DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2017 | XII LEGISLATURA | Núm. 65 | Pág. 1

DE SEGURIDAD NACIONAL

PRESIDENCIA DEL EXCMO. SR. D. JOSÉ MANUEL GARCÍA-MARGALLO Y MARFIL

Sesión núm. 9

celebrada el jueves 16 de noviembre de 2017 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

Comparecencia. Por acuerdo de la Comisión Mixta de Seguridad Nacional:

---

cve: DSCG-12-CM-65

Se abre la sesión a las once y treinta y cinco minutos de la mañana.

El señor **PRESIDENTE:** Buenos días, señoras y señores diputados y senadores.

Tres observaciones antes de empezar la sesión en su desarrollo ordinario. En primer lugar, quiero agradecer a los distintos grupos parlamentarios la flexibilidad q ue me han permitido para convocar esta Comisión a medida que han ido evolucionando los acontecimientos. No siempre es fácil reunir a diputados y senadores, mucho más cuando tenemos que contar también con las agendas de los comparecientes.

En segundo lugar, se va a repartir a lo largo de la sesión una documentación sobre los recientes incidentes relacionados con el ciberespacio y Rusia que espero que sean de utilidad y que iremos completando a lo largo de la semana.

En tercer lugar, si no tienen inconveniente, al finalizar esta sesión convocaría una Mesa informal con los portavoces para actualizar las comparecencias de la semana que viene, teniendo en cuenta también los acontecimientos recientes que estamos viviendo. Pero de eso hablaremos luego.

Sin más, voy a dar la palabra a nuestro compareciente, don Alberto Hernández Moreno, director general del Instituto Nacional de Ciberseguridad de España, para informar sobre diversas cuestiones relativas a la ciberseguridad en nuestro país. A continuación, cada portavoz contará con un turno de cinco minutos, sin perjuicio de un segundo turno después de que el compareciente haya respondido a las primeras inquietudes de los diputados y senadores.

Tiene la palabra don Alberto Hernández Moreno.

El señor **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD, S.A., INCIBE** (Hernández Moreno): Muchas gracias, presidente. Buenos días, señorías.

En primer lugar, he de decir que para mí es un honor comparecer en esta Comisión Mixta y tener la oportunidad de compartir con ustedes mi visión sobre la ciberseguridad tanto en nuestro país como también a nivel mundial, así como las actividades que desarrollamos desde el instituto que dirijo, el Instituto Nacional de Ciberseguridad, Incibe, instituto que es dependiente del Ministerio de Energía, Turismo y Agenda Digital a través de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. Tenemos como foco principal la protección de nuestros ciudadanos y del sector privado en España.

Teniendo en cuenta la primera comparecencia en esta Comisión llevada a cabo por el don Joaquín Castellón, director operativo del Departamento de Seguridad Nacional, en la que explicó de forma detallada cuál era el esquema nacional de ciberseguridad, los organismos públicos que trabajamos en ella y cómo nos coordinamos, me gustaría, señorías, centrar mi intervención en dos puntos. El primero, los retos a los que nos enfrentamos a nivel país en el ámbito de la ciberseguridad de nuestros ciudadanos y nuestras empresas y, por supuesto, exponer las estrategias y líneas de acción que estamos llevando a cabo para elevar ese nivel de seguridad y de protección. El segundo, la oportunidad que la ciberseguridad supone para el desarrollo de nuestro país.

La ciberseguridad no es solamente un reto para la seguridad nacional sino una verdadera oportunidad para el desarrollo industrial, económico y social de nuestro país. Tenemos la oportunidad de jugar un papel importante en el desarrollo de la industria y en la creación de puestos de trabajo en este nuevo sector profesional y, por lo tanto, quería compartir en primer lugar esta doble visión de reto a la seguridad nacional y de oportunidad como país para el desarrollo de nuestra economía. Como saben, Internet, el ciberespacio o las tecnologías se han convertido a día de hoy en una herramienta básica y diaria de nuestras empresas, administraciones y ciudadanos. De hecho, estas herramientas están cambiando la forma en la que nos relacionamos, la forma en la que nos comunicamos y ya están produciéndose avances sustanciales en campos como la sanidad, el transporte, la energía, la producción alimenticia, etcétera. Por lo tanto, diría que las tecnologías suponen un avance claro en el desarrollo de los países y de las sociedades. Creo, además —y ahora hablaremos de ciberseguridad— que debemos mantener esa visión positiva y constructiva del uso de las tecnologías, la apuesta por el desarrollo de las mismas y la incorporación en todos los aspectos de nuestra sociedad e industria.

Sin embargo, el ciberespacio, Internet o las tecnologías constituyen un dominio nuevo tan real como es el espacio terrestre, el marítimo, el aéreo o el espacio exterior. Un dominio tan real en el que la forma en la que nos relacionamos tiene también cabida en este nuevo espacio; además, las amenazas que conocemos en los espacios tradicionales, en los espacios físicos pueden tener materialización en este nuevo dominio virtual pero, como decía, igualmente tan real como el resto de los dominios. ¿Por qué? Porque el ciberespacio, Internet o las tecnologías en general tienen unas características que lo hacen

cve: DSCG-12-CM-65

especial. En primer lugar, hablamos de un dominio global; es un dominio que llega a todos los rincones del mundo. Estamos hablando que, a día de hoy, ya se ha superado la cifra de 3600 internautas en el mundo. Además, el coste de acceso es pequeño; pensemos, por ejemplo, en un dispositivo móvil, el más barato del mercado —estamos hablando de unas decenas de euros—, que nos permite conectarnos a Internet allí donde estemos. El tiempo se mide en milisegundos y amenazas que se originan en lugares que están a miles de kilómetros de distancia, en el ciberespacio pueden tener un impacto en solamente unos pocos milisegundos. Es, además, un espacio asimétrico en la medida en que pueden producirse impactos que de otra manera tendrían que haber sido pensados y desarrollados con mucho tiempo y mucho dinero y que, sin embargo, en el ciberespacio, con poca inversión y únicamente con un conjunto de personas con la capacidad y conocimiento técnico adecuado, pueden generar un impacto de forma teórica de igual manera que podría ocurrir en el espacio físico, pero para lo que necesitaríamos un Estado trabajando durante muchos años e invirtiendo miles de millones de euros.

Por último, el ciberespacio incluye una característica que lo hace muy atractivo para la comisión de delitos y actividades delictivas en él, que es la dificultad de la atribución en las acciones, es decir, hablamos de anonimato. El anonimato se debe fundamentalmente a varias razones. La primera de ellas, la tecnología, que permite cifrar, enmascarar las acciones que tienen lugar en Internet y en el ciberespacio. Además, existen diferentes aproximaciones y concepciones de lo que es el ciberespacio, de lo que es la ciberseguridad y, por poner un ejemplo, lo que es la privacidad. Pensemos que los aspectos políticos, culturales e históricos tienen una influencia en cómo un país puede percibir las acciones para proteger la privacidad de los ciudadanos. Nos podemos encontrar en países de nuestro entorno, y también en nuestro propio país, donde tenemos leyes que permiten conservar los datos de navegación cuando estamos conectándonos a Internet, que permiten, bajo autorización judicial, que nuestra Policía, Guardia Civil y Fuerzas y Cuerpos de Seguridad en general puedan perseguir los delitos cometidos en Internet. Pero si nos vamos a países, también nuestro entorno, pero a nivel mundial, encontramos que esas leyes no tienen cabida puesto que la percepción que tienen a la influencia o el impacto en la privacidad no lo permiten.

Por lo tanto, estamos hablando de diferentes maneras de percibir y entender la ciberseguridad y de cómo implementarla; además, cada vez más tenemos un avance tecnológico que hace que el ciberespacio crezca y lo haga de forma desigual. En el Internet de las cosas o en los dispositivos de uso doméstico que se están incorporando a Internet, el crecimiento está siendo muy importante. Según diferentes estudios, en concreto, uno de ellos de la compañía Gartner, para 2020 habrá más de 25 000 millones de dispositivos conectados a Internet y en los siguientes tres años podremos duplicar esa cifra y llegar a los 50 000 millones de dispositivos, muchos de los cuales no reunirán las características de seguridad necesaria. Si tenemos en cuenta la primera característica que he citado, señoría, la globalidad, hay que entender la seguridad nacional como una seguridad que debemos construir desde dentro y también desde el ámbito de la colaboración internacional y la colaboración público-privada, puesto que las amenazas pueden provenir de cualquier sitio.

Finalmente, me gustaría indicar una última característica asociada a los avances tecnológicos, que es la innovación disruptiva, que aborda la evolución rápida de la tecnología, la forma de usarla y, por tanto, la forma en que hay que entender la propia ciberseguridad de la misma. Si echamos la vista atrás, podemos ver herramientas que a día de hoy se han convertido en herramientas cotidianas, de uso general para todos nosotros, para nuestros hijos, para nuestros ciudadanos y ciudadanas, y que hace tan solo diez años no existían. Me remito a poner una serie de ejemplos como Whatsapp, Uber, Dropbox, YouTube, Gmail, Facebook, Linkedin, que son redes sociales o herramientas tecnológicas que hace tan solo diez o quince años no existían y que ahora mismo están liderando la transformación no solo tecnológica, sino la transformación social de nuestro país y de todo el mundo.

Como les decía, todas estas características hacen que el ciberespacio juegue un papel fundamental en la seguridad nacional de todos los países. Las recientes crisis que hemos vivido este año, como han sido WannaCry, o más tarde, en el mes de junio, Petya, han puesto de manifiesto a las sociedades, a los ciudadanos que la ciberseguridad es un asunto de todos y no solamente un asunto reservado a aquellos organismos o especialistas que trabajamos en este campo. Pudimos ver en esas crisis de mayo y junio cómo la preocupación de nuestra sociedad aumentaba de forma muy rápida en torno a los incidentes de ciberseguridad.

Permítanme describirles cuál es la situación de la ciberseguridad en el marco de nuestros ciudadanos y de nuestras empresas. Desde el centro de respuesta ante incidentes de seguridad e industria, centro

cve: DSCG-12-CM-65

operado por Incibe bajo la coordinación del propio Incibe del Ministerio del Interior, venimos gestionando desde hace muchos años incidentes de ciberseguridad que afectan a nuestros ciudadanos y al sector privado, desde la pequeña y mediana empresa hasta la empresa estratégica. En el año 2014, gestionamos cerca de 18 000 incidentes que afectaron a nuestros ciudadanos y a nuestras empresas y cerca de 60 estuvieron relacionados con grandes empresas o empresas estratégicas. En el año 2015, esta cifra aumentó hasta los 50 000 incidentes y se duplicó el número de incidentes que afectaron a empresas estratégicas. En el año 2016, gestionamos más de 115 000 incidentes de ciberseguridad en nuestro país, que afectaron a ciudadanos y empresas; más de 400 de ellos estaban asociados a empresas estratégicas. A 31 de octubre, hemos gestionado más de 113 000 incidentes de ciberseguridad y más de 700 en empresas estratégicas, lo que pone de manifiesto que se está incrementando el número de incidentes —y hablaré ahora de incidentes y no de ciberataques— que gestionamos en nuestro país. Esto se ha debido fundamentalmente a cuatro razones, que creo que son razones positivas, optimistas —diría más bien realistas— y también conclusiones que requieren que sigamos trabajando e implementando esfuerzos.

En primer lugar, gestionamos más incidentes porque las capacidades públicas de detección han mejorado considerablemente en estos tres últimos años; hemos venido haciendo inversiones considerables para tener una mayor capacidad de detección sobre lo que ocurre en nuestro país. En segundo lugar, porque el nivel de confianza que se genera entre Incibe —el CERT, centro de respuesta a los ciudadanos— y las empresas está creciendo año a año, de tal forma que son cada vez más los ciudadanos y las empresas que nos comunican, nos hacen saber a Incibe, que están sufriendo un incidente y nos piden ayuda y, nosotros, por supuesto, les apoyamos en la resolución. El tercer factor tiene que ver con el aumento de los ciberataques puesto que, como decía anteriormente, las características del ciberespacio lo hacen un nuevo dominio tan real como el resto y en el que se permite que amenazas tradicionales de los entornos físicos se puedan materializar de forma más rápida, de forma anónima y de forma global en este nuevo dominio. Finalmente, como avanzaba, el incremento de los dispositivos y tecnologías conectados al ciberespacio están provocando que el campo de exposición a nivel de vulnerabilidad también crezca.

Podemos decir que el negocio de la ciberseguridad, las inversiones, la facturación de las empresas que se realiza a nivel mundial están en torno a 75 000 u 80 000 millones de euros anuales, si bien en cuanto al negocio del cibercrimen diferentes estudios hablan de que puede ir desde el 0,1 % del producto interior bruto mundial hasta el billón de euros anual. Como ven, en cualquiera de los casos, estamos hablando de un negocio muy lucrativo, fundamentalmente porque el ciberespacio presenta esas características.

Cuando hablamos de ciberseguridad en el ciudadano y en la empresa debemos abordar este reto desde diferentes puntos de vista. Si volvemos la vista atrás y analizamos el estudio de cibercriminalidad del Ministerio del Interior correspondiente al año 2016, las Fuerzas y Cuerpos de Seguridad del Estado tuvieron constancia de más de 66 000 delitos informáticos en España, un 10,7 % más que en el año 2015, con un 68,9 % correspondientes a fraudes informáticos —es decir, volvemos a reforzar el tema del negocio que supone el ciberdelito— y otra parte importante, el 17,2%, a amenazas y coacciones.

Cuando analizamos lo que pasa en España a nivel técnico, fundamentalmente observamos que ocurre de todo, desde movimientos activistas, ataques de denegación o disrupción de servicios en nuestras compañías, pero fundamentalmente nos encontramos con tres tipologías de incidentes. La primera de ellas es el *malware* en general, es decir, ese virus, código malicioso, o como queramos llamarlo, que se desarrolla con el objetivo de infectar las redes de nuestras empresas, de nuestros ciudadanos y controlarlas cuanto más tiempo, mejor y, mientras las están controlando, robar información y con esa información, por supuesto, intentar conseguir dinero.

La segunda tipología de incidentes se refiere a fraude general, normalmente suplantando la identidad de empresas para acercarse al ciudadano o a la empresa con el mismo objetivo, robarle dinero. Por último, el intento de acceso o intrusión, es decir, incidentes relacionados como WannaCry o Petya, en el mes de mayo y junio, *malware* que tiene como objetivo entrar en los sistemas de un ciudadano, de una empresa, cifrarlos y pedir un rescate. Es decir, como vemos, los tres tipos de incidentes de ciberseguridad que tienen mayor impacto en nuestro país están relacionados, si bien en el ámbito del ciudadano y del sector privado tienen una motivación claramente económica. ¿Qué podemos hacer para protegerlos? Llevamos trabajando intensamente desde hace muchos años. Podemos recordar que el primer virus de la historia se desarrolló a principios de los años setenta. Llevamos trabajando en el sector público y el sector

cve: DSCG-12-CM-65

privado intensamente muchos años en este campo y podemos decir que desde el año 2013, cuando se aprobó la Estrategia de Ciberseguridad Nacional, tenemos los instrumentos para trabajar de forma coordinada y colaborativa en la protección de nuestros ciudadanos, empresas y administraciones públicas.

En Incibe trabajamos en varias líneas de acción para proteger a nuestros ciudadanos y a nuestras empresas, todas ellas son muy importantes, puesto que la ciberseguridad tiene un componente holístico fundamental. La primera de ellas es la concienciación. Tenemos que trabajar y concienciar a nuestros ciudadanos y a nuestras empresas. Todos usamos tecnologías, tanto en el ámbito profesional como en nuestro ámbito doméstico. Nuestros hijos, nuestros menores, utilizan tecnologías; deben hacerlo y cada vez lo harán más, pero deben hacerlo de forma segura y aplicando una serie de medidas de seguridad. Por lo tanto, hemos venido trabajando intensamente en campañas de concienciación en colegios e institutos y el próximo año haremos una campaña intensiva en medios de comunicación en este campo. Hemos lanzado un programa de voluntariado para que todos aquellos profesionales que puedan y quieran aportar a la mejora de la ciberseguridad en nuestro país lo hagan y tenemos más de trescientos cibercooperantes. Hemos incorporado materiales para educación primaria y secundaria y estamos trabajando con el Ministerio de Educación. Hemos desarrollado una iniciativa pionera en el mundo denominada CyberCamp que celebraremos por cuarto año consecutivo. Este año será en Santander, el pasado año fue en León. Mediante juegos, herramientas, discusiones y charlas acercamos la ciberseguridad de una forma lúdica a nuestros ciudadanos y a nuestros menores. El pasado año en la ciudad de León tuvimos la oportunidad de tener la presencia de más de veinte mil personas en los cuatro días del CyberCamp.

Trabajamos también en el ámbito de la formación. Es muy importante formar a nuestros profesionales, independientemente del campo profesional al que se dediquen. Hemos trabajado en estos últimos años para formar jueces, fiscales, abogados y profesionales de diferentes ámbitos. Me gustaría resaltar la iniciativa Cybersecurity Summer BootCamp que, en colaboración con la Organización de Estados Americanos, hemos desarrollado este año por segundo año consecutivo en la ciudad de León; trescientas personas de treinta países del mundo vinieron a España —a León— a formarse en ciberseguridad: profesionales del ámbito técnico, del ámbito policial y también jueces y fiscales.

Por supuesto, hay que trabajar en servicios preventivos y en ello estamos trabajando intensamente. En estos tres últimos años hemos desarrollado numerosos ciberejercicios en empresas estratégicas para capacitar a su personal en el ámbito de la ciberseguridad, para que sean capaces de resistir a un incidente y responder. Señorías, me gustaría indicarles de nuevo que la realidad es que gestionamos cientos de incidentes de forma diaria. Nuestras empresas y nuestros ciudadanos sufren incidentes y creo que es buena noticia decir que el impacto que hasta este momento se ha producido en nuestro país ha sido muy bajo.

Trabajamos también en servicios para nuestros ciudadanos a través de la Oficina de Seguridad del Internauta. Tenemos teléfonos de atención a ciudadanos y a menores y canales especializados dependiendo de la edad, puesto que la problemática y la forma de llegar son diferentes. Por supuesto, trabajamos en la respuesta y tenemos un servicio 24 por 7 y, en caso de situaciones de crisis —WannaCry o Petya han sido buenos ejemplos-, podemos trabajar en ese formato. De hecho, tenemos los equipos permanentemente preparados para cualquier situación de crisis. Es muy importante notificar a nuestros ciudadanos y a nuestras empresas que hemos detectado que les pasa algo; si no, no estaríamos trabajando en la mejora de su protección.

Una iniciativa novedosa e innovadora en el mundo es el denominado servicio AntiBotnet. Mediante la colaboración publico-privada de Incibe con los operadores de telecomunicaciones, de forma diaria enviamos a los operadores de telecomunicaciones aquellas direcciones de abonados que han sufrido un incidente. Los operadores de telecomunicaciones se ponen en contacto con sus clientes, les comunican que han sufrido un incidente y les indican que se pongan en contacto con Incibe para resolverlo. En este caso, desde el inicio del servicio se han mandado desde los operadores de telecomunicaciones más de 400 000 notificaciones a ciudadanos en España y tenemos una tasa de desinfección superior al 65 %. Creo que es una buena noticia comentarles que muchas de estas iniciativas que estamos desarrollando en España las estamos compartiendo a nivel internacional y son muchos los países de nuestro entorno, de América y de otros continentes que nos están solicitando compartir esta experiencia que estamos haciendo en España.

Como les decía, otro pilar fundamental es la colaboración internacional. Estamos en un nuevo dominio mundial hiperconectado en el que no existen fronteras. La seguridad nacional también depende de la

cve: DSCG-12-CM-65

seguridad del resto de los países. Por lo tanto, hemos trabajado intensamente en los tres últimos años para afianzar alianzas a nivel internacional y a nivel bilateral con países para reforzar sus capacidades de ciberseguridad y mejorar el intercambio de información y alerta temprana. Me gustaría destacar la alianza mantenida con la Organización de Estados Americanos con la que el Reino de España tiene un acuerdo en materia de ciberseguridad y que ha permitido desarrollar iniciativas como el Cybersecurity Summer BootCamp que antes les comentaba, y que expertos españoles de Incibe hayan estado participando como expertos internacionales en el desarrollo de las estrategias nacionales de ciberseguridad de países de Latinoamérica. Además, hemos implementado ejercicios internacionales —los ha organizado Incibe junto con la OEA— con el objetivo de adiestrar las capacidades de respuesta de estos países, puesto que lo que ocurre en España en general no se origina en España, sino que se origina a miles de kilómetros y pega varios saltos antes de llegar a nuestro país. Por lo tanto, mantener una colaboración estrecha con equipos similares en otros países es fundamental a la hora de proteger a nuestros ciudadanos y a nuestras empresas. Quiero destacar también la organización del I Foro Internacional de Género y Ciberseguridad: creando un mundo digital más inclusivo, que desarrollamos este año en la ciudad de León por primera vez a nivel mundial. En coordinación con la Organización de Estados Americanos, el Banco Interamericano de Desarrollo, el Ministerio de Asuntos Exteriores y más de quince países, discutimos acerca de la posibilidad de trabajar en la diversidad de género en el ámbito de este nuevo sector —porque la ciberseguridad también es una oportunidad— y de desarrollar estrategias para la lucha contra la violencia de género en este ámbito.

Me gustaría terminar indicándoles que es importante trabajar en el ámbito tecnológico. En Incibe trabajamos muy intensamente en el ámbito tecnológico para apoyar a nuestra Policía, a nuestra Guardia Civil y a las Fuerzas y Cuerpos de Seguridad en general para que dispongan de tecnologías que les permitan luchar contra el cibercrimen y el ciberdelito en todas sus facetas. Además, señorías, es importante indicar que tenemos que trabajar para minimizar la dependencia tecnológica de nuestro país. Tenemos servicios esenciales que dependen de tecnologías que no son de nuestro país. En algunos casos es importante que tengamos en nuestro país capacidad tecnológica para satisfacer esos nuevos servicios.

Por último, quiero comentarles que igual de importante que trabajar en nuestra seguridad nacional es trabajar para el desarrollo de la economía de nuestras empresas. La ciberseguridad es una oportunidad real de desarrollo de la industria. España cuenta a día de hoy con más de 140 empresas especializadas en el ámbito de la ciberseguridad. Es un sector con un crecimiento del orden del 11 al 13 % anual en el que, según datos de la Comisión Europea, España crecerá un punto por encima de la media europea; es decir, nos igualaremos a la media a nivel mundial. Por lo tanto, tenemos oportunidad de trabajar para que nuestras empresas desarrollen productos y servicios que sean competitivos a nivel internacional —puesto que estamos hablando de un sector global— y para que puedan jugar un papel importante y crear puestos de trabajo. A día de hoy la ciberseguridad da trabajo directo a más de 6500 personas en España y estamos nada más que en el inicio. Estamos trabajando intensamente en Incibe en estos tres últimos años en colaboración con la industria española, con la industria nacional, para desarrollar esta capacidad. Para eso tenemos un programa muy amplio para analizar la demanda para los próximos años y hacer que la industria española trabaje en el desarrollo de servicios y productos que satisfagan esa demanda y que los centros de I+D+i nacionales tengan la capacidad de investigar, desarrollar e innovar en aquellos productos cuyo tiempo de transferencia sea corto y se puedan incorporar a las empresas. Y, por supuesto, también estamos trabajando —esto es muy importante— en la promoción e identificación del talento. Sabemos que a nivel mundial hay un problema en cuanto al talento en ciberseguridad. Diferentes estudios hablan de que en los próximos años habrá una demanda no satisfecha de uno a dos millones de puestos de trabajo en ciberseguridad en el mundo.

Por lo tanto, tenemos que trabajar desde edades tempranas para promocionar el interés en el ámbito de la ciberseguridad y facilitar a nuestros jóvenes que puedan desarrollar estudios, carreras y especialidades para dedicarse a la ciberseguridad. Es un sector que no está reducido ni es específico de los técnicos. La ciberseguridad es un sector profesional en toda regla en el que tienen cabida psicólogos, pedagogos, profesores, responsables de proyecto, técnicos o periodistas. Si miramos atrás, en la crisis de WannaCry podemos ver que la comunicación en este tipo de situaciones es muy importante y tenemos que tener a nuestros equipos preparados.

Señorías, creo sinceramente que estamos haciendo un trabajo muy intenso en los últimos años y que empezamos a ver ciertos resultados. Uno de ellos —me gustaría compartirlo con ustedes— es que

cve: DSCG-12-CM-65

nuestro equipo español de jóvenes talentos quedó en la ciudad de Málaga hace tres semanas de nuevo campeón de Europa de jóvenes talentos en el ámbito de la ciberseguridad por encima del catorce países europeos. Creemos que las estrategias y acciones que estamos llevando a cabo para promover el talento, para identificarlo y para entrenarlo están dando resultados. Creo que estamos yendo por el buen camino a nivel nacional, pero por supuesto tendremos que seguir trabajando.

Señor presidente, muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias a usted.

Damos comienzo a las intervenciones de los portavoces, empezando por el Grupo Parlamentario Mixto. Señor Yanguas.

El señor **YANGUAS FERNÁNDEZ:** Muchas gracias, señor presidente.

Intervendré brevemente. Antes de comenzar con lo que ha dicho el compareciente y tomando sus últimas palabras —o las palabras que ha dicho usted, señor presidente— cuando hablaba de flexibilidad en los horarios y de venir aquí, estaría bien que alguna de estas reuniones se celebrase en nuestra casa, en la Cámara Alta, en el Senado. Puesto que esta es una comisión mixta, le pediría, por favor, que fuéramos allí alguna vez. Es un pequeño comentario que quiero dejar aquí.

En segundo lugar, como no podía ser de otra manera, quiero agradecer las explicaciones del compareciente, el señor Hernández Moreno. Voy a ir a salto de mata porque he ido anotando lo que ha comentado. Prefería no tener un discurso y anotar preguntas a medida que usted iba hablando. Por eso, perdónenme si voy un poco a salto de mata.

Aunque usted no ha hecho referencia a ello, me gustaría saber qué papel juega la Ley orgánica de protección de datos de carácter personal que tenemos ahora misma aprobada en nuestro país. ¿Cree usted que en este campo de la ciberseguridad está siendo superada? ¿Está obsoleta esa norma, aunque en otros campos funcione muy bien? Porque creo que en este habría que modificarla.

Usted ha hablado —y estoy de acuerdo con usted— de dominios globales, de espacios asimétricos y de un aspecto transversal a todas las profesiones. Por lo que ha dicho, ustedes también asesoran a empresas grandes, pequeñas, estratégicas, por lo que le pregunto: ¿estamos preparados? ¿Qué nivel de preparación tenemos nosotros ante un ataque masivo a las infraestructuras críticas de nuestro país, que muchas de ellas están regidas por empresas estratégicas? En segundo lugar, ¿qué posibilidades hay de que pase esto que le acabo de decir, que haya un ataque masivo?

No le voy preguntar —además nos han dado una documentación al respecto que agradezco al presidente— sobre el tema ruso. A lo mejor otro portavoz se lo pregunta o incluso seguro que lo hace algún medio de comunicación, pero yo no lo voy a hacer; de todas formas, sí le diré que su discurso, su exposición me ha gustado. Dice que todos los años se duplican los incidentes, ¿de dónde vienen esos incidentes? Ya sabemos que son globales, pero de entre los países que nos están atacando —vamos a decirlo así—, ¿cuáles son los más activos? Y si se están duplicando los incidentes, ¿qué está pasando con su personal, también se está duplicando? ¿Y su presupuesto? Ya que no está aquí el ministro, vamos a pedir —y usted también lo podría hacer— más presupuesto para poder trabajar mejor y para esas inversiones en ciberseguridad que seguro —de su discurso así lo he percibido— que necesitamos en España.

Usted ha hablado de la colaboración que mantiene con las Fuerzas y Cuerpos de Seguridad del Estado. Como senador de Unión del Pueblo Navarro —vengo de la Comunidad Foral de Navarra—, le pregunto: ¿ustedes también mantienen una colaboración específica con las policías autonómicas, con la Policía Foral de Navarra y con otras policías, o hay otros cauces que yo desconozco?

Esas eran mis preguntas. Le agradezco de nuevo sus explicaciones y su clara exposición.

El señor **PRESIDENTE:** Muchas gracias, señor Yanguas. La Mesa y los portavoces tomamos nota de su invitación de ir al Senado, cosa que a mí me complace mucho.

Por el Grupo Ciudadanos, señor Salvador.

El señor **SALVADOR GARCÍA:** Muchas gracias, señor presidente.

Señor Hernández, en primer lugar, le doy la bienvenida a esta Cámara en nombre de mi grupo en un día de plena actualidad de la ciberseguridad y la necesidad que tenemos de invertir en este campo para ser un país seguro y confiable en todos los sentidos.

cve: DSCG-12-CM-65

He escuchado muy atentamente su intervención. Conozco la trayectoria de Incibe, también la de su precursor —aunque era más transversal—, que era Inteco y, por tanto, sé que es un buen instrumento al servicio de los buenos en esta cruzada mundial para intentar que los malos no terminen ganando esa batalla.

De la información que ha traído, ha mostrado algo que no por conocido deja de ser relevante, me refiero al ámbito al que afecta la ciberseguridad, que es el marco mundial. Ha mencionado la velocidad y la globalización como dos elementos fundamentales y nos ha dicho que el ataque puede venir de cualquier sitio y afectar a cualquier ámbito. Por lo tanto, la primera sensación es que o nos organizamos muy bien e invertimos bastante en ciberseguridad para tener un sistema muy fiable o, si no, podemos tener muchas fallas y, a partir de hay, vulnerabilidades y problemas.

La vertiente de pymes y empresas es algo fundamental. Si estamos promocionando el comercio electrónico, que haya planes para que las empresas se metan en Internet, si estamos haciendo que ese mundo digital genere nuevas oportunidades, evidentemente tenemos que acompañar esta promoción con medidas de protección. Estas medidas no deberían implantarse exclusivamente a petición de las propias empresas, sino que, igual que el sistema determina que hay ciertas reglas para actuar en el cibercomercio, en el comercio electrónico y en las relaciones de las empresas con los clientes —y eso después tiene que ver con unas contabilidades y unas rendiciones de cuentas—, el concepto de la ciberseguridad también debería ser más obligatorio o por lo menos que quien no quiera agregar medidas de ciberseguridad sea consciente de lo que está haciendo y de los riesgos que corre.

En la era de la comunicación, de las redes y de las oportunidades evidentemente existen riesgos, como estamos mencionando. Le quiero hacer algunas preguntas. De todas formas, hoy es un día en el que hemos aterrizado con el tema de los activistas rusos en Cataluña en todos los diarios. Ya nos despertamos con esto hace unos meses, viendo la capacidad e influencia que han tenido en Estados Unidos. Si partimos de la base de que la información es poder, de que hoy tenemos un *big data* que permite gestionar muchísimos datos de una manera muy potente, quisiera saber si también existe un sistema que pueda alterar esa información, convertirla en desinformación y meterla dentro del sistema, lo cual es un riesgo potencial muy grande porque puede cambiar opiniones públicas, puede cambiar la percepción de las personas sobre las cosas y, por tanto, tener efectos en el mundo real. Por ejemplo, una persona va a votar un día y va determinada a cambiar su voto o a apoyar algo que cree que es lo mejor, pero al final lo que ha habido es una sobredesinformación que ha terminado induciendo a hacer algo como si fuera una campaña de publicidad más. Por lo tanto, respecto a todo esto, le quiero preguntar si cree que existe una conciencia real al más alto nivel pero también al resto de niveles sobre las amenazas que representa el ciberdelito y los riesgos que estamos corriendo. Más allá de que en este momento esto esté de moda porque cuatro diarios y tres grandes presentadores lo metan en la agenda pública del país —esto debería ser cotidiano—, ¿entiende que contamos con los medios necesarios a nivel económico, no solamente ya con instrumentos, para poder afrontar este reto con garantías? Lo digo porque cuando hablamos de economía hablamos también de recortes y de que no hay que invertir en un sitio o en otro porque tenemos poco, pero este es un sector estratégico en el que nos estamos jugando, como usted ha dicho, todo lo demás: lo social, lo económico, incluso, como hemos visto, hasta la opinión pública. ¿Piensa que la estrategia de ciberseguridad actualmente diseñada en España da respuesta completa al conjunto de amenazas que estamos sufriendo en este momento? ¿Piensa que debería ser más flexible e ir retroalimentándose conforme se van produciendo este tipo de situaciones y, por tanto, ser algo mucho más vivo? ¿Existe una adecuada publicidad del conocimiento de Incibe para pymes y empresas? Esto ya lo he mencionado en otros ámbitos respecto al Centro para el Desarrollo Tecnológico Industrial, que es el que favorece la innovación en casi todas las empresas, pero si estas no lo conocen no lo pueden utilizar. Con Incibe pasa lo mismo. Si las pymes de nuestro país, si las empresas no tienen conocimiento de la importancia de Incibe en su propia capacidad y en que no corran riesgos, probablemente no lo utilizarán. Por tanto, quiero saber si usted está satisfecho o si cree que habría que hacer una campaña que exceda al propio Incibe, a nivel de Gobierno, para todas esas empresas, uniéndolo con el primer argumento, y obligar a que haya protección para que evitemos riesgos. También quiero saber si cree que el marco legislativo que actualmente tenemos en España es suficiente, si ese marco normativo, que se entronca en una legislación internacional y en este caso también, en lo que nos afecta más directamente, en la propia Unión Europea, nos cubre bien en ese ámbito o si cree que deberíamos profundizar y qué tipo de cambios piensa que se deberían hacer.

cve: DSCG-12-CM-65

Como anécdota y respecto al tema del anonimato, del que usted hablaba antes, le diré que yo personalmente lo he sufrido; he sufrido que una persona cree un correo electrónico sin ninguna identificación, que simule ser de una asociación en defensa de cosas muy sagradas y que lo mande a un montón de diputados, a partidos políticos y a mucha gente sin que nadie respondiera ante ello y con merma de la reputación, si eso fuera creíble. Evidentemente, lo primero que hice fue ir a la policía, presentar correos y, a partir de ahí, investigar de dónde venía la autoría. Eso, que me ha sucedido a mí que formo parte de esta Comisión, le podría suceder a cualquier ciudadano que en ese momento fuera menos conocedor de cómo puede ejercer sus derechos. Por eso le insisto en el tema de si serían necesarios cambios normativos, porque lo que yo he entendido y visto hay ciertas cosas que en un momento determinado, aunque exista una denuncia, pueden perder interés y ni siquiera en ese sentido seguir adelante. Por tanto, quiero mostrar este caso práctico y personal como un ejemplo de lo que creo que puede afectar al conjunto de los ciudadanos españoles.

Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señor Salvador.

Tiene ahora la palabra el senador Comorera.

El señor **COMORERA ESTARELLAS:** Muchas gracias, presidente.

Muchas gracias, señor Hernández, por su comparecencia hoy aquí y por la claridad de su exposición. Voy a pasar directamente a formularle una serie de preguntas porque me considero bastante lego en cuestiones de ciberseguridad; he estado leyendo mucho pero prefiero escucharle a usted. En primer lugar, voy a comentarle algunos datos que he visto al preparar su comparecencia y que me llaman la atención: la industria sanitaria sufrió el 26 % de los incidentes de seguridad producidos durante el segundo trimestre de 2017. Esto me parece muy preocupante, dada la naturaleza de los datos y la dependencia de los sistemas informáticos para ejecutar correctamente los flujos habituales del trabajo clínico. Me gustaría preguntarle qué tipo de medidas prevé al respecto el Incibe.

Otro dato preocupante en el que me he fijado es el del aumento del *malware* en los móviles. Así, por ejemplo, las infecciones a dispositivos móviles a nivel mundial aumentaron un 8 % en el segundo trimestre, con Asia liderando nuevamente la clasificación con un 18 %. Entre los métodos de fraude más habituales se encuentra el de obtener dinero ilegal mediante los programas maliciosos móviles, con el típico —eso es más antiguo— envío de los SMS a números premium, los troyanos o actualmente el *ransomware* móvil, que sigue su ascenso. También me gustaría saber qué tipo de medidas prevé el Incibe para luchar contra esta lacra.

Otro tema que me preocupa es el de la inversión en ciberseguridad, como ya ha comentado el senador Yanguas. Así, por ejemplo, he leído unas declaraciones del pasado mes de junio de don Enrique Cubeiro, jefe de operaciones del Mando Conjunto de Ciberdefensa, que manifestó que se invierte más en vallas que en ciberseguridad y preguntaba de dónde creen que vendrá el próximo ataque si de la valla o de un *firewall*. Creo que no se está respondiendo a esta amenaza ni con la agilidad ni con la contundencia que hacen falta y parece que estemos esperando a que pase algo más grave. Algunos datos: el Gobierno británico destina aproximadamente 2300 millones de euros a los programas de seguridad en Internet; Estados Unidos, 1500 millones de dólares; España, si no tengo malos datos, 24,3 millones de euros al Incibe y 161 al Centro Nacional de Inteligencia para reforzar la ciberseguridad. Le pregunto si tenemos un problema grave por la falta de inversión en ciberseguridad. Acogiéndome a sus palabras, ¿no debería aprovecharse precisamente esto como una oportunidad de crear empleo y desarrollo y, por tanto, invertir mucho más en ciberseguridad?

Otro dato preocupante es que han descendido los ciberataques *ransomware,* a pesar del WannaCry, a las grandes multinacionales y ahora se ceban más, por lo que he leído, en la pequeña y mediana empresa y hasta en autónomos, con el propósito de secuestrar sobre todo datos de clientes, proveedores y facturación, exigiendo rescates en *bitcoins.* Le hablo, por ejemplo, de Bad Rabbit, y algunos expertos comentan que posiblemente se continúe con usuarios particulares. ¿Qué medidas piensa implantar Incibe para adaptarse a este cambio de tendencia de los cibercriminales?

También me gustaría que me explicara, si es posible, qué participación —si es que ha tenido alguna— ha tenido el Incibe en lo que se llamó la crisis de Lexnet y la investigación de unos accesos no autorizados que se produjeron, por las últimas noticias que han salido esta última semana en prensa, sobre descarga de escritos y documentos. También llevamos días oyendo, en relación con el tema de Cataluña, ataques de Anonymous a webs de poderes del Estado, como el Tribunal Constitucional, la Casa Real o el Ministerio

cve: DSCG-12-CM-65

de Justicia, y sobre la referida injerencia de *hacker* rusos o venezolanos. ¿Qué nos puede contar sobre esto, si nos puede contar alguna cosa? ¿Han supuesto estos ataques realmente algún riesgo para tales instituciones? Me gustaría que me explicara un poco si hay algún tipo de diferenciación, porque lo que tenemos más que nada es desinformación. Hablamos de *hacker* rusos, venezolanos, etcétera, pero nos gustaría que nos explicara, al menos a los que somos más legos en todo esto, si entendemos como un ataque de ciberseguridad determinada desinformación, si realmente existe, y quién determina que esa información publicada por medios rusos es o no veraz. Quería saber su opinión sobre todo este tema.

Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, senador.

Tiene ahora la palabra, por el Grupo Socialista, el senador Raffo.

El señor **RAFFO CAMARILLO:** Muchas gracias, presidente.

En primer lugar, quiero agradecer la presencia del director general del Incibe. En unas circunstancias como las actuales es muy difícil abstraerse de lo que probablemente haya sido la crisis de seguridad más importante que ha tenido nuestro país en los últimos cuarenta años, en el sentido de su estabilidad política conectada con la situación de crisis económica y social, agravada por esa circunstancia que ahora mencionaré, que creo que todos conocemos, y a cuya información hemos tenido posibilidad de acceder a través de un medio público de nuestro país que se considera —creo que todos coincidiremos— serio, no estamos hablando de páginas web raras que aparecen en ningún sitio extraño del ciberespacio. Lógicamente, como representantes de la ciudadanía, vamos a centrarnos exactamente ahí. No obstante, queremos agradecer la información que se nos ha facilitado que, junto con todas las comparecencias que quedan pendientes, nos va a ir ayudando a conformar el conocimiento y una visión mucho más clara de ante qué tipo de problemas estamos, por otro lado, problemas complejos en un contexto muy complejo, en un mundo en tránsito, cambiante, de una gran incertidumbre que evoluciona de la bipolaridad en cuanto a la hegemonía política a nivel mundial a la multipolaridad y la lucha por esa hegemonía política. A nadie se nos escapa que en la región europea existen una serie de conflictos en los que España, por formar parte de la Unión Europea y de la OTAN, se encuentra inmersa y que ha sufrido probablemente, si esas informaciones son ciertas, un ataque claro de una de las partes que se pueden considerar como adversario en las circunstancias actuales que estamos mencionando. Nosotros consideramos que esa gravedad precisamente es la que lleva a que prioricemos algunos comentarios y algunas reflexiones. La existencia del ciberespacio, que es propia y coincidente con esta situación de crisis económica, social, política, institucional, de falta de crédito, de liderazgos políticos e incluso sociales, de liderazgos institucionales, facilita un nuevo espacio, como he mencionado, para lo que es, digamos, el campo de batalla del siglo XXI. Nosotros consideramos, por la información que hemos recibido, que parece ser que, procedente —procedente, no sabemos si con respaldo de poderes públicos o no— de Venezuela y de Rusia ha habido una coincidencia en participar en el descrédito de las instituciones, de los liderazgos políticos y también del tránsito de la mentira a través del ciberespacio, algo que ha restado mucho crédito a nuestro país. Yo no voy a hablar de la marca España, hablo del país, de los valores de nuestro país, de nuestra posición estratégica como país serio y sólido en su sistema democrático.

El formato de conflicto que se plantea es una línea muy difusa entre lo que es el extremo de la competencia cotidiana entre los países en situaciones de paz y lo que es la guerra total clásica, como fueron la Primera y la Segunda guerras mundiales. Después de la caída del bloque del Este todo esto ha cambiado muchísimo y, como he mencionado anteriormente, se ha incorporado todo el desarrollo de las nuevas tecnologías, las TIC, Internet, etcétera. Esa zona denominada zona gris incorpora lo que hoy en día se viene a denominar la guerra híbrida, el método híbrido, la guerra de las sombras, el conflicto híbrido —no son palabras mías, son palabras de expertos y profesionales en la materia—. Voy a leer una frase. Me habría gustado encontrar la de un responsable militar de otro país, pero en este caso casualmente es ruso. Habla de que en la guerra híbrida el factor de más relevancia es la guerra informativa. Dice: «Hay que prestar una atención especial al que es el elemento esencial de los métodos híbridos. La falsificación de acontecimientos, la limitación de la actividad de los medios de información se convierten en uno de los métodos asimétricos más eficaces para la conducción de las guerras. Su efecto puede ser comparable a los resultados de un uso masivo de tropas». Esto lo dice un general de Estado Mayor del Ejército ruso, tampoco lo digo yo. No estoy diciendo con esto ni dando por hecho que los poderes públicos de la ex Unión Soviética, hoy día Rusia o Federación Rusa, estén detrás de los acontecimientos de Cataluña, pero es evidente que el desarrollo tecnológico también ha llegado allí y que existen conflictos que nos llegan y

cve: DSCG-12-CM-65

nos alcanzan de cerca por nuestra pertenencia a dos organizaciones multinacionales como la OTAN y la Unión Europea.

Esta famosa guerra híbrida, que se caracteriza porque es poliédrica, multidimensional, tiene como elemento nuclear precisamente lo que es la guerra informativa —insisto, tampoco lo digo yo sino profesionales de gran prestigio y capacidad de liderazgo en lo que son sus propios espacios de desarrollo profesional—. Hoy día consideramos que tenemos —a modo de un DAFO simplificado— debilidades y amenazas que dependiendo de cómo se gestionen se pueden convertir en fortalezas y oportunidades. ¿Cuál es la amenaza o la debilidad más importante que podemos tener dentro de lo que es el núcleo de potenciales adversarios? Pues que si uno mira, son sistemas poco democráticos o nada democráticos a los que por tanto caracteriza una gran capacidad de movimiento al no tener contrapesos institucionales ni de desarrollo de sociedad civil, con una gran rapidez y agilidad en las decisiones y las acciones que hay que tomar. En las democracias, como es el caso de nuestro país —insisto, democracia en profundidad y con solidez—, existen contrapesos institucionales y también de la sociedad civil, y en libertad, como no podía ser de otra manera en democracia, los grupos se organizan, también con nuevas tecnologías, para dar dimensión a lo que son sus legítimas aspiraciones a la búsqueda de resolver sus necesidades y sus propios conflictos. Esos objetivos o necesidades algunas veces son coincidentes con adversarios de estos países democráticos, que podría ser el caso —no digo que lo sea, pero podría—, y ocurre que no tenemos tanta capacidad en la agilidad ni en la rapidez de las decisiones y tampoco en responder a la necesidad de la búsqueda de consenso rápido, lo cual es una limitación. Teniendo en cuenta esto, es cierto que nos estamos adelantando. ¿Cómo responder en esta situación de un mundo de incertidumbre y de inestabilidad? Este sería el gran interrogante en las circunstancias que tan de cerca hemos vivido recientemente en nuestro país. Tenemos leyes, informes, planes estratégicos, organización, nuevos recursos tecnológicos, un nivel de formación profesional importante, investigación, formación, con las limitaciones propias de lo que puedan ser las capacidades presupuestarias. Es más, las claves del éxito son las capacidades de previsión y anticipación para aventajar a los adversarios. Según su opinión, ¿qué elementos o medidas sería deseable priorizar para mejorar estas capacidades? En este sentido, me gustaría adelantar que ante estas experiencias recientes y nuestra gran preocupación por los hechos ocurridos el Grupo Socialista va a solicitar a través de una PNL que desde el Gobierno se impulse, fruto de un análisis y un diagnóstico riguroso y en profundidad, la mejora de los recursos tecnológicos, materiales y humanos para tener mayor capacidad, mayor rapidez, porque sinceramente la batalla online y del ciberespacio en ese primer periodo —creo que todos estaremos de acuerdo— la hemos perdido. Sin llevar la iniciativa, hemos tenido que lograr una recuperación que cuesta bastante trabajo, pero si hubiéramos tenido más capacidad, decisiones rápidas y agilidad en las respuestas, probablemente no habría tenido un costo tan elevado.

También queremos solicitar varias peticiones de comparecencia, y queremos avanzar al menos dos de ellas. Si es posible, nos gustaría que estuviese el responsable del departamento East Stratcom Task Force y el responsable de la OTAN de ciberdefensa. También, la señora Mira Milosevich-Juaristi, investigadora del Instituto Elcano.

Muchas gracias, señor presidente, y gracias también al señor compareciente. En la segunda tanda probablemente incorporaremos algún elemento más.

El señor **PRESIDENTE:** Muchas gracias, señor senador. Tomo nota de las peticiones que ha formulado. Precisamente en la documentación que será repartida hay dos documentos del Instituto Elcano que han sido elaborados por una de las personas cuya comparecencia acaba de solicitar.

Para terminar esta primera ronda, tiene la palabra la portavoz del Grupo Parlamentario Popular, señora Vázquez.

La señora **VÁZQUEZ BLANCO:** Muchísimas gracias, señor presidente.

Agradezco la intervención de don Alberto Hernández, director general del Incibe, en esta Comisión. La verdad es que ha sido muy explícito. Nos ha facilitado toda la información que necesitamos para ir preparando el informe de esta ponencia sobre ciberseguridad. La verdad es que en esta Comisión algunas veces vamos por delante de los acontecimientos. Cuando todavía no se había producido ese ataque masivo a nuestras empresas, dos semanas antes, en esta Comisión, con la Mesa y portavoces, ya habíamos acordado crear esta ponencia. Consideramos que la cibercriminalidad va al mismo tiempo que los avances de la sociedad; a medida que se avanza para lo bueno, también avanzan los malos. Consideramos que el trabajo que está realizando el Incibe es inmenso. Si no llega a ser por la labor que

cve: DSCG-12-CM-65

está haciendo el Incibe posiblemente no serían incidentes, serían ataques mucho más agresivos y preocupantes. Nosotros estamos estos días, como todos, perplejos: cómo un individuo desde la Embajada de Ecuador puede remitir cuarenta mil mensajes sobre la situación secesionista en Cataluña, cómo un 55 % de esos mensajes, con mentiras sobre las cargas policiales y lo que ha sucedido durante esos días, puede venir de territorios ajenos, como Rusia, otro 30 % desde Venezuela, etcétera. Y nosotros aquí, en España, nos estábamos creyendo parte de esos mensajes que se trasladan. La injerencia es brutal, no solo con las empresas, que es a lo que se dedica el Incibe, a particulares, sino con la propia estructura del Estado y de la Unión Europea. Como usted decía, este es un desafío global, internacional, mundial; el propio presidente del Gobierno así lo trasladó a la Unión Europea recientemente al mostrar su preocupación por defendernos de los ciberataques. Han tenido injerencias con el *brexit*, han tenido injerencias en Francia, y esperemos que haya tranquilidad de cara a las elecciones del 21 de diciembre. Sabiendo ya lo que sabemos, espero que muchos españoles cuando vean ciertos mensajes de ciertos individuos, de ciberactivistas que se dedican a romper las estructuras de los Estados, no se los crean de primeras y hagan una valoración de lo que es cierto y lo que no es cierto.

Nosotros necesitamos la colaboración internacional. Yo no sabía que efectivamente se estaba colaborando en Alerta Temprana con países como Estados Unidos; me parece que esa colaboración es importantísima. En cuanto a ese desafío al que usted nos remite, a la posible creación de 1 o 2 millones de puestos de trabajo que se van a necesitar en materia de talento en ciberseguridad, ahora son 6500 empleos en España, pero se van a necesitar muchos más empleos en esta materia. Viendo las cifras, que yo me las apunté porque me parecen increíbles, usted hablaba de que pasamos de 50 000 incidentes en 2015 a 115 000 en 2016, es decir, se triplican año a año los incidentes en ciberseguridad. La verdad es que son datos que nos alarman mucho.

Le voy a hacer algunas preguntas, porque como esta es una ponencia de estudio, y nosotros necesitamos información para después hacer el informe, a las que espero me pueda responder porque ya sabemos que hay cosas que no se pueden responder. ¿Considera que el Incibe dispone de medios económicos adecuados para realizar sus funciones en materia de prestación de servicios a pymes con el nivel de conocimiento tecnológico actual? ¿Cómo evalúa la disponibilidad de talento especializado en su instituto? ¿Cree que cuenta con los suficientes medios humanos para acometer las tareas que tiene encomendadas el Incibe en estos momentos? ¿Considera que se están usando los canales adecuados —creo que esto ya nos lo ha explicado bien— para diseminar la información de ciberseguridad con las pymes? Esta pregunta la puedo retirar porque usted me la ha respondido ya en su exposición. No sabía que efectivamente se alertaba ya a los proveedores de comunicaciones. Por tanto, esta pregunta la retiro. ¿Cómo evalúa la incidencia de sus campañas de concienciación en el sector pyme? Porque he visto que tienen bastantes campañas en marcha. ¿Considera que los modos de acceso a la red por parte de nuestras pymes se encuentran adecuadamente protegidos? ¿Tienen a lo mejor las pymes que incrementar también su protección? No siempre el padre Estado es el que tiene que poner de su parte, sino que a lo mejor puede dar alguna recomendación para las pymes. ¿Cree que sería deseable ofrecer a nuestras pymes servicios automatizados de detección y respuesta de actividades maliciosas con la implantación de sondas?

Este dato lo desconozco, ¿existe en España —sé que no tiene que ver con el Incibe— algún servicio de contrainformación o contraprogramación respecto a los ciberataques que recibimos? Usted antes hablaba del tipo de empleos que se necesitan: periodistas, pedagogos y psicólogos. ¿Tenemos en este momento cómo parar esas campañas que nos puedan venir desde el exterior? ¿Existe algo? Porque no lo sé.

A título personal cogí el guante del Centro Nacional de Excelencia de Ciberseguridad de crear reservistas en ciberseguridad, gente que disponga de su tiempo. Sin perjudicar los empleos que se puedan crear, si en un momento dado alguien tiene los conocimientos suficientes para poder colaborar con el Estado con disponibilidad absoluta como se hace en las reservas del ejército, ¿usted cree que sería bueno o no contar con gente que de manera altruista o no tan altruista se pueda poner a disposición del Estado en un momento dado?

Muchísimas gracias por su información.

El señor **PRESIDENTE:** Muchas gracias, señora Vázquez.

Voy a dar la palabra ahora al compareciente para dar satisfacción a los que han interrogado en esta primera ronda.

Tiene la palabra.

cve: DSCG-12-CM-65

El señor **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD, S.A., INCIBE** (Hernández Moreno): Muchas gracias, presidente.

Muchas gracias por las preguntas. Empezando por el señor Yanguas, me gustaría decir que las leyes y normativas de ciberseguridad que tenemos en nuestro país son buenas, están funcionando y están surtiendo efectos positivos y una de ellas es la Ley Orgánica de Protección de Datos, que, como sabemos, está impulsada también en el ámbito de la Unión Europea. De hecho, uno de los pilares fundamentales para mejorar la ciberseguridad de ciudadanos, empresas y también, por supuesto, administraciones públicas es tener una legislación adecuada. Tenemos un Código Penal actualizado que recoge la figura del ciberdelito, es bastante completo, y yo creo que ese es el camino, seguir manteniendo y actualizando las leyes. Creo que a día de hoy estamos en una disposición buena.

Además, con el marco legal y jurídico que tenemos, contamos con un marco adecuado en el que podemos trabajar en el desarrollo de iniciativas de ciberseguridad. ¿Estamos preparados para ataques masivos? Al principio de mi intervención compartía con ustedes que desde el Centro de respuesta ante incidentes de seguridad e industria llevamos gestionados más de 700 incidentes que han afectado a operadores estratégicos o críticos, algunos de los cuales pueden estar gestionando una infraestructura crítica. Eso no significa que esos incidentes hayan llegado a afectar a la propia infraestructura, pero sí pone de relieve que se están produciendo incidentes en empresas y organizaciones importantes de nuestro país, pero que han tenido un impacto mínimo. De hecho, si miramos en los medios de comunicación y tiramos de hemeroteca, podemos ver que no ha habido un impacto importante. La pregunta no es si vamos a sufrir ciberataques en nuestras empresas o en nuestras organizaciones porque esa pregunta está contestada, sí los vamos a seguir sufriendo y probablemente más, la pregunta es si vamos a estar adecuadamente protegidos.

En el ámbito de las leyes sabemos que tenemos desde hace varios años la Ley de protección de infraestructuras críticas. Se constituyó el Centro Nacional de Protección de Infraestructuras Críticas. Tenemos un real decreto que desarrolla esa ley. España, además, es un referente en este ámbito a nivel internacional y muchos países —lo adelantaba en mi intervención inicial— están utilizando como modelo las leyes que hemos desarrollado y aprobado en nuestro país para desarrollar modelos similares. Por tanto, está funcionando bien la aplicación de las leyes que tenemos y los organismos y los instrumentos que tenemos para ponerlas en marcha y aplicarlas.

En cuanto a posibilidades de ataque masivo, me gustaría volver atrás y recordar el año 2007, año en el que un país, Estonia, sufrió un ataque masivo y mantuvo al país bloqueado durante varias semanas. Fue un ataque que se derivó de un conflicto social-político y que produjo ciberataques que afectaron fundamentalmente a los sistemas financieros y también, por supuesto, propaganda modificando páginas web del Gobierno y de políticos de aquel país. Ya hemos visto en la historia que existe el riesgo de sufrir ataques masivos. La cuestión es que eso lo tenemos en la mente, en nuestro plan de trabajo y lo importante es estar adecuadamente preparados para, si ese momento ocurre, poder detectarlo lo antes posible y poder responder en el menor tiempo posible y que nuestras organizaciones sean resilientes. De hecho, desde Incibe desarrollamos el pasado año 2015 un modelo de indicadores de resiliencia en el ámbito de la ciberseguridad con el objetivo de que nuestras organizaciones estratégicas tengan la capacidad de medir qué nivel de resiliencia tienen ante un ciberataque de alto impacto y la capacidad de recuperarse. Ese modelo se ha venido aplicando y puedo decir que este año el modelo se ha aplicado a más de setenta organizaciones. Esto permite, por un lado, saber el nivel de resiliencia, que ha mejorado respecto al año anterior y es un nivel alto, y por otro lado, dar un instrumento a las organizaciones para la automejora.

Me decía el señor Yanguas que se han duplicado los incidentes, y eso es cierto, y me hablaba del origen. En cuanto a la atribución, tal como comentaba en mi intervención inicial, es una de las características fundamentales del ciberespacio, es decir, la facilidad de mantener el anonimato en cualquier tipo de acción. Por tanto, determinar la atribución de una acción requiere de una aproximación holística, requiere de una aproximación que tenga en cuenta más parámetros además de los parámetros técnicos que podemos manejar desde los organismos como Incibe que trabajamos desde un punto de vista técnico.

Como decía, cuando España sufre un incidente, sufre un ciberataque, normalmente se ha producido a miles de kilómetros de distancia, ha pasado varios saltos, es decir, ha vulnerado e infectado sistemas de varios países antes de llegar al nuestro. En el proceso de investigación nosotros empezamos a ver cuál es el salto más cercano a España y ahí podemos tener una orientación de con quién tenemos que hablar

cve: DSCG-12-CM-65

en el otro lado, con qué país, para seguir en el proceso de investigación. A partir de ahí, aparecen problemas, dificultades que tienen que ver con las características del ciberespacio, porque, como decía, la tecnología permite el anonimato, cifrar las comunicaciones y, además, las diferentes leyes y normativas que se aplican en cada país facilitan en mayor o menor medida avanzar en esa investigación. Por tanto, poder determinar la atribución de un ciberataque requiere de información mucho más allá que la que es puramente técnica y que puede manejar un centro de respuesta o un centro técnico como es Incibe.

En cuanto a personal y presupuesto, puedo decir que Incibe este año ha venido dotado con el mayor presupuesto de la historia de la entidad. Se ha producido un incremento presupuestario significativo y, además, tenemos la aprobación y estamos en ello en este momento, en la incorporación de veintisiete personas a la organización, lo que supone un 23 % de incremento de personal. Es un dato muy positivo y también hay que tener en cuenta que, para que una organización pueda absorber un incremento de personal, hay un límite. Es decir, podemos incorporar cierta cantidad de personas cada cierto tiempo, pero no podemos hacer una incorporación masiva. Creo que es un dato muy positivo y que refleja el compromiso y el esfuerzo que estamos haciendo en la mejora de la protección de nuestros ciudadanos y de nuestras empresas.

Para terminar con sus preguntas, señor Yanguas, en el año 2012, en la Secretaria de Estado —en aquel momento de Telecomunicaciones y para la Sociedad de la Información y en este momento Secretaría de Estado para la Sociedad de la Información y la Agenda Digital— suscribí un acuerdo de colaboración con la Secretaría de Estado de Seguridad del Ministerio del Interior para colaborar en la lucha del ciberdelito en tres ámbitos de actuación. En primer lugar, en el apoyo al Centro Nacional de Protección de Infraestructuras Críticas, en la protección de las infraestructuras críticas en el ámbito de la ciberseguridad y, como resultado de esa colaboración, hemos implementado desde los indicadores de ciberresiliencia, los ciberejercicios con los operadores críticos, guías de configuración, buenas prácticas, apoyo, consultoría y apoyo en la respuesta. Por lo tanto, hemos estado trabajando en la protección de las infraestructuras críticas. También, en el marco de ese convenio con el Ministerio del Interior, trabajamos en el apoyo en la capacitación y en el adiestramiento de las Fuerzas y Cuerpos de Seguridad. De hecho, a la iniciativa Summer BootCamp han venido no solo Guardia Civil y Policía Nacional, sino también policías autonómicas. Por tanto, esa colaboración a través del Ministerio del Interior está llegando. La vocación de Incibe no es solamente trabajar de una forma directa con cada uno de los cuerpos policiales, sino también a través del Ministerio del Interior, dándole herramientas tecnológicas que permitan a todas las unidades luchar contra el ciberdelito y avanzar en la investigación.

Respecto a las preguntas del señor Salvador, de Ciudadanos, me gustaría empezar hablando de la obligatoriedad que establece la ley de que las empresas incorporen mecanismos de seguridad. Como decía previamente, en contestación a las preguntas del señor Yanguas, es muy importante no solo que las empresas estén concienciadas, sino también que estén obligadas a incorporar mecanismos de seguridad, al igual que están obligadas a día de hoy en ciertos procesos a incorporar certificaciones de calidad o certificación de la gestión de la ciberseguridad o que estén conformes al reglamento de protección de datos. Por lo tanto, creo que el establecimiento de mecanismos de certificación de productos, servicios y procesos en las organizaciones es una línea de acción por la que debemos apostar y de hecho puedo decir que estamos trabajando en ella. La reciente publicación en el mes de septiembre en el paquete legislativo de impulso de la ciberseguridad, dentro de la Unión Europea, que además dota a Enisa de nuevas competencias en el ámbito de la ciberseguridad, va por ese camino. En ese paquete legislativo y en las competencias de Enisa, de la Agencia Europea de Seguridad de las Redes y de la Información, se propone la necesidad de establecer una certificación europea que mejore la seguridad fundamentalmente de los dispositivos de Internet de las cosas, pero también de los procesos y de las organizaciones.

Como decía en mi intervención inicial, vamos a ver un escenario en los próximos años en el que tendremos millones de dispositivos conectados a Internet y esos dispositivos tienen que ser seguros. Es verdad que los ciudadanos y las empresas tienen una responsabilidad en el uso seguro de los mismos, pero es igualmente cierto que los fabricantes y los productores tienen que desarrollar los productos conforme a estándares de seguridad, lo que los que trabajamos en este campo llamamos seguridad por diseño. Por lo tanto, trabajaremos en el marco europeo en el desarrollo de estos estándares, buenas prácticas y garantías de ciberseguridad para que se incorporen en el desarrollo de productos, servicios y en las propias empresas, independientemente de su tamaño. Si bien es importante que, como decía, el segundo aspecto que tenemos que tener en cuenta en el ámbito de la ciberseguridad es la oportunidad para el desarrollo de nuestras empresas. Sabemos que el tejido empresarial de nuestro país, en cuanto a

cve: DSCG-12-CM-65

tamaño de las empresas —y hablamos del 90 %, que son pequeñas y medianas empresas— y en cuanto al número de empresas de ciberseguridad, es pequeño, en tamaño y número, en las dos cosas. Por lo tanto, tendremos que ir hacia estándares de certificación ligeros que permitan facilidad de incorporación por nuestras empresas y que no supongan una barrera para que nuestras empresas se desarrollen en este nuevo mercado. Tienen que ser estándares de certificación que mejoren la ciberseguridad y que, por otro lado, faciliten el desarrollo industrial de nuestro país.

En cuanto a la desinformación y las nuevas amenazas, como decía anteriormente, estamos ante un escenario en el que todas las amenazas, absolutamente todas las amenazas que podemos identificar e imaginar en el mundo físico, insisto, todas y cada una de ellas, pueden tener una materialización en el ciberespacio. ¿Por qué? Porque es un entorno global, porque es asimétrico, porque cualquier acción que se desarrolla a miles de kilómetros puede ser difícil de atribuir a una organización o a un Estado y puede tener un impacto elevado por la asimetría. Por lo tanto, las estrategias que tenemos que abordar y que estamos abordando, las que tenemos en marcha nos llevan a todos los organismos que trabajamos en el ámbito de la ciberseguridad a analizar la amenaza, el estado de la amenaza. Las amenazas están identificadas; es la forma en la que la amenaza se materializa la que está sufriendo transformaciones de forma continua, aprovechando el desarrollo tecnológico. Todos los organismos públicos que trabajamos en este ámbito y en el ámbito que nos ocupa a Incibe, ciudadanos y empresas, analizamos la amenaza de forma continua y además —y es muy importante— la probabilidad de que esta amenaza tenga una materialización, puesto que la unión de la amenaza, la vulnerabilidad que pueden presentar las tecnologías y la probabilidad nos va a dar el nivel de riesgo al que están sometidos nuestros ciudadanos y nuestras empresas, y es sobre el nivel de riesgo sobre el que tenemos que actuar. Tenemos que trabajar en la implementación de medidas de ciberseguridad que reduzcan ese riesgo de que una amenaza que siempre estará ahí se materialice y tenga un impacto significativo en nuestras empresas y en nuestros ciudadanos.

Para gestionar el riesgo, y como introducía inicialmente, contamos con un conjunto de medidas que van desde la concienciación de los propios ciudadanos y de las empresas hasta la formación, la colaboración internacional, proporcionando además herramientas gratuitas, guías de configuración, adiestramiento a las empresas en nuestro país. En ese sentido, si la concienciación en nuestros ciudadanos y nuestras empresas es real, nosotros consideramos que la crisis de WannaCry —que puedo decir que afectó a menos de diez empresas estratégicas en nuestro país, es decir tuvo un incidente de bajo impacto— fue una crisis muy mediática porque fue la primera vez en nuestro país —no en otros países; como decía, en Estonia— que todos los ciudadanos estuvieron viendo durante el fin de semana por los medios de comunicación que un incidente de ciberseguridad se estaba convirtiendo en una crisis nacional y mundial. Entendemos que la crisis de WannaCry ha supuesto un antes y un después en la toma de conciencia por parte de nuestros ciudadanos y, por lo tanto, en su desarrollo en el ámbito profesional de que la ciberseguridad es un asunto de todos. Si bien es cierto que, desde mi punto de vista, la concienciación pasa por varios niveles diferentes.

El primero de ellos es la toma de conciencia de que existe un problema. Yo creo que podemos decir que en nuestro país nuestros ciudadanos y nuestras empresas saben que la ciberseguridad es un reto. El segundo es entender en qué consiste, y creo que en eso es en lo que estamos trabajando intensamente ahora. Es decir, los ciudadanos saben que la ciberseguridad es un reto, pero tienen que entender en qué consiste, tienen que entender qué pueden hacer para mejorar la ciberseguridad y, por último, y muy importante, tienen que interiorizarla, o sea, tienen que adquirir de forma repetitiva y automática ciertas conductas de ciberseguridad. Si pensamos que cada vez que entramos en un coche nos ponemos el cinturón de seguridad, en el ámbito de la ciberseguridad ocurre lo mismo, tenemos que conseguir que nuestros ciudadanos entiendan y automaticen las medidas de seguridad. A nivel internacional, y cuando hablamos con nuestros homólogos, la situación es la misma en todos los países, es decir, el desarrollo tecnológico va tan rápido, estamos utilizando las tecnologías de una forma tan rápida, que nuestro nivel de concienciación va un poco por detrás. Estamos trabajando y además de forma conjunta en ese sentido.

En cuanto a la estrategia de ciberseguridad, desde mi punto de vista, tenemos una estrategia de ciberseguridad que por supuesto será actualizada en el futuro, pero creo que es bastante completa, que establece las prioridades, los objetivos y las líneas de acción que tenemos que ocupar en nuestro país. Además, países que están desarrollándola ahora, la están utilizando como referencia. Como decía, hay varios países latinoamericanos a los que estamos apoyando a desarrollar estrategias y están utilizando la estrategia española.

cve: DSCG-12-CM-65

Si bien es importante una estrategia que marque los objetivos, que identifique la amenaza, como decía, es la forma en que la amenaza se materializa la que cambia continuamente. Por lo tanto, son muy importantes los instrumentos de todo tipo —incluidos los técnicos— que tengamos en marcha para poder adaptarnos a esa nueva forma de materialización de la ciberamenaza. Un ejemplo de ello son los servicios que prestamos desde Incibe y los equipos que tenemos, es decir, estamos gestionando continuamente, como decía, cientos de incidentes de ciberseguridad que se están materializando de forma diferente. Incidentes como WannaCry se producían anteriormente recibiendo un correo electrónico, que suplantaba la identidad de un proveedor de energía, de un banco, de una entidad conocida, y al abrirlo nos infectaba. El objetivo, la amenaza, tiene que ver con el robo de credenciales bancarias, de tarjetas de crédito para robar dinero. Esto evoluciona y estamos empezando a ver que ya no se hace a través de correos electrónicos, sino que se intenta entrar a través de vulnerabilidades que están sin corregir en las redes de las empresas. El objetivo sigue siendo el mismo, la amenaza sigue siendo la misma, la forma de materializarse cambia. Por tanto, tenemos que actuar en eso, en trabajar para concienciar en cómo mitigarlo.

Puedo decirles —y también es un aspecto importante— que si bien la tecnología cambia muy rápido, la forma de protegernos no ha cambiado tanto. Si miramos atrás, las recomendaciones que estábamos dando a nuestros ciudadanos y a nuestras empresas para que se protegiesen y que tienen que ver con tener los sistemas actualizados, con tener un antivirus, con desconfiar de lo que le llega que no conoce, siguen siendo igual de válidas a día de hoy. Si miramos a WannaCry, mayo del año 2017, WannaCry utilizaba para materializarse una vulnerabilidad para la que ya existía una actualización; por lo tanto, todo aquel que hubiese implementado la actualización previamente no era vulnerable.

Respecto a las pymes, estamos trabajando intensamente para ellas, pero tenemos que seguir haciéndolo. Nuestra percepción en este momento es que el nivel de conciencia del reto ya existe, por lo que tenemos que seguir trabajando en que lo entiendan y lo automaticen. Además, una parte importante, y por lo que me han preguntado, es que esto supone un coste. La ciberseguridad supone un coste, igual que la seguridad de una empresa cuando hablamos de seguridad física, es decir, alarmas, seguridad privada. La ciberseguridad supone un coste. Quizás esta sea una de las barreras de mejora de la ciberseguridad en el entorno empresarial. Los empresarios tienen que ver que la ciberseguridad supone un coste a sus operaciones, pero, por otro lado, la tecnología les está dando una ventaja en la mejora de sus procesos productivos y en la mejora de sus servicios. Es importante —y lo estamos diciendo en las campañas de concienciación— que en el caso de que haya un incidente se denuncie a las Fuerzas y Cuerpos de Seguridad. Esta parte es muy importante, puesto que desde el Instituto Nacional de Ciberseguridad, el Incibe, nosotros brindamos respuesta para contener el ciberataque, damos recomendaciones de prevención, pero la persecución del primer delito corresponde a las Fuerzas y Cuerpos de Seguridad. Trabajamos intensamente con el Ministerio del Interior, con la Secretaría de Estado de Seguridad, con las Fuerzas y Cuerpos de Seguridad en la lucha contra el ciberdelito dándoles herramientas y, por supuesto, proporcionándoles aquella información técnica que hemos obtenido a la hora de identificar el incidente y a la hora de brindar respuesta y apoyo a los ciudadanos y empresas afectados.

Paso ahora a las preguntas del señor Comorera. Los incidentes dirigidos a los diferentes sectores industriales dependen de diferentes parámetros. Hay sectores que han incorporado la tecnología de una forma más rápida, han encontrado una ventaja mucho mayor en la incorporación de la tecnología, como puede ser el sector sanitario, pero hay otros sectores que están yendo detrás, que están incorporando la tecnología poco a poco en los procesos industriales —como, por ejemplo, en la industria 4.0— pero, sin lugar a dudas, absolutamente todos los sectores van a ir hacia una conectividad intensiva a Internet y el uso intenso de las tecnologías.

En cuanto a la industria de sanidad, el año pasado realizamos un análisis de las tendencias de ciberseguridad para los próximos años que podían tener una materialización importante en nuestro país, entre las cuales identificamos diecisiete tendencias. Varias de ellas tenían que ver con el entorno sanitario y tienen que ver con la protección de los datos del paciente, la protección de la integridad y confidencialidad de los datos del paciente, así como la protección de los propios dispositivos tecnológicos que se utilizan en las diferentes intervenciones quirúrgicas y pruebas diagnósticas en el ámbito de la ciberseguridad. La tecnología está disponible, la forma de implementarla también y sabemos que, además, en el ámbito público y privado se está trabajando en la mejora de la ciberseguridad de estos entornos.

cve: DSCG-12-CM-65

Respecto a los dispositivos móviles, es cierto que se está produciendo un incremento de los dispositivos conectados a Internet en el ámbito de los dispositivos móviles y también es cierto que la conciencia en el ámbito de la ciberseguridad cuando hablamos de las redes corporativas o del ordenador que tenemos en casa es mayor que la que tenemos cuando utilizamos un dispositivo móvil. Son muchas las ocasiones en las que estudiamos y preguntamos qué nivel de seguridad tiene una empresa respecto a sus redes corporativas y respecto a sus dispositivos móviles y nos encontramos una diferencia importante. Se ha puesto el foco en los sistemas tradicionales y no tanto en los dispositivos móviles. Estamos trabajando intensamente en el campo de los dispositivos móviles en varios puntos. Me gustaría compartir con ustedes que desde hace dos años tenemos disponible de forma gratuita una aplicación para dispositivos móviles con el sistema operativo Android —que supone más del 90 % del parque de dispositivos móviles de nuestro país—, aplicación gratuita que permite al ciudadano analizar la seguridad del dispositivo móvil, es decir, qué nivel de seguridad tiene a nivel de configuración, qué aplicaciones pueden contener contenido malicioso y la posibilidad que estamos dando a aplicaciones para que accedan a datos personales. En estos dos años hemos tenido más de 100 000 descargas de esta aplicación y estamos trabajando a nivel internacional para que esté disponible en *markets* internacionales. En las campañas de comunicación que tenemos previstas para los próximos años tenemos incorporadas recomendaciones, buenas prácticas y mensajes para los ciudadanos en el ámbito de las comunicaciones y dispositivos móviles. Respecto a la inversión en ciberseguridad, quiero recalcar de nuevo el incremento de la ciberseguridad que se ha producido en Incibe.

En cuanto a la generación de empleo, es una parte importante. Como decía, según diferentes estudios va a haber una demanda no satisfecha de puestos de trabajo a nivel mundial de entre uno y dos millones de puestos. Hay una oportunidad de crear puestos de trabajo en nuestro país derivada de las inversiones que hagamos desde el ámbito público pero también desde el ámbito privado, por supuesto, pero hay una mayor oportunidad en el mercado mundial. Nuestras empresas venden internamente en el mercado español —mercado que se encuentra en torno a los 1000 y 1200 millones de euros y, como he dicho, con un crecimiento del 11 % al 13 %— pero realmente el mercado grande está fuera de nuestras fronteras y es un mercado global, en el que nuestras empresas pueden jugar un papel importante vendiendo productos y servicios a otros países. Entendemos que va a ser muy difícil poder cubrir ese millón o dos millones de puestos de trabajo puesto que la promoción del talento requiere de años. Estamos hablando de que tenemos que motivar a jóvenes de catorce y quince años y animarles a que estudien disciplinas relacionadas con esta materia para que cuando tengan veintidós, veintitrés o veinticuatro años se puedan incorporar a la industria. Por lo tanto, estamos aplicando medidas e iniciativas que tendrán una respuesta a medio y largo plazo. Esa necesidad de las empresas a nivel mundial de tener talento la tendrán que satisfacer mediante la contratación de servicios y productos a terceros, tendrán que ir al mercado a que sean otras empresas las que les proporcionen esos servicios y es ahí donde podemos jugar un papel importante, que nuestras empresas sean competitivas a nivel internacional y puedan prestar esos servicios y productos que no van a poder ser desarrollados internamente en las compañías con proyección mundial. Para terminar con sus preguntas, quiero reforzar el tema de la atribución. No es un aspecto únicamente técnico, es importante conjugar diferentes aspectos como a qué intereses puede responder una acción o a quién puede beneficiar en el panorama actual.

Pasaré a las preguntas del senador Raffo. Coincido con usted en el concepto de la amenaza, el conflicto y la amenaza híbrida. El ciberespacio puede ser utilizado como medio para materializar una amenaza que podría materializarse en el ámbito físico y además se podría materializar en los dos a la vez, como medio pero también se puede utilizar como fin. Es decir, sabemos que tenemos entidades u organizaciones que prestan servicios en Internet. Si se realiza un ataque a esos servicios, esas empresas verán perjudicada sustancialmente su operativa y, por lo tanto, su negocio. Efectivamente, estamos ante una amenaza híbrida, una amenaza híbrida con diferentes motivaciones. Yo he comentado que en el ámbito del ciudadano y del sector privado la motivación fundamental es económica. Eso es lo que motiva a las organizaciones criminales a ir a un ciudadano, el robo de información con el objetivo de robarle dinero o a atacar a una empresa con el objetivo de hacerle un perjuicio económico, robarle propiedad intelectual, robarle propiedad industrial, es decir, con una motivación económica. A día de hoy la tecnología ha llegado a todos los rincones del mundo, no es un asunto exclusivo de los países más desarrollados. Cualquier ciudadano, cualquier organización, cualquier país que tenga una conexión y un dispositivo móvil —hablaba anteriormente de menos de 100 euros— está conectado a Internet y ha entrado por una puerta abierta a los sistemas de todos los países. Por tanto —esto refuerza la necesidad de trabajar en la

cve: DSCG-12-CM-65

colaboración internacional— es necesario trabajar intensamente para nuestra seguridad nacional con el resto de países en mejorar sus capacidades de ciberseguridad. Ciertamente nos encontramos ante un entorno que presenta unas características especiales, que es global, que no existen fronteras y ningún país tiene un control del mismo, por lo que tenemos que trabajar con esas características. Forma parte del reto de seguridad nacional que tenemos por delante. Hay que gestionar que nuestras empresas, nuestras administraciones y nuestros ciudadanos se conectarán y utilizarán las tecnologías y tenemos que trabajar para que el impacto que pueda tener un incidente sobre ellos sea el mínimo posible.

Respecto a la mejora de las capacidades de prevención y previsión consideramos desde Incibe que es uno de los aspectos fundamentales a la hora de mejorar la protección de nuestros ciudadanos. Una vez que les ha pasado algo tenemos que tener la capacidad de brindarles apoyo y responder en el menor tiempo posible y minimizar el impacto, pero es mucho más importante tener las capacidades preventivas para que cuando sufran un incidente realmente no les pase nada. Por tanto gran parte de los esfuerzos que hacemos desde Incibe, tanto con ciudadanos como con empresas, tienen que ver con servicios preventivos. Nuestros ciudadanos, nuestros autónomos, nuestras pequeñas empresas tienen que incorporar esas recomendaciones básicas de ciberseguridad; son sencillas y probablemente solucionarán más del 80 % de los incidentes que tienen lugar en nuestro país. Es una de las claves en las estrategias que debe implementar cada país para mejorar la ciberseguridad y que nuestra Estrategia Nacional de Ciberseguridad incorpora.

Pasando a las preguntas de la señora Vázquez, en primer lugar, es importante trabajar en el ámbito de la concienciación y en la mejora del juicio crítico. Cuando nuestros ciudadanos están en el mundo físico, cuando andan por la calle toman ciertas precauciones en cuanto a, por ejemplo, hablar con un desconocido. Eso lo vemos todos los días. Cuando un desconocido se acerca a un menor, a un ciudadano o a una ciudadana, responden de forma defensiva. Cuando utilizamos Internet y estamos en nuestra casa, en un entorno que consideramos seguro, ese nivel de guardia lo bajamos y empezamos a aumentar el nivel de confianza en cosas en las que no la teníamos en el mundo físico. Por tanto es muy importante trabajar en mejorar el nivel de confianza o desconfianza y en el juicio crítico, porque nos seguirán llegando muchas cosas. Estamos en un mundo abierto, en un mundo en el que vamos a seguir conectados con amigos y con conocidos de países que están a miles de kilómetros, y por ello accederemos a información de todo tipo, y aquí es muy importante trabajar en el juicio crítico de todos los usuarios que se conectan a Internet.

He hablado anteriormente de los puestos de trabajo y de los medios económicos de Incibe. En cuanto a disponibilidad de talento hay un incremento del 23 % del personal. Y respecto a las pymes, como decía, estamos viendo que están mejorando su nivel de conciencia, y eso hay que reforzarlo. Estamos trabajando para que eleven su nivel de entendimiento. Y por último deben entender que la tecnología conlleva un coste en el uso y en el propio desarrollo. Hablaba anteriormente de la necesidad de trabajar con los fabricantes para que desarrollen productos seguros, lo que encarecerá su precio, pero es un aspecto fundamental, igual que la propia funcionalidad del producto.

Respecto a la figura del reservista, por la que me preguntaba la señora Vázquez, consideramos que el apoyo de la ciudadanía puede ser muy importante en determinadas situaciones. Si miramos hacia atrás, en el año 2007 —en la crisis de Estonia— un grupo civil denominado la Liga Estonia participó apoyando a los organismos del Gobierno en la defensa contra los ataques. Son muchas las ocasiones en las que los ciudadanos nos preguntan cómo colaborar con Incibe en el ámbito de la ciberseguridad. Por tanto pensamos que una figura de reservista puede ser muy interesante y muy útil, y será la forma en la que simplemente se apoye a cada uno de los organismos donde habrá que trabajar más intensamente. Como decía también al principio de mi intervención en el ámbito de la concienciación de los ciudadanos sabemos que los organismos públicos tenemos que trabajar de forma intensa, clara y permanente, y llegar a todos los rincones de nuestro país de forma continua. Para hacer eso necesitamos que el sector privado y los propios ciudadanos se involucren. Eso fue lo que nos motivó a lanzar el pasado año el programa de cibercooperantes, un programa de voluntariado por el cual cualquier ciudadano que esté interesado en participar en esa labor de concienciar a nuestros menores pueda ir a colegios e institutos, y trasladar el mensaje que desde Incibe estamos construyendo. Ha pasado un año y tenemos más de 300 cibercooperantes en España que están dando charlas en colegios e institutos. Esta iniciativa pone de manifiesto la necesidad de la colaboración público-privada de los ciudadanos, la colaboración internacional, y el compromiso que estamos viendo por parte de diferentes agentes en esta misión que tenemos encomendada.

cve: DSCG-12-CM-65

Para terminar, antes de pasar al segundo turno, si el presidente lo considera oportuno, me gustaría aprovechar esta comparecencia para invitarles a visitar nuestra sede de Incibe en la ciudad de León. Tendremos la oportunidad de enseñarles aquello en lo que estamos trabajando y cómo estamos gestionando los incidentes en nuestro país.

El señor **PRESIDENTE:** Muchísimas gracias, señor Hernández, por su intervención y por su invitación.
Abrimos el segundo turno, empezando por el Grupo Mixto. Tiene la palabra el señor Yanguas.

El señor **YANGUAS FERNÁNDEZ:** Muchas gracias, señor presidente.
No tengo mucho más que añadir. Simplemente quiero agradecerle que haya respondido con muchísima claridad a todas y cada una de las preguntas que le he formulado. Le vuelvo a dar las gracias por su claro discurso.

El señor **PRESIDENTE:** Muchísimas gracias, señor Yanguas.
Señor Salvador.

El señor **SALVADOR GARCÍA:** Muchas gracias, señor presidente.
También me sumo a la cantidad de respuestas que nos ha dado y a lo que ya nos había comunicado, y simplemente voy a profundizar un poquito más en los incidentes sobre todo de las empresas estratégicas. Ha manifestado que se ha detectado que ese tipo de ataques ha aumentado año tras año de manera exponencial. También ha dicho que el número de incidentes ha sido pequeño, y quiero preguntarle si ha sido pequeño porque la amenaza en la forma en que se ha planteado era débil o si porque realmente esas empresas que en este momento son estratégicas ya estaban protegidas para poder defenderse de esos ataques que puedan ser un poquito más fuertes.
Por lo que se refiere al tema de WannaCry, cuando se empezó a hablar de todo ello vimos que por lo visto el FBI había detenido a una persona que supuestamente había sido el héroe que había proporcionado la vacuna para sanarnos a todos. Sin embargo después detectó la Policía —en este caso el FBI— que era uno de los responsables de que eso sucediera. Digo esto también en relación con los ataques a estas empresas de los que estamos hablando. Si, primero, se ha detectado ya quiénes estaban detrás de esos ataques, si eso ha dado lugar a acciones judiciales contra los responsables, y si eso está teniendo algún tipo de repercusión. Usted ha dicho una cosa que yo le iba a preguntar sobre los fiscales y jueces especializados, que en este momento cada vez van siendo más, pero le quiero preguntar si entiende que ya son los suficientes para poder atender a este mundo tan global, donde la incidencia de la tecnología es tan absolutamente determinante, o si todavía los jueces y fiscales especializados son pocos para los que debieran de ser. Los Cuerpos y Fuerzas de Seguridad del Estado sí lo están haciendo adecuadamente, y lo estamos viendo día tras día, pero me gustaría saber si la justicia también lo está haciendo bien.
Para terminar, con este mismo argumento, quería preguntarle sobre esa sensación de impunidad que existe, precisamente por tener capacidad para garantizar el anonimato para realizar ataques, y que en caso de salir victoriosos serían muy lucrativos y daría muchísimos beneficios a los que los ocasionan. También quisiera saber si la defensa de los buenos está englobada dentro de la justicia y si se están consiguiendo detectar e identificar, abrir procesos que después terminen en condenas. Creo que es lo único que va a terminar disuadiendo en esa práctica tan fácil de intentar algo, porque si se piensa que no se va a enterar nadie, o no se consigue descubrir quiénes están detrás de ello, o si la jurisdicción desde la que lo hacemos nos afecta relativamente poco, esos intentos serán muy permanentes, mientras que también se puede disuadir desde la vía de que quien la haga, la pague.
Mi grupo evidentemente está feliz por la invitación que ha hecho. Estoy seguro de que el presidente de esta magnífica ponencia y de la Comisión de Seguridad Nacional va a aceptar, porque creo que es muy importante.
Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Salvador.
Senador Comorera.

El señor **COMORERA ESTARELLAS:** Muchas gracias, señor presidente.
Gracias por las respuestas que ha dado, en general, a todas las preguntas formuladas, en particular a las que anteriormente le he formulado. Entiendo que son imprescindibles —las echo en falta— muchas más campañas para automatizar estas medidas de seguridad que nos explicaba. Me ha gustado el

cve: DSCG-12-CM-65

ejemplo que ha puesto sobre la aplicación para móviles Android para comprobar la seguridad de los móviles, pero es la primera noticia que tengo, y en teoría soy una persona más o menos informada que está en redes casi diariamente. Y este es el ejemplo de que esto no llega al ciudadano de a pie, ni seguramente a los autónomos ni a muchas pymes. Creo que se debería profundizar en el tema publicitario para saber qué está haciendo Incibe.

Una de las preguntas a las que no me ha contestado es sobre el tema de Lexnet. Estaría interesado en que me contestara si tuvo alguna actuación el Incibe en cuanto a la crisis de Lexnet. Respecto a lo de la desinformación, usted decía que hay que plantear a quién interesa y a quién beneficia, pero a mí lo que me interesa es quién determina que esa información es veraz o qué es desinformación, porque si eso lo dejamos en manos del Gobierno de turno podemos tener un problema, ya que podemos preguntar a quién interesa y a quién beneficia hablar de una determinada campaña sobre *hackers* rusos, venezolanos, etcétera.

Esas eran las aclaraciones que quería. Muchas gracias.

El señor **PRESIDENTE:** Gracias, senador.

Señor Raffo.

El señor **RAFFO CAMARILLO:** Antes de nada quisiera agradecerle las respuestas, así como el análisis y el asesoramiento, que son muy útiles para la tarea que tenemos que desempeñar.

Me gustaría que nos ampliara cómo se ha producido, si es que se ha dado, el proceso de coordinación transversal con otras organizaciones relacionadas con la seguridad nacional, al hilo de estos ciberataques que ocurrieron en torno al debate del artículo 155 —han mencionado por aquí una de las páginas del Tribunal Constitucional, creo que el día 21 de octubre—, y también en relación con los acontecimientos de la desinformación o la guerra informativa, entre comillas, relacionada con esos acontecimientos. Y nos interesa conocer cómo se producen las relaciones en situaciones de alerta o de alarma con organismos supranacionales, como por ejemplo el que corresponde a la Unión Europea.

El señor **PRESIDENTE:** Muchísimas gracias, señor Raffo.

Señora Vázquez.

La señora **VÁZQUEZ BLANCO:** Muchas gracias, señor presidente.

Simplemente para agradecer las magníficas y claras explicaciones que nos ha dado el director del Incibe, así como la invitación a visitarles, porque sin lugar a dudas vamos a ir. Está bien que esta Comisión conozca el inmenso trabajo que hace el Incibe. Al igual que el senador de Podemos, no conocía esa aplicación, y ahora la conocemos. Por tanto hay que dar las gracias al Incibe, que realiza muchísimo trabajo que podríamos decir que no se ve, pero que realmente está ahí. Así que le felicito por el trabajo que desarrollan en el Incibe, así como a toda la gente que está colaborando allí por la seguridad en las redes.

Muchísimas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señora Vázquez.

Señor Hernández.

El señor **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, S.A., INCIBE** (Hernández Moreno): Muchas gracias, presidente.

Gracias de nuevo por las preguntas. Respecto a la pregunta del señor Salvador sobre los incidentes en las empresas estratégicas, como comentaba, hemos gestionado más de 700. Algunos de ellos tienen que ver con intentos de acceso o intrusión, estilo el WannaCry, que hizo una intrusión en un sistema para luego descifrarlo y pedir un rescate. El resultado de que el impacto sea mínimo tiene mucho que ver con la capacidad de respuesta-protección que tienen esas infraestructuras, estas empresas. Comentaba anteriormente que tenemos la Ley de Protección de Infraestructuras Críticas, y desde el ámbito público llevamos trabajando mucho con el sector privado y con el sector público para que implementen mecanismos de seguridad. Tenemos empresas que además son pioneras en algunas soluciones y referentes a nivel internacional. Por tanto el resultado de por qué, después de 113 000 incidentes de ciberseguridad a finales de octubre y más de 700, no hayan tenido un impacto significativo que hayamos podido ver en nuestro país es fundamentalmente por el nivel de protección que tenemos en las empresas estratégicas.

cve: DSCG-12-CM-65

Respecto a la crisis de WannaCry vimos sobre todo numerosas noticias asociadas a la propia crisis, y también previendo cuál iba a ser la evolución de la crisis. Pudimos ver la noticia de esta persona de Reino Unido que identificó un dominio de internet al que se conectaba uno de los TIC de *malware* asociados a WannaCry, porque no solamente hubo uno, y que al registrar ese domino desactivaba la actuación de este *malware*. Puedo decir que antes de que esta persona publicase que lo había detectado, en España ya lo conocíamos. Una cosa es el trabajo que realizamos y que no se hace público porque estamos trabajando en él, y otra cosa es la información que muchas veces circula. Es decir, Telefónica, que fue la primera empresa afectada por este tema, desde el primer momento que se vio afectada lo puso en conocimiento de los organismos públicos que trabajamos en este campo. Además trabajó intensamente y con el resto de empresas de ciberseguridad que tenemos en nuestro país en el análisis de lo que estaba pasando, y desde el primer momento estuvimos compartiendo a nivel internacional información para que el resto de países estuviesen prevenidos y adecuadamente protegidos. De los estudios que hicimos en Incibe, tras la crisis de WannaCry, España no estaba entre los diez primeros países en número de infecciones, siendo uno de los primeros, quizá el primer país, que fue afectado por WannaCry, y eso vino en gran medida por el trabajo que se hizo desde Telefónica y el resto de empresas de ciberseguridad y los organismos públicos. Estuvimos trabajando intensamente durante cinco días intercambiando información, y el resultado fue que países que ya tenían información cuando les llegó el incidente, que nosotros no tuvimos cuando empezó, porque empezó prácticamente en España, han tenido un nivel de afectación muy superior al nivel de España. Puedo decir que en España —son datos el Ministerio del Interior, del *Estudio sobre la cibercriminalidad en España*, del año 2016—, como comentaba anteriormente, nuestras Fuerzas y Cuerpos de Seguridad del Estado tuvieron conocimiento de un total de 66 586 hechos delictivos, con un incremento del 10,7 % respecto al año anterior. También como comentaba antes, todo hay que mirarlo desde diferentes puntos de vista. Están ocurriendo más cosas, pero también es verdad que los ciudadanos denuncian más, que se están detectando mayores casos, por eso se produce el incremento de estos hechos. De esos 66 586 hechos, 54 446 correspondían a victimizaciones. No tengo el dato aquí, pero sí recuerdo que el número de hechos esclarecidos supera el 30 % de los hechos, es decir, las investigaciones que se llevan a cabo a posteriori están llegando a buen término, y las detecciones que se producen de individuos, a los que se llega al final del caso, superan los cinco mil. Por tanto podemos decir que en este nuevo entorno en el que nos encontramos, que es global, asimétrico, donde es difícil de atribuir las acciones y que presenta muchas dificultades, sí encontramos que en muchos de los casos se llega al origen del problema, y esto es por muchas razones. Una de ellas es porque nuestras Fuerzas y Cuerpos de Seguridad están trabajando intensamente y tenemos unidades especializadas, que además son un referente a nivel internacional, y que están participando en el adiestramiento de policías de otros países.

Respecto a jueces y fiscales nosotros hemos llevado a cabo varias iniciativas de formación de jueces y fiscales. Tenemos una fiscalía especializada en asuntos de ciberdelitos, fiscalía que además participa en el ámbito internacional en el apoyo a la mejora de las capacidades de los fiscales en otros países. En el ámbito de la ciberseguridad, igual que en el de la seguridad, todavía hay mucho por hacer, y además será una tarea que se mantendrá durante muchísimos años. Tenemos mucho que hacer, mucho que autoevaluarnos, y mucho que incrementar y amplificar en nuestras actuaciones, pero creo que lo estamos consiguiendo y tenemos resultados bastante positivos. Permítanme recordar un caso que podemos ver en los medios de comunicación. Ustedes pueden ver que en las últimas semanas han aparecido acciones de nuestras Fuerzas y Cuerpos de Seguridad del Estado en las que han desmantelado grupos u organizaciones criminales que estaban operando en el ámbito europeo, por ejemplo, haciendo extorsiones a consejeros delegados y CEO de compañías, de forma que mediante el engaño a sus responsables financieros y secretarios, estaban haciendo transferencias internacionales a espaldas del CEO, lo que estaba siendo un negocio millonario. Nuestras Fuerzas y Cuerpos de Seguridad del Estado desactivaron hace unas semanas a esta organización criminal que estaba actuando en toda Europa. Por tanto podemos decir que, a pesar de las dificultades que presenta este nuevo entorno, se están consiguiendo resultados.

Respecto a las preguntas del señor Comorera tengo que decir que efectivamente la comunicación es muy importante. Los servicios públicos que no se conocen no son suficientemente válidos. Debemos trabajar intensamente —lo hemos venido haciendo, pero creo que es otro reto que tenemos ahora por delante— en acercar la ciberseguridad a todos los ciudadanos para su ámbito personal y también en el contexto empresarial. Como decía hemos trabajado en muchas iniciativas, hemos llegado a más de 9600 alumnos el pasado año y a más de 1500 profesores en charlas de ciberseguridad. Hemos tenido más de 20 000 personas asistiendo al Cybercamp, tenemos más de 1500 alumnos participando en campeonatos

cve: DSCG-12-CM-65

por Internet. Este año hemos organizado por segunda vez unas ciberolimpiadas entre colegios, en las que han participado más de 170 colegios, y los diez mejores colegios irán a competir en el Cybercamp, de donde sacaremos el equipo europeo que competirá el año que viene en el campeonato europeo, que ya ganamos este año. Pero no es suficiente, tenemos que seguir trabajando en esa línea y lanzar campañas en todos los medios de comunicación en los próximos años para concienciar a ciudadanos y empresas. De hecho son iniciativas que tenemos planificadas y diseñadas para lanzar en los próximos meses.

En cuanto a Lexnet diré que Incibe tiene su foco en ciudadanos y empresas. El incidente afectó a sistemas de la Administración pública. Como saben ustedes el Centro Criptológico Nacional hace una importante y muy buena labor en la protección de todas las administraciones públicas, y es el competente en este caso.

Respecto a la influencia extranjera, como preguntaba el señor Raffo, la amenaza es híbrida. Para determinar el origen de las diferentes actuaciones se necesita aplicar una visión holística. La visión de Incibe es técnica. Nosotros llegamos a conocer lo que le está pasando al ciudadano y a la empresa, en qué consiste y cuál es el siguiente salto en cuanto al origen. Para determinar la atribución adecuada a este tipo de casos y a todos los incidentes hay que ir más allá; se necesitan actuaciones de las Fuerzas y Cuerpos de Seguridad del Estado en el caso del ciberdelito, y se requiere analizar el problema desde otra visión mucho más amplia que la que puede proporcionar Incibe.

Señor Raffo, WannaCry fue un incidente que generó una crisis a nivel mundial y nacional. El impacto que tuvo fue limitado. Fue una crisis muy mediática, apareció en los medios de comunicación. Ver empleados de una gran compañía saliendo del trabajo por un ciberataque causó un impacto importante en nuestra sociedad. En ese caso, igual que en todos los que afrontamos todos los días —porque todos los días gestionamos cientos de incidentes de ciberseguridad, y algunos muy parecidos al WannaCry—, mantenemos una coordinación estrecha con todos los organismos públicos y privados que trabajamos en el ámbito de la ciberseguridad. Cada día estamos en permanente contacto e intercambiando información de carácter técnico y operativo sobre lo que está pasando a nuestros ciudadanos y a nuestras empresas, que puede ser útil para lo que le puede pasar a nuestras administraciones. Del mismo modo los organismos que trabajan en el ámbito de la defensa, en el ámbito de las administraciones públicas, nos proporcionan de forma permanente información sobre amenazas e incidentes que ocurren en la Administración, y que pueden ser importantes a la hora de prevenir los incidentes en el sector de ciudadanía y de empresas, y así responder adecuadamente. Por tanto mantenemos una coordinación de forma diaria que tiene que ver también con la evaluación de la amenaza constante. Esta coordinación es importante mantenerla en el ámbito internacional, y me preguntaba por la coordinación en el ámbito de la Unión Europea. Es esencial la coordinación con los organismos internacionales que tienen competencias en el ámbito de la ciberseguridad, y por tanto Incibe, igual que el resto de organismos públicos en España, estamos integrados en la Red Internacional de Centros de Respuesta ante Incidentes, que se denomina First, y que establece una red de contactos en los que, en caso de un incidente, podemos trabajar conjuntamente, podemos saber a quién llamar, y también si ellos tienen un problema nos llaman. Es muy frecuente y forma parte de la operativa diaria que incidentes que tienen lugar en España los trabajemos conjuntamente con organismos similares a Incibe de otros países, y también que ante incidentes que ocurren en otros países los organismos correspondientes se pongan en contacto con Incibe para buscar ayuda.

El fortalecimiento de NISA vendrá a contribuir en tres ámbitos fundamentales: en el desarrollo de la estandarización y certificación; también en la mejora de la concienciación en aquellos países que van un paso por detrás, y en la construcción de las capacidades de ciberseguridad en países que aún no tienen las capacidades que tenemos en España. Respecto a las ondas en las e-pymes, que se me ha quedado anteriormente sin contestar, diré que es muy importante que a la hora de trabajar en la protección de nuestros ciudadanos y nuestras empresas generemos confianza, es decir, hasta este momento no existe una legislación en España que obligue en el ámbito de los incidentes de ciberseguridad a que aquellos que los sufran lo pongan en conocimiento de los organismos públicos que trabajamos en ello. Pero es verdad que estamos en proceso de trasposición de la Directiva europea de seguridad en redes y sistemas de información, que se traspondrá en los próximos meses. En el ámbito de esa directiva se establecerá la obligatoriedad de que los operadores de servicios esenciales lo notifiquen cada vez que sufran un incidente, pero creo que tenemos una buena noticia, y es que este incremento en el número de incidentes que hemos gestionado los operadores estratégicos —hemos pasado de 60 a más de 100, a más de 400 y a más de 700— se ha producido también porque nos lo han notificado cada vez más las empresas

cve: DSCG-12-CM-65

cuando han tenido problemas. Es decir, nos lo están notificando a pesar de que todavía no existe una norma o una ley que les obligue a hacerlo, y ese es un dato muy importante, que tiene que ver con el incremento de la confianza que debemos tener con nuestros, llamémosles, clientes, en nuestro caso ciudadanos y empresas. Por lo tanto establecer mecanismos que permitan analizar el tráfico de nuestros ciudadanos y empresas en Internet no forma parte de la estrategia de Incibe, puesto que nosotros tenemos que intentar dar confianza a través de la transparencia y de la detección de la información, sin intentar interferir o al menos sin que el ciudadano o las empresas puedan entender que estamos analizando su tráfico. Ese análisis que hacemos proactivo y detectivo de incidentes que ocurren en España no lo hacemos analizando el tráfico ni las conexiones de nuestros ciudadanos y empresas, sino en el marco de acuerdos internacionales por los cuales el resto de países y organizaciones internacionales nos lo comunican cada vez que conocen un incidente o que las redes están infectadas en nuestro país. De forma recíproca lo hacemos nosotros con ellos, y de esa forma generamos y mantenemos —y por ahí tenemos que ir— la confianza de nuestros ciudadanos y nuestras empresas, y por otro lado, les podemos dar un apoyo en la mejora de su ciberseguridad.

El señor **PRESIDENTE:** Muchísimas gracias, señor Hernández.

¿Algún portavoz necesita alguna aclaración adicional? **(Pausa).** Si no es el caso, damos por concluida esta comparecencia. Rogaría a los miembros de la Mesa y a los portavoces que nos reunamos cinco minutos.

Se levanta la sesión.

Era la una y treinta minutos de la tarde.

cve: DSCG-12-CM-65