), y facilitar la circulación y la protección de datos. Siempre, minimizando la utilización de datos personales y bajo el principio de respetar los derechos fundamentales de los afectados pero buscando un equilibro que no limite la competitividad, la economía y el buen funcionamiento del tejido empresarial".


Leopoldo Mallo

"La tecnología y la Privacidad van o deberían ir unidas". Según **Leopoldo Mallo, director general de Alcatraz Solutions**, "existen herramientas tecnológicas que realizan todas estas tareas de forma transparente y permiten a las empresas e instituciones cumplir con la normativa, evitar riesgos y multas, dedicándose por completo al core de sus negocios".


Rosa García Ontosa

Rosa García Ontosa, creadora y directora de la Agencia de Protección de Datos de Madrid (desaparecida el pasado 1 de enero por motivos presupuestarios), habló en concreto de la videovigilancia. "Son datos como cualquier otro de carácter personal con la circunstancia de que es obligatorio avisar de que se está recogiendo esa información". Para Rosa García, hay que buscar la proporcionalidad en función del objetivo. Y recalcó que en el nuevo Reglamento europeo se hace mención a la calidad de los datos (sólo se recogerán aquellos que necesitemos).

Especialízate en Seguridad TIC con nuestro

Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC

Más información

www.uam.es/masgdtic

info@iaitg.eu

91 389 67 91

E-Salud, historias clínicas

El curso de experto también ha revisado el estado de nuestra E-Salud. Cada vez que un ciudadano acude a su médico de cabecera, a urgencias, a un especialista de un hospital y, en general, a cualquier profesional de la salud, se le abre una historia clínica. La historia clínica es un documento válido desde el punto vista clínico y legal donde se recoge la información necesaria (asistencial, preventiva y social) para la correcta atención de los pacientes.

Son datos considerados sensibles o especialmente protegidos por la Ley (al mismo nivel que el origen racial y la vida sexual) y dependen enormemente de la confianza entre el médico y el paciente. Una confianza que debe estar apoyada por la tecnología y los conocimientos sobre la ley que permitan salvaguardar los datos contenidos en las historias clínicas.

Joan Camps Pons

"En estos momentos el sistema sanitario está diseminado y no es interoperable (a pesar de existir la tecnología que lo permitiría)". Son palabras de **Joan Camps Pons, director de Estrategia Tecnológica del Consejo General de Oficiales de Médico de España**. La clave está en asegurar un acceso seguro de los médicos a la información de los pacientes, con total trazabilidad.

Un acceso a una información muy sensible en la que participan tanto quienes pagan los servicios de Salud (administraciones públicas, autoridades de salud, aseguradoras privadas), como los que prestan esos servicios (centros de atención primaria, hospitales, farmacias, atención domiciliaria), los actores y los responsables de la custodia de la información. La clave está en buscar un modo eficiente de consumir los recursos buscando los mejores resultados".

Seguridad digital y Privacidad, negocio y comunicación

Cumplir con la normativa y establecer los medios de protección necesarios para evitar ataques internos o externos a cualquiera de los sistemas de nuestras empresas permiten evitar sanciones y obtener la confianza de los clientes y trabajadores. Por lo tanto, parece claro que hace falta formar a profesionales que tengan en cuenta estas tres patas (normativa, técnica y gestión de empresa) sobre las que gravita el futuro éxito de nuestro tejido empresarial.

Íñigo Núñez

Para **Íñigo Núñez, director general de Dagonpress y partner de la agencia EFE**, "este trabajo es básico para el negocio y la imagen de marca, evita riesgos ciertos y transciende de los departamentos técnicos o jurídicos, aportando una ventaja competitiva".

El punto de vista del estado de la ciberseguridad y la Privacidad desde el lado de la Comunicación también estuvo secundado por **Carlos Bages Riva, director asociado de All2com**. "La comunicación es poder y si no se toman medidas, habrá

riesgos en la comunicación digital". Bages habló de la infección vía comunicaciones, no mediante virus. "Las pantallas comerciales en estaciones de trenes, aeropuertos, autopistas, etc. (en España hay 40.000, en Estados Unidos un millón) son una forma de comunicación directa e intrusiva que pueden convertirse en una oportunidad para los delincuentes (saboteándolas para mostrar sus mensajes) o para la policía (como medio de prevención). Un arma de doble filo".

Siguiendo en el apartado de la Comunicación, para **José Ignacio Sanz Cerezuela, director gerente de la Agecia EFE**, "con el advenimiento de las nuevas tecnologías, la inmediatez ha desaparecido, y a los medios de comunicación sólo les queda explotar la veracidad y el rigor de sus informaciones".

De izquierda a derecha; Carlos Bages Riva, José Ignacio Sanz Cerezuela y Javier Tamayo

Según Sanz, la democratización en el acceso y la creación de la información conlleva el problema de la atomización de los medios y la falta de garantías sobre sus contenidos. "Los 'incendios digitales' (difusión de noticias no reales) tienen efectos económicos muy importantes. La oportunidad está en crear la necesidad de consumir marca y trasladar al usuario final nuestro sello de calidad". Para el director gerente de EFE, la solución puede estar en filtrar la información que entra en las compañías a través de departamentos de IT (mediante herramientas digitales e inteligentes) y/o subcontratando empresas externas que realicen esta tarea.

"Los datos personales son el medio de pago en Internet". Para **Javier Tamayo, abogado sénior de la plataforma social web y móvil Tuenti**, una red social cien por cien española, "la privacidad es un elemento esencial para el negocio digital junto con la tecnología y los usuarios. Hay que buscar un equilibro entre los derechos de los ciudadanos y el avance de la tecnología para no frenar el crecimiento empresarial". Para Tamayo, el problema está actualmente en que no existe una normativa estándar que pueda aplicarse en todo el mundo. "Nosotros abogamos por el cumplimiento de la normativa y la autorregulación".

Cloud computing y privacidad

La consolidación del cloud computing en el escenario empresarial ha propiciado la aparición de las dudas sobre la salvaguardia de los datos ubicados en la nube. Es una de las preocupaciones de la **Agencia Española de Protección de Datos, cuyo adjunto al director, Jesús Rubí Navarrete**, matiza que los usuarios que contraten esta tecnología deben tener en cuenta que siguen siendo los responsables de los datos, el tipo de cloud que

Jesús Rubí

suscriben (privada, pública, híbrida o comunitaria) y de las modalidades de servicios que se precisen y ofrezcan los proveedores para ajustarlas a las garantías jurídicas exigibles en cada caso en materia de protección de datos.

"Estamos ante un cambio de paradigma, en el que los proveedores de cloud tienen casi plena autonomía para elegir lo que ofrecen (seguridad, socios, tecnología)". Por eso hay que tener en cuenta (a la hora de contratar

De izquierda a derecha; Xavier Alamán Roldán, Pablo Pérez San-José y Aitor Cubo Contreras

este servicio) la portabilidad; los derechos ARCO (cómo los va a aplicar el proveedor cuando se le solicite); las medidas de seguridad (niveles, auditorías, cifrado, incidencias); posibilidad de realizar una auditoría externa e independiente (incluso en los niveles básicos, al estar externalizados los datos en la nube); comunicación de brechas de seguridad a clientes y responsable de los datos; un contrato que exponga claramente si tienen empresas subcontratadas para ofrecer sus servicios y las garantías vinculantes que se van a ofrecer.

TIC, globalización, interconectividad, Cloud. Por todas estas razones la normativa sobre protección de datos y seguridad están cambiando. Para **Xavier Alamán Roldán, profesor de Ciencias de la Computación e Inteligencia Artificial y director del Máster de Auditoría, Seguridad, Gobierno y Derecho de las TIC de la UAM**, "el reto es formar profesionales que sepan trabajar en este nuevo entorno".

Además de a las empresas, el cloud computing también ha llegado con fuerza a la Administración. **Aitor Cubo Contreras, subdirector general de Programas, Estudios e Impulso de la Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas**, confirma que la nube es de un interés prioritario para el Estado. "Hay que priorizar la adopción de medidas de seguridad atendiendo a la máxima de 'menos coste y mayor impacto', y utilizar infraestructuras y servicios comunes". Para Contreras, los proveedores de servicios cloud juegan un papel esencial para prevenir la brecha digital (sobre todo en los pequeños ayuntamientos).

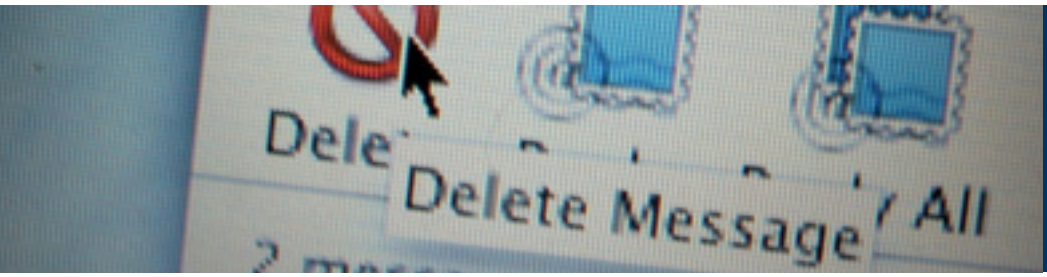
"En la Administración Pública el cloud ha llegado para quedarse", así lo confirma un estudio sobre el Cloud Computing en el sector Público, dado a conocer por **Pablo Pérez San-José, gerente de INTECO**. "Uno de cada tres organismos públicos es usuario de algún servicio cloud (sobre todo las entidades locales). Hay que tener cautela para llevar a la nube los procesos críticos. El cloud es una ventaja pero también un riesgo para la seguridad y la privacidad.

Estudios sobre seguridad y privacidad

Según un estudio de INTECO sobre el fraude a través de Internet, en los tres últimos meses el 52.9% de los internautas españoles ha sufrido un intento de "engaño digital" (petición de claves de bancos, supuestos premios, ofertas de trabajo falsas, etc.); y a pesar de ello, más del 90% sigue mostrando su confianza en la Red de redes. En muchas ocasiones no es un problema de herramientas para prevenir, sino de hábitos prudentes y buenas prácticas.

Los ataques son cada día más complejos, sofisticados y personalizados. En el último año, un 2,5% de los internautas españoles ha sido objeto de "microfraudes" (un fraude de poca cuantía, menos de 400 euros, lo que les convierte en una falta y conlleva menor sanción).

Es reseñable cómo los estudios de INTECO revelan que los menores tienen más conocimiento sobre los riesgos técnicos que sus padres; que la mayor parte de las empresas desconocen que una falta de seguridad para proteger los datos les afecta en lo que se denomina "continuidad económica" y que la mayoría no monetiza las incidencias o ni siquiera toma medias cuando surge algún problema.



Cibercrimen y "hacking ético"

Vicente Díaz, analista sénior de Seguridad en Kaspersky, expuso un estudio realizado por su compañía sobre la denominada "Campaña Octubre Rojo", un caso real de ciberespionaje que empezó (según los datos que manejan) en 2007 con la compilación de datos de multitud de personas, que en 2010 se inició con el registro de al menos 60 dominios para recopilar los datos de los espiados (embajadas, institutos gubernamentales, centros de energía, empresas aeroespaciales, etcétera), y que hoy día sigue activa sin llegar a descubrirse quién recibe toda esta información.

Vicente Díaz

Los datos compilados proceden de Europa, Oriente Medio, Brasil, Oceanía y parte de África. En España el total de afectados es del 2% del total. Utilizan métodos clásicos, con vulnerabilidades al alcance de cualquiera. Infectan ordenadores con el envío de correos con un fichero adjunto (con Asuntos como "la foto de la embajadora"). Una vez que se abre, el código malicioso se conecta a los servidores y espera instrucciones. Puede capturar lo que se teclea, contraseñas, documentos, routers, agenda de teléfonos, incluso los archivos cifrados.

¿Existe el "hacking ético"? Para **Andrés Guzmán Caballero, director de Adalid Corporation Colombia**, la respuesta es "sí".

Contó el ataque realizado contra la web oficial encargada de la difusión de resultados de las elecciones presidenciales de Colombia llevadas a cabo en 2010. La web se cayó durante muchas horas y se tuvo que recurrir a los medios convencionales (radio, prensa escrita y televisión) para informar de la evolución de las urnas.

Fue entonces cuando contactaron con ellos. Analizaron a los posibles "enemigos" (otros partidos políticos, grupos de presión internos, hackers y agentes externos internacionales), sus estrategias de ataque (utilizaban sobre todo las redes sociales) y las duplicaron. Infiltraron a varios usuarios haciéndose pasar por simpatizantes del movimiento conspirador, comenzaron a realizar ataques a webs para, finalmente, atacar (ficticiamente) la web institucional y derivar ese ataque contra los verdaderos boicoteadores. Difundieron los resultados en las redes sociales posibles para replicar los resultados por todas partes y hacer imposible su control.

Emilio Aced Félez

Mientras tanto, Europa está preparando una nueva Directiva contra el cibercrimen. Para **Emilio Aced Felez, jefe de área de la Agencia Española de Protección de Datos**, el objetivo de esta normativa es crear un marco común de garantías cuya elaboración tiene más complicaciones que la propuesta europea de Reglamento para la Privacidad, y que busca ofrecer garantías de protección de datos para que las autoridades competentes puedan luchar contra los ciberdelitos. "El objetivo es armonizar estas reglas con el objetivo de crear un ambiente de libre circulación de datos a la hora de luchar contra el cibercrimen".

Entre sus contenidos, Emilio Aced destacó el principio de disponibilidad (garantías sobre los datos que se comparten entre las distintas fuerzas y cuerpos de seguridad de los Estados); distinción de categorías de afectados (sospechoso, condenado, terceras personas involucradas, víctimas, etc.) para evitar daños al honor de las personas; exactitud y fiabilidad (datos basados en hechos se diferenciarán de los datos basados en apreciaciones personales); licitud (causas de

> "El objetivo es armonizar estas reglas con el objetivo de crear un ambiente de libre circulación de datos a la hora de luchar contra el cibercrimen"

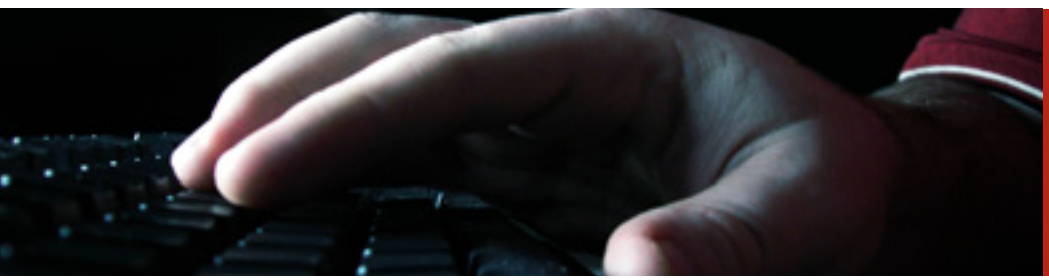
legitimización de un tratamiento de datos, prevenir una amenaza inminente y grave para la seguridad pública); datos sensibles; elaboración de perfiles (con restricciones, no podrán basarse exclusivamente en datos sensibles); derechos del interesado (los derechos fundamentales requerirán de un tratamiento individualizado y rigor en la aplicación de las excepciones); transferencias internacionales para luchar contra el crimen globalizado (instrumentos jurídicos vinculantes o acuerdos puntuales en casos concretos); autoridad de control (independiente, cualificada y en cooperativa); y documentación (como garantía de la verificación).

En representación de la defensa contra el cibercrimen en España, **José Rodríguez Fuente, inspector jefe de la Brigada de Investigación Tecnológica** (BIT), relató que la actividad de la BIT se centra en la lucha contra la pornografía infantil, el fraude por Internet y la seguridad tecnológica (Anonymous, hackers, etc.) y que algunas de las dificultades ante las que se encuentran vienen por la imposibilidad de aplicar la tecnología debido al corsé que marcan las leyes procesales. "La actuación de la Brigada está marcada en función de la proporcionalidad de los hechos y de los recursos". La finalidad de la investigación es doble: obtener las pruebas inmediatas para impedir la comisión de un delito, y obtener evidencias que puedan justificar la culpabilidad para el juicio.

El uso los dispositivos móviles, ponencia a cargo de **Fernando Fernández, inspector de la Brigada de Investigación Tecnológica**, centró también su interés en la seguridad que se aplica al mismo. Según este especialista, la mayoría no utiliza PIN y menos del 30% bloquea su pantalla. Ni que decir que la inmensa totalidad no apunta el IMEI del teléfono e hizo especial hincapié en la importancia de realizar volcados de la memoria periódicos y cuidar de dónde se realizan.

De izquierda a derecha; José Rodríguez Fuente, Fernando Fernández y Santiago Delgado

Santiago Delgado, doctor en Medicina, médico forense en excedencia y director del Tratado de Medicina Legal y Ciencias Forenses, se centró en hacer un repaso de cómo han ido evolucionando las tecnologías en su ámbito (desde los años 50 a través del diagnóstico clínico y el análisis conductual; la década de los 60 con la creación de la Unidad de Ciencias de la Conducta del FBI, y el uso de la Estadística en los noventa, donde se utilizan modelos matemáticos y software específico para la elaboración de perfiles criminales). "Los ordenadores son una extensión del criminal, de sus comportamientos. Los ordenadores son pruebas".



Ciberterrorismo

A pesar de que la prevención debería ser esencial y los sistemas críticos los más protegidos, **Antonio Ramos, Presidente de ISACA (Asociación de Auditores de Sistemas de Información)**, desveló que muchas de las infraestructuras (los sistemas de control de los flujos eléctricos, circulación, energía, transportes, etcétera) de alto riesgo (por el impacto que tendría un posible fallo en la sociedad) no tienen ni mucho menos las medidas de protección suficientes para protegerse de un ataque.

"A pesar de que son sistemas que no se pueden 'caer', están conectados a Internet con un nivel de seguridad muy bajo, preocupante, y los equipos no están siquiera actualizados, con un grado de

De izquierda a derecha desde la zona superior; Antonio Ramos, Juan Miguel Velasco, Víctor Manuel Hernández y Enrique Polanco González.

estandarización ínfimo". Según Antonio Ramos, el problema es a nivel mundial. "Donde no hay 'business' no hay interés".

Para intentar remediar esta situación existen empresas que realizan auditorías de los denominados sistemas SCADAS (sistemas de control industrial) y que permiten recopilar datos que están muy distribuidos, donde se toman muchas variables y se presentan en una interface para que, finalmente, alguien tome una decisión sobre lo que hacer al respecto. "Nosotros buscamos certificar la confidencialidad, integridad y disponibilidad de esos sistemas. Las auditorias persiguen que el riesgo sea cero, sin tocar el sistema (muy frágil) y, lo que no se pueda, probarlo en laboratorio".

> "Durante los últimos cinco años, el 80% de las empresas han sido objeto de ataques avanzados dirigidos"

El nacimiento del ciberterrorismo está íntimamente ligado a la proliferación de dispositivos digitales y las tecnologías de comunicación. En la cumbre de Davos de 2012 los ciberataques ya se habían colocado como la cuarta amenaza. La Historia reciente (desde la década de los 70) está repleta de ataques dirigidos. Para **Juan Miguel Velasco, consultor independiente en Cloud / IT Security**, "ya no hay dificultad técnica para crear ataques y distribuirlos, casi con la seguridad del anonimato total".

Según Velasco, "durante los últimos cinco años, el 80% de las empresas han sido objeto de ataques avanzados dirigidos. Muchos de ellos a grandes empresas, incluidas las tecnológicas". Destacó los ataques DDoS como una de las amenazas crecientes y más persistentes. "Un ataque que es universal, barato, eficiente, con gran impacto, reiteradamente posible y habitualmente menospreciado por sus víctimas (el riesgo frente a la inversión para prevenirlo)". También destacó que el Cloud Computing debe ser una extensión de nuestro perímetro de seguridad exterior.

Víctor Manuel Hernández, consultor independiente especializado en temas de seguridad, opina que lo importante es saber qué es lo que debemos proteger, analizar los riesgos e integrar soluciones que no interfieran con los procesos existentes".

Aplicar la inteligencia para pensar como el enemigo y mejorar así nuestra seguridad. Esta es la idea aportada por **Enrique Polanco González, coronel en la Reserva de la Inteligencia Militar y director de Global Technology 4E**. Tras definir este concepto como el proceso matemático de resolución, evaluación y análisis de información, cuya finalidad es producir conocimiento útil a alguien, Enrique Polanco destaco que la inteligencia en una empresa vale, entre otras muchas cosas, para tomar decisiones, hacer planificaciones, estudiar a la competencia. "En estos momentos si los ataques afectan a la seguridad lógica también pueden afectar a la física".

Curso de Experto en Ciberseguridad y Privacidad

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

OMC ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA

Consejo General de Colegios Oficiales de Médicos de España

Para más Información:

INSTITUTE OF AUDIT & IT-GOVERNANCE

info@iaitg.eu

91 389 67 91