DOCUMENTOS SiC
Nº 24
NOVIEMBRE 2017

11ENISE

Retos de ciberseguridad en un mundo conectado

ENISE 2017

León acoge la edición más multitudinaria

LAS CIFRAS

- 1.300 asistentes
- 136 ponentes

Álvaro Nadal

Ministro de Energía, Turismo y Agenda Digital

Apoyo a la industria

CPPP y marco europeo

Desarrollo profesional

ENTREVISTA

Alberto Hernández

Director General de INCIBE

El evento congregó a 1.300 profesionales los pasados 24 y 25 de noviembre, en León

El Ministro Álvaro Nadal clausura 11ENISE, un encuentro marcado por los retos en ciberseguridad de un mundo hiperconectado

Álvaro Nadal, Ministro de Energía, Turismo y Agenda Digital

Bajo el lema 'Retos de ciberseguridad en un mundo conectado' transcurrieron dos intensas jornadas de análisis y debate acerca de los desafíos y tendencias de la ciberseguridad. El encuentro contó además con la presencia de Álvaro Nadal, Ministro de Energía, Turismo y Agenda Digital, encargado de realizar el acto de clausura, quien afirmó que la ciberseguridad es uno de los pilares básicos del estado de derecho.

Participaron en el acto inaugural (de izquierda a derecha): Antonio Silván, Alcalde de León; Alberto Hernández, Director de INCIBE; Juan Carlos Suárez-Quiñones, Consejero de Fomento y Medio Ambiente de la Junta de Castilla y León.

Analizar el estado y los retos de la ciberseguridad en España y en el panorama internacional en un mundo hiperconectado donde la salvaguarda de la información y los datos se vuelve cada vez más crítica, tanto para organizaciones como para ciudadanos, ha sido uno de los principales objetivos de la undécima edición del **Encuentro Internacional de Seguridad de la Información (ENISE),** celebrado los pasados 24 y 25 de noviembre en la ciudad de León.

Abanderando el lema 'Retos de ciberseguridad en un mundo conectado', más de 1.300 asistentes y 136 ponentes participaron en este evento organizado por **INCIBE** en el que, como novedad, se abordaron con especial énfasis las amenazas y los retos circunscritos a la expansión del Internet de las Cosas (IoT).

En su inauguración, el acto contó con la presencia del Director General de INCIBE, **Alberto Hernández**, el Consejero de Fomento y Medio Ambiente de la **Junta de Castilla y León**, **Juan Carlos Suárez-Quiñones** y el Alcalde de León, **Antonio Silván**. Este último comenzó su intervención haciendo alusión a los más de 50.000 millones de dispositivos conectados a internet que se esperan registrar en el año 2022 y "la necesidad de profundizar en las medidas de protección ante esta realidad desde el sector de la tecnología y la ciberseguridad, con sus componentes industrial y empresarial". Silván enfatizó así mismo la importancia de un evento como ENISE para la industria, ofreciendo León como opción donde establecer nuevos proyectos.

Tras él, Hernández destacó la apuesta clara del Gobierno por impulsar el apoyo para mejorar la seguridad cibernética. Además, señaló que la "ciberseguridad y la ciberprotección de nuestras infraestructuras tecnológicas deben asumir un papel protagonista en el desarrollo de la hoja de ruta digital de nuestro país". "Así se recogerá en la Estrategia Digital para una España

Mesa redonda: Retos de la ciberseguridad en España

Camino Kavanagh, del King's College London

Gloria Placer, Directora del Gabinete de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información

Inteligente, que está elaborando la SESIAD y que busca la actualización ética de nuestra sociedad a través de un nuevo marco de innovación y convergencia con el futuro", terminó puntualizando el directivo.

Por su parte, Suárez-Quiñones puso el foco en la importancia de proteger el "planeta digital" hacia el que caminamos, donde la Estrategia Europa 2020 se considera pieza clave del desarrollo europeo: "la sociedad digital es también vulnerable y los esfuerzos que hagamos todos, desde lo público y lo privado, dependerá que sirva para que éste sea un mundo mejor", afirmó.

La visión de las instituciones

Precisamente, la mejora del marco normativo internacional y nacional fue uno de los puntos más candentes del encuentro. La coordinación y la colaboración entre las distintas instituciones competentes resultan clave, así como el desarrollo de productos nacionales e I+D+i. Así quedó patente en la mesa redonda realizada tras el acto de inauguración, en la que participaron **Joaquín Castellón,** Director Operativo del **Departamento de Seguridad Nacional** (moderador), **Ángel Gómez de Agreda,** Teniente Coronel del Ejército del Aire del **Ministerio de Defensa, Javier Candau,** Jefe del Departamento de Ciberseguridad del **CCN, José Ignacio Carabias,** Jefe de Operaciones del **CNPIC** y **Marcos Gómez**, Subdirector de Servicios de Cibereguridad de INCIBE. Todos destacaron la importancia de estar preparados ante futuras crisis como la que generó WannaCry así como la integración de los organismos y el resto del Estado y empresas para fomentar un mayor y mejor gobierno de la ciberseguridad.

Por su parte, la Directora del Gabinete de la **Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD), Gloria Placer**, explicó el camino emprendido en estos años para adecuar la estrategia española a la nueva Estrategia europea con una especial aproximación a la ultima comisión de la UE en la que se establecieron nuevas medidas para mejorar la ciberresiliencia, las nuevas perspectivas de ENISA y el desarrollo de una certificación de ciberseguridad de las TIC.

En el ámbito internacional, **Camino Kavanagh**, del **King's Collage London**, hizo un repaso de las principales iniciativas de cooperación y capacidad emprendidas, principalmente la planteada en el seno de la OSCE, que está desarrollando un framework de ciberseguridad global para estados.

Un pilar del estado de derecho

Sin duda, uno de los momentos más esperados del evento fue la participación del **Ministro de Energía, Turismo y Agenda Digital**, **Álvaro Nadal**, que por primera vez visitaba la sede del Instituto. En este sentido, Nadal destacó la importancia de la concienciación, protección y educación de la sociedad en ciberseguridad y el papel que juega INCIBE como organismo crucial para la administración española, en su labor de promoción y defensa de la misma, con eventos como ENISE.

"El mundo digital cambia nuestros derechos y estos derechos necesitan una defensa. Por eso, la ciberseguridad forma parte de uno de los pilares básicos del estado de derecho, donde debemos de poner el foco mediático, político y social que se merece", concluyó Nadal. ●

RETOS Y TENDENCIAS EN EL ÁMBITO PRIVADO

En este módulo se celebraron en 11ENISE cinco mesas redondas y se llevó a efecto una presentación, a cargo de **Pedro Antón** (**Red.es**) y de **Marco A. Lozano** (**INCIBE**) del Estudio panel de hogares y encuesta a empresas sobre ciberseguridad. El representante de Instituto presentó dos nuevos servicios para pymes: el de autodiagnóstico y el de políticas de ciberseguridad. Por su parte, el representante de Red.es explicó los resultados más relevantes del Estudio en hogares, entre los que constató el descenso en la confianza digital causado por ciberataques como WannaCry.

En lo que toca a las mesas redondas, la primera, moderada por **Alejandro López** (**INCIBE**), se centró en las **Tendencias en el sector privado**. En él participaron **Francisco Lázaro** (**Renfe**), **Alejandro Villar** (**Repsol**), **Delfim Martins** (**Santander**) y **Juan Carlos Gómez** (**Telefónica**). Los participantes coincidieron en lo positivo de la notificación de incidentes, siempre y cuando se haga en un clima de lealtad, se armonicen los sistemas de notificación y se especifique qué hay que notificar. En lo referente a la gestión de la ciberseguridad IT y OT, caló el mensaje de que requieren de un enfoque global y multidisciplinar.

También se trató la **Evolución de las ciberamenazas** en otra mesa redonda, moderada por **Elena García** (**INCIBE**), en la que tomaron parte **Iván Mateos** (**Sophos**), **Rosa Díaz** (**Panda Security España**), **José Ramón Díaz** (**Symantec**) y **Josep Albors** (**Eset**). Al decir de los participantes, el spam se mantiene, se incrementa el malware en correo, baja el phishing en navegación y aumentan los ataques por sesiones cifradas. Las viejas amenazas siguen funcionando, al tiempo que se empieza a generar malware sofisticado.


Mesa redonda: Tendencias en el sector privado


Mesa redonda: Evolución de las ciberamenazas

El tercer debate, titulado **Nuevas amenazas e investigaciones en mercados underground y monedas virtuales** estuvo moderado por **Raúl Riesco** (**INCIBE**) y protagonizado por **Juan Antonio Rodríguez Álvarez de Sotomayor** (**Guardia Civil**), **Carlos Yuste** (**Policía Nacional**), **Jarek Jarubcek** (**Europol**) y **David Sancho** (**Trend Micro**). Los miembros de las FF y CC del Estado y Europol explicaron algunas investigaciones contra el tráfico de armas en la Dark Web con pago en criptomoneda, o contra la venta de tarjetas de crédito con bitcoins, moneda cuyo uso por la delincuencia se expande.


Nuevas amenazas e investigaciones en mercados underground y monedas virtuales

DESARROLLO PROFESIONAL

En este módulo se celebraron dos debates, uno centrado en la figura del **Data Protección Officer** (**DPO**), consagrada por el RGPD, y otro dedicado al Desarrollo profesional de la ciberseguridad. El primero, moderado por **Francisco Pérez Bes** (**INCIBE**), contó con la participación de **Andrés Calvo** (**AEPD**), **Carlos Saiz** (**ISMS Forum**), **José Calvo** (**CSIC**) y **Gianluca D'Antonio** (**FCC**). Todos reconocieron que la privacidad y la ciberseguridad son parte nuclear de las funciones empresariales. Por su parte, Andrés Calvo anunció que en breve la AEPD activará el canal de comunicación con los DPOs.

En el segundo debate, moderado por **José de la Peña** (**Revista SIC**), participaron **María Jesús Casado** (**IGAE**), **Rafael Hernández** (**Cepsa**), **José Ramón Monleón** (**Orange España**) y **Antonio Ramos** (**ISACA Madrid**). Se reivindicó al CISO como defensor de la seguridad de los datos personales, y se reivindicó el reconocimiento oficial de la función y una capacitación reglada, hitos todavía por alcanzar.

Mesa redonda: Data Protección Officer (DPO)

Mesa redonda: Desarrollo profesional de la ciberseguridad

MARCO INTERNACIONAL

Abrió la sesión **Alison August Treppel** (**Organización de Estados Americanos, OEA**), quién pronunció una conferencia sobre los retos en Latinoamérica y Caribe, cuyos países se encuentran en una fase de madurez inicial; de 32, solo 25 tienen estrategia. De los que sí la tienen, Colombia, Chile, Paraguay, Costa Rica, Jamaica, Panamá y Trinidad y Tobago la han realizado gracias a OEA, en tanto que Guatemala, México, Argentina y República Dominicana están ahora mismo en proceso de creación. Treppel indicó que los datos que actualmente se tienen de la zona se desprenden del Informe Ciberseguridad 2016 de OEA, entidad con la que colabora de forma decisiva INCIBE en diversos proyectos.

Seguidamente tomó la palabra **Philip Lark** (**Centro de Estudios de Seguridad George C. Marshall**) que se centró en el rol de los países en desarrollo en la construcción de una ciberseguridad global, abogando por hacer énfasis en las personas físicas, que son las auténticas 'infraestructura críticas'.

Mesa redonda: ECSO: Building together a European Cyber Ecosystem

Iniciativas para el desarrollo de la ciberseguridad a nivel internacional

Líneas de Apoyo a la internacionalización en I+D+i, por Guillermo Álvarez (CDTI)

Tras la intervención de Lark, tuvo lugar la mesa redonda **ECSO**, Construyendo juntos el ecosistema de ciberseguridad europeo, moderada por **David Ginard** (**Minetad**), quien manifestó que la ECSO, en la que participa la **SESIAD**, es una plataforma de CPPP creada por acuerdo entre la propia ECSO y la **CE**. Los miembros de la mesa, **Luigi Rebuffi** (**ECSO**), **Carlos Prieto** (**AIE Ciberseguridad**), **Antonio Ramos** (**Leet Security**) y **Rames Sarwat** (**Telefónica**), coincidieron en que la ECSO, en la que hay hoy más de 200 entidades, se ha convertido en un foro decisivo para la industria. Particularmente, Ramos indicó que la ECSO debería ser disruptiva en materia de certificación y además plantear la creación de un grado europeo en ciberseguridad.

La sesión matutina incluyó también dos presentaciones, una dedicada a las iniciativas para el desarrollo de la ciberseguridad a nivel internacional, a cargo de **Félix Barrio** (**INCIBE**) y de **Gonzalo García-Belenguer** (**OEA**), y la otra centrada en las líneas de apoyo a la internacionalización en I+D+i, que fueron explicadas por **Guillermo Álvarez** (**CDTI**).

Alberto Hernández

Director General del Instituto Nacional de Ciberseguridad, INCIBE

Centrado en la promoción de la ciberseguridad, el apoyo a la industria y la colaboración publico-privada, INCIBE está inmerso en una transformación interna para hacer frente a nuevos retos en el desarrollo del emprendimiento, el apoyo a la innovación y a la industria española, y una mejor prevención, detección y respuesta ante amenazas especialmente en las áreas de IoT y la Industria 4.0. Sobre estos nuevos horizontes del Instituto habla en la presente entrevista su Director General, Alberto Hernández.

"El destacado presupuesto del que disponemos muestra la apuesta por INCIBE y la creciente preocupación por la ciberseguridad"

– Como Director General de INCIBE, ¿va a seguir la línea de sus antecesores o, por el contrario, tiene en mente reorientar el enfoque del organismo?

– En mi desempeño como Director de Operaciones durante estos últimos tres años, impulsamos nuevas líneas de actuación y mi objetivo es seguir potenciándolas. Dichas líneas se articulan en tres ejes: el desarrollo de servicios públicos dirigidos a ciudadanos y empresas en sus diferentes vertientes, tanto en la parte de prevención como en detección y respuesta ante ciberamezanas; el desarrollo tecnológico para el apoyo a las FF y CC del Estado; y el apoyo e impulso al desarrollo de la industria española, especialmente enfocado en sus componentes de I+D+i y promoción de talento.

Además, estamos inmersos en la transformación del organismo: el paso de INTECO a INCIBE ya supuso una transformación en cuanto a imagen, y ahora queremos llevar a cabo una transformación interna. En este sentido, recientemente hemos publicado una convocatoria con 27 plazas a cubrir con un perfil joven, que suponen la cantera y el futuro de la organización.

– La cooperación con el sector privado, así como la concienciación en ciberseguridad, son dos de las principales apuestas de INCIBE. ¿Qué nuevas medidas tiene previsto llevar a cabo en estos frentes?

– Con el sector privado tenemos dos formas de relacionarnos. La primera, a través de la contratación. INCIBE es un motor para este sector. En este sentido, las capacidades del Instituto deben crecer y nutrirse de las capacidades que la industria proporciona; nuestra pretensión no es duplicar capacidades ni desarrollarlas nosotros, sino apoyarnos en lo que existe y contribuir al desarrollo de la industria. Por otro lado, La CPP es muy importante para llegar tanto a ciudadanos como a las empresas de forma continua y más en situaciones de crisis, como hemos visto con WannaCry y con Petya/NotPetya.

De forma paralela, y respecto a nuestras actividades de concienciación, me gustaría destacar el programa Cibercooperantes, que acabamos de lanzar, una iniciativa cuyo objetivo es apoyar a los profesionales que de forma voluntaria quieran ir a dar charlas a centros escolares. Con este objetivo, estamos en contacto con empresas para que a través de su área de Responsabilidad Social se sumen al programa y que sean las propias empresas las que también motiven a sus empleados a que se unan al programa.

– El Programa Internacional de Aceleración, Cybersecurity Ventures, supone un importante apoyo para la creación de empresas de ciberseguridad. ¿Qué balance y proyección hace de esta edición?

– Cuando en 2014, con la nueva Dirección del Instituto, lanzamos la línea de apoyo al emprendimiento en ciberseguridad –que va desde la fase de incubación, hasta la fase de emprendimiento y de aceleración– recibimos 14 proyectos. En 2015, el número de proyectos ascendió a 25, el pasado año se in-

crementó a 55 y, este año, hemos recibido 76 proyectos para la fase de la aceleradora internacional, de los cuales, preseleccionamos 15 y durante 11ENISE dimos a conocer los 10 ganadores. Este año, quizá, la parte más importante es que al ser un proyecto de aceleradora internacional, propiciamos la existencia de inversores y proyectos extranjeros, que se suma al hecho de ser un programa realizado en colaboración con la Junta de Castilla y León, y con el Ayuntamiento de León.

– Otra importante iniciativa es la European Cybersecurity Challenge, que este año acogió Málaga y que pone a prueba las capacidades y habilidades técnicas de jóvenes talentos. ¿Qué pasos se deberían seguir para mejorar la captación de talento?

– Es cierto que hay que trabajar más en identificar el talento y ponerlo en contacto con las empresas y, de hecho, desde INCIBE estamos en ello; pero la cuestión también es si vamos a tener talento en el futuro. En este sentido, llevamos dos años trabajando en promocionar el talento a través de visitas a institutos no solo para concienciarles sino también, para despertarles el interés en trabajar en ciberseguridad. Además, hemos creado programas de becas para que los jóvenes talentos puedan especializarse en este ámbito. A ello, se unen las iniciativas llevadas a cabo en CyberCamp con el CTF, el Hackathon o las Ciberolimpiadas, además del apoyo que damos a las Cons para que implementen actividades de identificación de talento.

– INCIBE participa activamente en diferentes foros y encuentros a nivel internacional, especialmente junto con la OEA. ¿Qué iniciativas se plantea para aumentar la cooperación en ciberseguridad con otras regiones o estados?

– La acción internacional de INCIBE se desarrolla en función de dos objetivos. El primero, facilitar el intercambio de información y apoyar a que países con los que tenemos que trabajar tengan capacidades de detección y respuesta similares a las de España. El segundo, que se perciba a España como un referente en ciberseguridad. Por lo tanto, las acciones que realizamos con la OEA van con ese doble objetivo. Estamos participando, por ejemplo, como expertos internacionales, en el apoyo para el desarrollo de estrategias de ciberseguridad en países como Paraguay, México, República Dominica o Argentina, donde se utiliza la ECSN española como referente.

Asimismo, iniciativas como el Summer BootCamp, al que este año vinieron 300 profesionales de 29 países a formarse en la materia, ponen de manifiesto la identificación de nuestro país como un referente, lo que va a contribuir también a que cuando las empresas españolas vendan en esos mercados se las identifique como de referencia.

De igual forma, durante los dos últimos años estamos trabajando con el Banco Interamericano de Desarrollo y vamos a seguir fortaleciendo la relación con ellos. Además, tenemos una relación muy estrecha con Europol e Interpol. Y, de forma bilateral tenemos relación con otros países como Tailandia, donde recientemente hemos formado un acuerdo de colaboración con su CERT.

– Los Presupuestos Generales del Estado le asignan más de 23 millones de euros. ¿En qué los va a invertir?

– Este año, hemos tenido el mayor presupuesto para INCIBE en sus 11 años de historia con exactamente 23.220.000 de euros. Se invertirá en los tres pilares de actividad anteriormente comentados, junto con la transformación del Instituto y la potenciación de los servicios. En este último sentido, es vital la potenciación del CERT-SI derivada de las crisis que hemos vivido y del gran aumento de los ciberataques y ciberincidentes en España. Así pues, una apuesta de mi proyecto para INCIBE –apoyada en los presupuestos– en esa potenciación del CERT-SI, el cual, también se va a apoyar en las capacidades de la industria.

"El papel de INCIBE tiene que elevarse como centro de fomento de la discusión, del intercambio de experiencias y de conocimiento. Su rol es el de facilitador"

– ¿Con qué tipo de capacidades se va a potenciar el CERT-SI?

– Tienen que ver con la detección, ya que uno de los motivos del aumento de los ciberincidentes gestionados se debe a la mejora de la misma. También, tenemos que mejorar el análisis de la situación con el mayor detalle y fiabilidad posibles para poder tomar decisiones adecuadas y minimizar el impacto, compartir bajo ciertas circunstancias de seguridad nacional y alertar a los operadores estratégicos y a los afectados para que puedan reaccionar lo antes posible.

– Y, ¿en su vinculación con la ciberseguridad pública?

– Estrechar la colaboración con los organismos públicos es un objetivo prioritario. Estamos trabajando estrechamente con el CNPIC, y también con el Centro Criptológico Nacional (CCN), con el Mando Conjunto de Ciberdefensa (MCCD), y con las FF y CC de Seguridad del Estado.

– ¿Qué medidas va a tomar INCIBE para el desarrollo de la ciberseguridad en IoT y en la Industria 4.0?

– Nuestro objetivo es impulsar la innovación; en esa línea se constituyó el año pasado la Red Nacional de Laboratorios Industriales. La idea es fomentar la innovación en la creación de soluciones y servicios de ciberseguridad para la Industria 4.0. a través de un modelo de colaboración y de contratación de desarrollo de herramientas.

La Red Nacional de Laboratorios Industriales también abarca el área del IoT, un ámbito para el que, además, contamos con convenios bilaterales de colaboración con los propios fabricantes de dispositivos con los que trabajamos en el intercambio de conocimiento y, a través de los cuales, se están constituyendo laboratorios en la propia sede de INCIBE donde los fabricantes nos están cediendo material para que se investigue, se analice y se mejore la ciberseguridad, y podamos ponerlos a disposición de los centros de la citada Red. Asimismo, estamos llevando a cabo diversos estudios junto con la industria para establecer buenas prácticas en el IoT, arquitecturas genéricas que permitan mejorar el proceso de diseño, etc.

– Ante el RGPD, la Directiva NIS y la inminente publicación de la Estrategia de Ciberseguridad Nacional europea y doméstica, ¿qué papel desempeñará INCIBE en el contexto de los entes públicos de ciberseguridad?

– Como orquestador, el papel de INCIBE tiene que elevarse como centro de fomento de la discusión, del intercambio de experiencias y de conocimiento. Tenemos que facilitar que la industria conozca información sobre la demanda, y que lo que necesite la industria llegue a los centros de I+D+i para que innoven e investiguen. Jugamos el papel de facilitador, donde uno de los roles más importantes es el de llegar a acuerdos y estrategias consensuadas. ●

TENDENCIAS TECNOLÓGICAS Y REGULATORIAS

La sesión vespetina de la jornada se inició con una mesa redonda, moderada por **José Ignacio Carabias** (**CNPIC**), dedicada a la Ciberresiliencia en el sector privado, en la que tomaron parte **Juan Atanasio Carrasco** (**Centrales Nucleares Almaraz-Trillo, A.I.E. Industria Nuclear**), **Daniel Largacha** (**Mapfre**), **Antonio Simón Martínez** (**Metro de Madrid**) y **Juan Carlos Lafoz** (**Endesa**), que dio paso a una conferencia de **Andrea Cavina** (**Energypact Foundation**) sobre la ciberseguridad en el muy regulado sector nuclear.

La recta final de la jornada estuvo protagonizada por dos debates, uno dedicado a las tendencias en ciberinteligencia y contrainteligencia, moderado por **Luis Fernández** (**INCIBE**), en el que participaron **Yaiza Rubio** (**Telefónica**), **Román Ramírez** (**Ferrovial**), **David Barroso** (**CounterCraft**) y **Alfredo Pironti** (**IoActive**), y otro, conducido por **Mercedes Fuentes** (**Universidad de León**), en el que tomaron parte **José Luis Piñar Mañas** (**San Pablo CEU**), **Elvira Tejada** (**Fiscalía General del Estado**) y **Jorge Villarino** (**Vinces**), específicamente centrado en los retos regulatorios en el ámbito de la protección de datos personales de una parte, y de otra en la persecución de delitos.

La sesión terminó con una interesante conferencia, a cargo de **David Turón** (**Tip Tap Lab**) sobre las tendencias en IoT y las necesidades y alternativas de la gestión de riesgos de ciberseguridad en este escenario.

Mesa redonda: Ciberresiliencia en el sector privado

La Ciberseguridad en el Sector de la Energía Nuclear, por Andrea Cavina (Energypact Foundation)

Mesa redonda: Retos regulatorios

Mesa redonda: Tendencias en Ciberinteligencia y Contrainteligencia

Tendencias en IoT, por David Purón (Tip Tap Lab)

Tendencias en ciberseguridad en la industria 4.0 y la inteligencia artificial

La ciberseguridad necesita adaptarse a la Industria 4.0 y a la IA para mitigar las nuevas amenazas

A fin de analizar esta problemática que rodea al creciente uso intensivo de internet y las nuevas tecnologías por parte de los procesos industriales, el encuentro realizó una mesa de debate que contó con **Ignacio González** (**INCIBE**) como moderador, y las intervenciones de **Ignacio Álvarez** (**Siemens**), **Ramón Suárez** (**Asociación Europea Mentoring AMCES-EMCC**), **Elyoenai Egozcue** (**S21Sec**), **Ángela Zennaro** (**CERIC-ERIC**) y **Stefan Junestrand** (**Tecma Red**). En el ánimo de los intervinientes pesó mucho el rol que a futuro puede desempeñar la certificación (de productos y proveedores), planteándose la duda de si ello habrá de ser o no obligatorio en la fabricación y despliegue de tecnologías para la industria 4.0. Igualmente se cuestionó quién habría de pagar la ciberseguridad 4.0, abogándose por iniciativas de máxima colaboración de la totalidad de los distintos actores concernidos bajo el enfoque de una visión más holístico.

Mesa redonda: Tendencias en ciberseguridad orientadas a la Industria 4.0

Mesa redonda: Futuro de la Ciberseguridad a través del uso de la Inteligencia Artificial

Asimismo, el futuro de la Ciberseguridad a través del uso de la Inteligencia Artificial (IA) fue analizada por **Juan Santesmases** (**GTI NextWave**), **Enrique Alegre** (**ULE**), **Juan González Martinez** (**Gradiant**) y **Vicente Matellán** (**Centro de Supercomputación de Castilla y León**) en una mesa redonda moderada por **Beatriz García** (**INCIBE**). La necesidad de adaptar la ciberseguridad a los nuevos retos que la rodean –como la Industria 4.0– fue analizada por estos profesionales, los cuales, coincidieron en señalar la importancia del uso de la IA no solo como técnica de defensa, sino también para predecir nuevas formas de ataques con la búsqueda, interpretación e identificación de patrones de comportamiento. No obstante, quedó patente su carencia como técnica ofensiva debido al masivo volumen de datos que es necesario procesar y la limitada potencia de cálculo disponible en la actualidad.

Cybersecurity Ventures 2017

Durante el encuentro se anunciaron los 10 proyectos ganadores de la aceleradora internacional *Cybersecurity Ventures*: **Patrol**, **Techvolución**, **SmartLogin**, **CryptoCloud**, **HideAwayME**, **Crimantra Seguro**, **Keynetic**, **SecureKids** y **MrLooker**. Todos ellos recibirán apoyo en capacitación y "mentorización", tratando de atraer inversión y captar los primeros clientes, además de optar a premios por un valor total de hasta 120.000 euros.

Mesa redonda: Cybersecurity Ventures 2017

Sin duda, la importancia del apoyo al talento emprendedor en la maduración de sus proyectos es clave en esta iniciativa. Por este motivo, de la mano de **Félix Barrio** (**INCIBE**) se llevó a cabo una mesa redonda que contó con la participación **de Eckhard Koch** (**Entrepreneur in cybersecurity**), **Wolfgang Kniejski** (**EIT Digital Accelerator**) y **Fabio Carati** (**Telecom Italia**). Estos profesionales analizaron la complejidad de transformar una idea en un proyecto maduro en un mercado internacional marcado por diversas regulaciones, culturas y formas de comunicarse, que se unen a los problemas inherentes a la propia constitución de una empresa, como la gestión de equipos, las pruebas de producto, la búsqueda de inversores, etc., en un sector como es el de la ciberseguridad en auge y muy competitivo.

Transferencia tecnológica y colaboración

Impulsar la I+D y la innovación nacional, claves para el progreso en ciberseguridad

Al objeto de analizar la colaboración entre la industria y el ámbito académico en un marco en el que España ocupa el undécimo puesto en ciencia e investigación con 24 patentes por millón de habitantes –muy lejos de las 307 de Alemania o las 162 de Francia–, se llevó a cabo una mesa redonda bajo la batuta de **Juan Díez** (**INCIBE**) y la participación de **Antonio Sepúlveda** (**INCIBE**), **Jorge Ramió** (**UPM**), **Marta Beltrán** (**URJC**) y **Marcos Arjona** (**ElevenPaths**). Uno de los principales retos, desde la visión académica, es que el término investigación va estrechamente ligado a la publicación de *papers;* por ejemplo, cerca del 20% de las tesis doctorales se dedican a criptografía porque así es más fácil publicar. Existe por tanto, un exceso de celo por parte de la universidad en la publicación de artículos especializados que llegan a un público limitado. No obstante, estos profesionales coincidieron también en que las empresas en España apuestan poco en innovación, algo que existe en Estados Unidos a través de mecenas.

En otro orden de cosas, es necesario impulsar el uso de la ciberinteligencia dentro de las empresas más allá de los modelos de detección y prevención de amenazas, como se desprendió del debate conducido por **José A. Cascallana** (**INCIBE**) y que contó con la participación de **Javier Zubieta** (**GMV**), **Xavier Mitxelena** (**S21Sec**), **Juan Antonio Gómez Bule** (**Walhalla**) y **Mikel Rufián** (**Innotec**). Los ponentes examinaron el estado del arte de la ciberinteligencia, aún en vías de consolidación –con frecuentes confusiones de sus modalidades Aprendizaje Automatizado o Aprendizaje Profundo, que no son sinónimos)– y la necesidad de compartir información para poder alimentarla, además de aunar y unificar los tipos de tecnologías existentes para gestionar de forma más centralizada la información. Para los presentes, se van a sufrir nuevas patologías en ciberseguridad, como los efectos colaterales derivados del uso masivo de dispositivos IoT y, por ello, se hace vital impulsar la I+D y el desarrollo de tecnología nacional.

Presentación del observatorio europeo de ciberseguridad y privacidad

Mesa redonda: Transferencia, retos ciberseguridad Ciber Inteligencia

Mesa redonda: Transferencia tecnológica y colaboración Industria-Academia

Implicaciones del RGPD

En el contexto de la presentación del Observatorio europeo de ciberseguridad y privacidad (Cyberwatching.eu) tuvo lugar una mesa redonda en la que se cubrieron diversos aspectos del RGPD en cuanto a la debida protección de la información y, especialmente, en lo referente al asesoramiento jurídico, los seguros y las soluciones existentes que ayuden a las empresas a hacer frente a los daños generados por un ciberataque. Para ello, subieron al estrado **Javier Tobal** (**AEI Ciberseguridad**), **Pablo Montoliú (AON), Laura Senatore** (**ICT Legal Consulting**), **Mark Miller** (**Conceptivity**) y **Raúl Pérez** (**Panda Security**). Algunas de las conclusiones más relevantes del aspecto jurídico en ciberseguridad es que éste tiene que ayudar al cliente desde la perspectiva de la privacidad por diseño. Sin duda, las sanciones marcadas por el RGPD es uno de los principales quebraderos de cabeza para las empresas. En este punto, la importancia de los ciberseguros entra en juego. Aunque, sin duda, un punto a destacar es la notificación en 72 horas, algo que va cambiar las reglas de los ciberseguros en Europa. Por último, se consideró igualmente destacable el problema que genera la falta de visibilidad a las empresas, muchas de las cuales desconocen si están o han sido atacadas, y la necesidad de contar con soluciones de ciberseguridad apropiadas.

Emprendimiento en ciberseguridad

Los emprendedores deben demostrar que la ciberseguridad aporta valor a los negocios

La búsqueda de nuevas oportunidades de negocio en el mundo de la ciberseguridad fue uno de los principales asuntos que rigieron la undécima edición de ENISE, en un sector en el que se continúa alertando sobre la falta de especialización. Por este motivo, el encuentro reservó un espacio de debate donde se profundizó en el arte del emprendimiento en España, moderado por **Ignacio Caño** (**INCIBE**), y que tuvo como participantes a **Antonio Ramos** (**Mundo Hacker Day**), **José Manuel Vera** (**One Hacker**), **Francisco Javier Inaraja** (**Revista Emprendedores**), **Marta Yoldi** (**Diario Autónomos** y **Emprendedores**), **Simon Roses** (**Vulnex**) e **Iván Nabalón** (**ElectronicID**).

Mesa redonda: Situación actual del emprendimiento en ciberseguridad

Tras la presentación de Caño, quien destacó la necesidad de dinamizar el entorno especialmente desde las administraciones públicas y en colaboración con la empresa privada, los ponentes sentaron la base de que en el mercado de la ciberseguridad existe un amplio abanico de oportunidades para emprender. El problema es la falta de inversión, especialmente por parte de empresas de capital riesgo, debido sobre todo a la poca rentabilidad que las empresas de software generan a corto-medio plazo. Y, aunque la ciberseguridad ya no se considera una opción, la clave es demostrar que puede aportar valor.

Los participantes en la mesa de debate también consideraron determinante no solo tener una buena idea, sino además, un buen equipo detrás que la materialice, conocer bien el mercado y los clientes, e intentar ampliar las miras desde las oportunidades nacionales hacia las internacionales.

Panel de hogares y encuesta empresas sobre ciberseguridad 2017

El **Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI),** de la mano de **Pedro Antón Martinez (Red.es) y Marco A. Lozano (INCIBE),** presentó durante el encuentro dos informes. El primero de ellos, la Encuesta sobre Confianza Digital en las Empresas, la cual, puso de relieve que las empresas que más activos gestionan son más conscientes de la importancia de la seguridad, mostrando estar más preparadas. Por su parte, el Estudio de Confianza y Seguridad en los hogares españoles señalaba que la ciberconfianza ha alcanzado un valor mínimo histórico en el primer semestre de 2017, situándose en un 40% los usuarios que tienen mucha o bastante confianza en Internet.

Premio 11ENISE

Durante la celebración de 11ENISE se hizo público el ganador del Premio ENISE a la mejor iniciativa escolar 2016-2017 en ciberseguridad, que recayó en el centro **IES El Alisal** de Santander, por su proyecto “Escuela de ciberseguridad y hacking ético ciberalisal”. La entrega del premio –un cheque por valor de 2.500 euros en material tecnológico–, fue realizada por el Ministro Nadal, el cual, destacó que “este Premio ENISE pone de manifiesto el compromiso del Gobierno por impulsar la formación y la concienciación en ciberseguridad desde edades tempranas”.

El mayor evento de #ciberseguridad

¡Entrada gratuita!

SANTANDER

del **30** de noviembre al **3** de diciembre **2017**

https://cybercamp.es

@CyberCampEs #CyberCamp2017

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD