DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 105 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 18

celebrada el martes 18 de septiembre de 2018 en el Palacio del Senado

---

Página

---

cve: DSCG-12-CM-105

Se abre la sesión a las diez horas.

El señor **PRESIDENTE:** Buenos días. Se abre la sesión.

Sus señorías me dirán si me oyen bien, porque estrenamos un sistema nuevo y esto de las tecnologías no es lo mío.

SOLICITUD DE PRÓRROGA DE LOS TRABAJOS DE LA SIGUIENTE PONENCIA:

— PONENCIA PARA EL ESTUDIO DE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Senado 573/000003 y número de expediente del Congreso de los Diputados 154/000011).
AUTOR: COMISIÓN MIXTA DE SEGURIDAD NACIONAL.

El señor **PRESIDENTE:** El primer punto del día es la solicitud de prórroga de los trabajos de la Ponencia para el Estudio de Diversas Cuestiones Relativas a la Ciberseguridad en España.

¿Se puede aprobar la prórroga por asentimiento? **(Asentimiento).**

ELECCIÓN DE VACANTES. MESA DE LA COMISIÓN:

— ELECCIÓN DE LA VICEPRESIDENCIA PRIMERA DE LA COMISIÓN. (Números de expediente del Senado 570/000006 y 571/000005, y número de expediente del Congreso de los Diputados 041/000040).

— ELECCIÓN DE LA VICEPRESIDENCIA SEGUNDA DE LA COMISIÓN. (Números de expediente del Senado 570/000006 y 571/000005, y número de expediente del Congreso de los Diputados 041/000040).

El señor **PRESIDENTE:** Pasamos, por tanto, a los siguientes puntos del orden del orden del día, que son la elección de las Vicepresidencias Primera y Segunda de la comisión.

Les comunico a sus señorías que existe una propuesta del Grupo Parlamentario Socialista para nombrar a don Juan Jiménez Tortosa como vicepresidente primero de la comisión que, si ustedes no me contradicen, resultará elegido por asentimiento. **(Asentimiento).** No me contradice nadie, lo que me parece bien; espero tener el mismo éxito en la siguiente propuesta.

Les comunico, asimismo, que existe una propuesta del Grupo Parlamentario Popular, para nombrar a doña Pilar Rojo Noguera como vicepresidenta segunda de la comisión, resultando elegida por asentimiento, si no hay nadie en contra. ¿Es así? **(Asentimiento).**

Invito a ambos miembros de la Mesa a ocupar sus puestos.

CELEBRACIÓN DE LA SIGUIENTE COMPARECENCIA:

— DE DON JAVIER CANDAU ROMERO, JEFE DEL DEPARTAMENTO DE CIBERSEGURIDAD DEL CENTRO CRIPTOLÓGICO NACIONAL, PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Senado 713/001031 y número de expediente del Congreso de los Diputados 212/001726).
AUTOR: COMISIÓN MIXTA DE SEGURIDAD NACIONAL.

El señor **PRESIDENTE:** El siguiente punto del orden del día es el que se refiere a la comparecencia de don Javier Candau, jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional, para informar sobre diversas cuestiones relativas a la ciberseguridad en España. Señor Candau, bienvenido. Después de su intervención inicial intervendrán los portavoces, volverá a intervenir usted y, por último, habrá otro turno para los portavoces de los grupos.

Sin más preámbulos, le cedo la palabra.

El señor **JEFE DEL DEPARTAMENTO DE CIBERSEGURIDAD DEL CENTRO CRIPTOLÓGICO NACIONAL** (Candau Romero): Muy buenos días a todos. Quiero dar las gracias a los miembros de esta comisión mixta por permitirnos dar nuestro punto de vista sobre el estado de la ciberseguridad en España. **(El señor compareciente apoya su intervención con la proyección de diapositivas).**

Los puntos que voy a abordar son los siguientes: de cuál es la misión del CCN, del Centro Criptológico Nacional, y sobre la capacidad de respuesta a incidentes del Centro Criptológico; sobre cómo se está

cve: DSCG-12-CM-105

organizando la ciberseguridad en España; también del Esquema Nacional de Seguridad, por ser algo genuino en Europa, y que no tiene comparación con respecto a otras normativas; y, asimismo, hablaré un poco sobre notificación, que está de moda en todas las leyes y reales decretos que se están aprobando. Por último, si da tiempo, hablaré sobre ciberamenazas y sobre los retos que nos planteamos.

He dejado sobre la mesa dos documentos: la Aproximación Española a la Ciberseguridad, que está también en formato electrónico —y que puedo proporcionar a los miembros de la Mesa en este formato—, que nos indica cuál ha sido el itinerario de España durante estos últimos diez años en ciberseguridad; y el informe de amenazas en la edición de 2018, donde se habla sobre cuáles son, desde el punto de vista del CCN-CERT, las principales amenazas para la ciberseguridad. Por último, existe un informe de actividades que se elabora cada dos años y la siguiente edición se publicará el año que viene.

El CCN está organizado en dos departamentos: el Departamento de Ciberseguridad, que tengo el honor de dirigir; y el Departamento de Productos y Tecnologías, que es el que desarrolla todos los productos de cifra para Fuerzas Armadas, Presidencia, Ministerio de Asuntos Exteriores, etcétera. En la pantalla pueden ver nuestro portal web.

En relación con el mandato legal, el CCN se cre***ó*** mediante la Ley 11/2002, del CNI; el Real Decreto 421/2004 estableció sus funciones, que en un principio estaban bastante circunscritas a sistemas clasificados y a sistemas que manejaban medios de cifra; y, con el Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad y la creación del CCN-CERT, muchos de los servicios establecidos en 2004 para el CCN, solo para algunos ministerios, se extienden a toda la Administración del Estado: general, autonómica y local.

Se establece el CCN-CERT como el CERT gubernamental nacional. Y en la pantalla pueden ver su misión y su comunidad. Básicamente, nosotros tenemos que ayudar a todo el sector público; es decir, a la administración general, autonómica y local —unas 13000 entidades— y a lo que se llama el sector público institucional —unas 18000 entidades—.

Ahora hablaré de algunos de nuestros servicios y, en este sentido, les diré que proporcionamos muchos estándares de ciberseguridad, damos formación a todo el personal civil de la administración —tanto general, como autonómica y local—, respondemos ante ciberataques —lo que es nuestra principal misión—, por supuesto intercambiamos información y realizamos muchas auditorías. Asimismo, está pendiente de aprobación un acuerdo del Consejo de Ministros para empezar a trabajar en lo que llamamos Centro de Operaciones de Seguridad de la AGE; y estamos ya trabajando en el Centro de Operaciones de Seguridad para toda la Administración de Justicia.

Según nuestra experiencia, durante estos diez años hemos desarrollado muchas herramientas: de auditoría, de detección, de análisis, de intercambio y mucha formación. Yo me voy a centrar en la de intercambio de ciberincidentes por aquello de que toda la normativa obliga a su notificación.

Paso a mostrarles el camino que está tomando España y que es el que recomendamos a todos los países iberoamericanos que visitamos. Se trata de diez pasos fundamentales que hay que dar en ciberseguridad. El primero de ellos es tener una estrategia; establecer una gobernanza, de manera que todo el mundo tenga claros los papeles. Por ejemplo, el Reino Unido mantuvo durante bastante tiempo un conflicto de competencias entre el MI5 y el GCHQ, a costa de la ciberseguridad. Al final, han terminado tomando una decisión salomónica: la de crear un Centro Nacional de Ciberseguridad, en el cual se integran las capacidades cíber de ambos organismos.

El tercer punto es importante y casi ningún país lo aborda: se trata de contar con un desarrollo reglamentario posibilista; es decir, establecer un marco de medidas de seguridad de obligado cumplimiento, algo que se invita a hacer con la nueva directiva NIS, pero que antes se dejaba un poco de lado. Otro aspecto es la buena capacidad de detección; y resalto el intercambio de información, que trataré posteriormente. En muchos países, según qué ministerio lo aborde, no se trata igual, pero nosotros consideramos que la ciberseguridad es un asunto de seguridad nacional porque a través del mundo cíber van a atacar a nuestra soberanía, al patrimonio tecnológico de nuestras empresas y a algunos asuntos que pueden hacer daño a nuestra economía.

Desde el punto de vista de la estrategia, se creó el Consejo de Seguridad Nacional, a través de la Ley de la Seguridad Nacional, y dependiente de él está el Comité de Ciberseguridad o Consejo de Ciberseguridad Nacional. Ahora mismo, presiden este consejo el director del Centro Nacional de Inteligencia y el director del Centro Criptológico Nacional y ahí se sientan todos los ministerios y alguna agencia. Durante el proceso de vida de este consejo se vio que era poco operativo cuando sufríamos un incidente tipo WannaCry y, por ello, se decidió crear la Comisión Permanente de Ciberseguridad. ¿Qué

cve: DSCG-12-CM-105

ministerios están representados? El Ministerio de Función Pública, el Ministerio de Defensa, el Centro Criptológico Nacional, el Ministerio de Interior y el antiguo Ministerio de Industria. ¿Por qué están estos ministerios? Porque, dentro de estos ministerios, hay organismos que son los que ejecutan las acciones de defensa en el mundo cíber.

Durante el tiempo de vida de la estrategia de ciberseguridad, que se aprobó en 2013, se han hecho cosas. A principios de 2014 se creó el Consejo Nacional de Ciberseguridad, en octubre de 2014 se aprobó el Plan nacional de ciberseguridad y, en julio 2015, se aprobaron los planes derivados. Esto es importante porque, después de desarrollar las 8 líneas de acción de la estrategia —que pueden ver en las diapositivas—, se tomó la decisión de incluir la estrategia número 9, intercambio, dentro del Plan nacional de ciberseguridad y se asignaron cada una de las misiones y líneas de acción a determinados organismos, con lo cual empezábamos a trabajar para evitar solapes y que a un organismo le atendieran varios CERT de referencia.

La estrategia es un documento político, pero luego nosotros, los funcionarios, nos regimos por las leyes y reales decretos que publica el Gobierno. En este sentido, ¿qué hemos tenido hasta la fecha? La primera Ley Orgánica de protección de datos, allá por el año 1999; las funciones del CCN, en 2004; la Ley de administración electrónica, en 2007; y después se aprobó el Esquema Nacional de Seguridad. El Esquema Nacional de Seguridad es un documento en el cual se establecen unos principios básicos y unos requisitos mínimos y que ofrece homogeneidad de aplicación en relación con todas las medidas de seguridad a todo el sector público. Ese Esquema Nacional de Seguridad se modificó en 2015 y, ahora, en todas las leyes que ven en la pantalla con un cuadradito rojo existe la obligación de notificar los incidentes. La primera que obliga a notificar incidentes es el Esquema Nacional de Seguridad y, posteriormente, desde su creación, el Centro Nacional de Protección de Infraestructuras Críticas, para todas las infraestructuras críticas de los sectores estratégicos que se determinen. Además, últimamente nos han venido de la Unión Europea tanto la directiva NIS como la nueva regulación de protección de datos personales, que obligan a notificar incidentes. Es decir, que hemos pasado de un escenario en el que no teníamos obligación de notificar nada a, en dos años, no solo tener que notificarlo todo sino que, además, lo tenemos que hacer a muchísimas agencias.

El gobierno de la ciberseguridad cuenta con varios niveles: el nivel técnico, el nivel operacional, el nivel estratégico y el nivel político. En la nueva directiva NIS se otorga al CCN-CERT el papel de coordinador cuando tenemos que abordar incidentes severos, tipo WannaCry, NotPetya o cualquier otro.

Dicho eso, voy a pararme dos minutos en el Esquema Nacional de Seguridad. El Esquema Nacional de Seguridad, que se aprobó en 2010 y se actualizó en 2015, tiene previstas 8 instrucciones técnicas de seguridad, de las que 4 están ya aprobadas, y otorga a España un marco de comparación, como decía al principio, que no lo tiene ningún país de la Unión Europea. El Esquema Nacional de Seguridad tiene 6 principios básicos, 15 requisitos mínimos y 75 medidas de seguridad. Establece que el sector público tiene que establecer tres categorías —básica, media y alta— y, según esas categorías, vamos a exigir más o menos a los organismos. Además, resalto algo que heredamos de la antigua Ley Orgánica de protección de datos, que es la necesidad de auditoría. Ni la GDPR nueva ni la directiva NIS nueva obligan a hacer auditorías, pero si no hacemos auditorías no sabemos qué nivel de seguridad hay. Sin embargo, el ENS sí obliga a hacer auditorías para generar luego la capacidad de respuesta a incidentes. Me voy a centrar ahora en el detalle de las 75 medidas, por categorías. Así, para la categoría básica se exigen 45 controles, para la categoría media, 63 controles y, para la categoría alta, 75 controles. Si nos vamos al estándar internacional equivalente, esto sería lo que llamamos ISO/IEC 27001 e ISO/IEC 27002, que tienen un ámbito muchísimo más pequeñito que el Esquema Nacional de Seguridad. Pero, en una comparativa de las dos normas se aprecia que, en un 80 %, la 27001 cubre el ENS y que el otro 20 % indica que la normativa nacional exige más que el estándar internacional.

Como este real decreto es de obligado cumplimiento para todas las administraciones públicas, y dado que se aprobó en 2010 y que se dieron cuatro años, en teoría en 2014 deberíamos haber logrado el cien por cien del cumplimiento en todas las instituciones públicas. Realmente, hay un artículo dentro de este real decreto, el artículo 35, que obliga al Centro Criptológico Nacional a realizar una medición del nivel de seguridad que tienen todas las administraciones públicas. Empezamos a hacerlo en 2014, cuando se cargaron datos en el Informe Nacional del Estado de Seguridad, el informe INES, en el que se recoge que en 2014 se analizaron 118 organismos, en 2015, 355 y en 2017, 774. Por ahora, la información que están cargando los organismos se basa en su propia autoevaluación, pero lo ideal sería que la información que se cargue en INES esté basada en una auditoría de cumplimiento. Esto también lo contempla el Esquema

cve: DSCG-12-CM-105

Nacional de Seguridad, con estos dos sellos de certificación que aparecen en la derecha de la pantalla. En este sentido, nosotros damos dos notas: un índice de madurez y un índice de cumplimiento. El índice de madurez se refiere a qué nivel de seguridad real tiene el organismo y para ello comparamos su nivel de seguridad y la madurez con las 75 medidas, independientemente de la categoría del sistema; y comparamos el índice de cumplimiento solo con las medidas que le aplican. Por eso, la barra naranja del gráfico que ven en pantalla, que representa el índice de cumplimiento, tiene mejor nota que el índice de madurez. Así, aunque la AGE está un poquito mejor que las demás, las entidades locales no pasan, las universidades pasan con dificultad y, en el global, obtenemos un cinco justito. ¿Por qué? Porque todavía, por desgracia, en todas las administraciones públicas la ciberseguridad no ocupa el papel que debería ocupar. Esta sería la situación de nuestro Esquema Nacional de Seguridad.

Siguiendo el documento de aproximación a la ciberseguridad, en los puntos 4, 5 y 6 se recomienda encarecidamente mejorar la capacidad de vigilancia. Si tenemos monitorizados todo nuestro sistema y, gracias a nuestra capacidad de vigilancia, podremos detectar incidentes. En esta imagen se explica cuál ha sido la evolución de nuestro sistema estrella, que es el Sistema de Alerta Temprana de Internet. Este sistema estrella va creciendo con alrededor de 25 o 30 sondas que se despliegan y es un sistema de carácter voluntario, pues es el organismo quien decide y compra el *hardware* para adscribirse a este sistema de alerta. ¿Qué hace esto? Se coloca una sonda en la salida de internet del organismo, la sonda ve lo mismo que ve el proveedor de servicios de internet y se cargan una serie de reglas de las que estamos seguros que son *malware* que está activo en ese momento del día; las reglas se van cambiando a diario y con eso se van monitorizando incidentes. Por dar algunos datos, les diré que tenemos 13 comunidades autónomas y dos servicios de salud, 24 diputaciones y ayuntamientos, 18 universidades, un montón de empresas públicas y una serie de puertos del Estado, más toda la Administración General del Estado.

En la pantalla pueden ver las cifras de la administración autonómica y de los órganos constitucionales, por ejemplo Congreso y Senado, que están protegidos por el Sistema de Alerta Temprana en Internet. En la Administración General están cubiertos por supuesto todos los ministerios; por ejemplo, en el Ministerio del Interior tenemos al Cuerpo Nacional de Policía, a la Dirección General de Tráfico, a la Secretaria de Estado de Seguridad, a la Guardia Civil, al Centro Nacional de Coordinación Antiterrorista y a Instituciones Penitenciarias. También podemos ver a los ayuntamientos y a sus empresas de agua o a las propias universidades. Igualmente, se benefician algunas de las empresas del Sistema de Alerta Temprana.

Dicho esto me centraré en un punto importante, un asunto por el que se nos pregunta habitualmente, que es la necesidad de capacitación, de detección de talento, etcétera. Nosotros publicamos en el Boletín Oficial del Estado entre 14 y 17 cursos presenciales en los que se forman unos 500 o 600 funcionarios públicos. Existe un inconveniente y es que por temas presupuestarios y de dietas todos los cursos se hacen en Madrid, y hay comunidades autónomas y ayuntamientos que tienen dificultades para mandar personal a formarse. En la pantalla pueden ver el plan de formación. Se programan una serie de cursos específicos que se nos solicitan, algunos aquí y otros en Iberoamérica. El plan se complementa con una formación *online* —tenemos ahora mismo 10 cursos en marcha— y con una formación a distancia mediante una plataforma de video *streaming*. Además, y para detectar el talento, todo ello se completa con una plataforma donde se establecen retos de ciberseguridad. Ahora mismo hay 4000 usuarios accediendo a esta plataforma Atenea. Cuando se consigue un reto en el que el talento ciber de la persona es muy importante, se le dan una serie de puntos. Y cuando tienen 3000 o 4000 puntos se les considera, tanto para que trabajen con nosotros, como para un proceso de selección. Esta sería la formación.

Son muy importantes los itinerarios en los que se define el perfil cíber de la persona en el sentido de si va a gestionar incidentes, si va a hacer auditorías de seguridad o si se va a dedicar a la arquitectura de seguridad. Lo que todavía no se ha planteado es que ahora mismo tenemos especialistas TIC en la administración, pero no tenemos especialistas de seguridad TIC en la administración, o por lo menos no hay puestos de trabajo específicos para eso.

Por facilitarles algunos números, les diré que hay 300 guías publicadas. En este sentido, muchas veces me hablan de talento, y si la persona que viene a trabajar con nosotros ya lo tiene, está muy bien, pero si no, se le puede formar y se le puede facilitar toda la documentación para que adquiera las capacidades necesarias. Las guías tienen unas 225 000 descargas al año, y creo que este año superaremos esos datos.

Dicho esto, me voy a parar un poco en la normativa que obliga a notificar incidentes. Es decir, como pueden ver en la imagen: Notificación versus intercambio. Ahora mismo tenemos el real decreto, la Ley de

cve: DSCG-12-CM-105

infraestructuras críticas, el Reglamento de protección de datos de la Unión Europea, la directiva NIS de la Unión Europea con su real decreto de trasposición y el Banco Central Europeo, y todos ellos obligan a notificar incidentes, lo que llega a ser un infierno para el organismo o la empresa en cuestión. Por ello, estamos intentando ir a una plataforma de notificación única, que se representa de forma gráfica en la imagen que ven en la pantalla. Así, una empresa de infraestructuras críticas tiene que notificar a mucha gente —aparece en rojo—; si eres un organismo público, las notificaciones que se han de hacer aparecen en azul; si eres un proveedor de servicio esencial, tus notificaciones aparecen en negro; y, si eres una empresa pública o una empresa privada, las notificaciones aparecen en distinto color. Por tanto, necesitamos algo para que el organismo se dedique a lo que se tiene que dedicar; y si sufre un incidente lo tiene que resolver y reducir el impacto. Así pues, vamos a ir a una plataforma, a la que llamamos LUCIA, donde la notificación se hace por defecto y va directamente a la autoridad que lo necesita, de manera que el organismo solo tiene que notificar una vez. Por ejemplo, en el campo del Ministerio de Defensa, las Fuerzas Armadas notifican al mando conjunto ciberdefensa, y de ahí va a nuestra LUCIA central; si es una comunidad autónoma —por ejemplo, Andalucía—, el proceso es similar a través de las diputaciones y los ayuntamientos; y si es un ministerio o un organismo del Estado, se hace a través de la Secretaría General de Administración Digital. Esta capacidad ya está incorporada a la misma herramienta y, además, tienen constancia de esta herramienta tanto el Centro Nacional de Protección de Infraestructuras Críticas como la Agencia Española de Protección de Datos, que pueden recibir las notificaciones vía portal web o vía los organismos públicos, a través de esta plataforma LUCIA. Con esto conseguimos una notificación única; que el organismo o la empresa manden la notificación y le llegue a la autoridad responsable, sin que tenga que estar notificando multitud de veces. En el caso de la Secretaría General de Administración Digital será el SOC-AGE el que aglutine todo esto.

En cuanto a ciberincidentes, voy a dar dos ideas. Todo lo escribimos normalmente en las tendencias que figuran en el informe que les muestro. Este informe, que es el ejecutivo, está colgado en el portal web, y luego hay otro un poquito más voluminoso, de 200 páginas, que desarrolla todo esto un poco más en detalle. En este informe decimos que los incidentes están creciendo. Así, en 2017 se notificaron 26 000 incidentes, pero con esto no quiero crear alarma porque también hemos mejorado mucho la capacidad de detección, con lo cual es normal que crezcamos en cuanto a notificaciones. Además, también hay otra cosa muy importante, y es que a través de la plataforma Lucia los organismos nos mandan ya casi 10 000 incidentes. Es decir, que ya tenemos una realimentación de abajo arriba con todos los incidentes que están sufriendo estos organismos.

Para ponerlos en su justa medida, nosotros categorizamos o clasificamos los incidentes en cinco niveles: bajo, medio, alto, muy alto y crítico. ¿Y cuáles son los incidentes que a nosotros realmente nos preocupan mucho? Pues los muy altos y los críticos, donde hay compromiso de información, hay algún tipo de cibersabotaje o algún tipo de daño relevante contra alguna institución del Estado o alguna empresa del sector público. Actualmente estamos notificando ya, en 2018, una media de 3000 incidentes, y de esos 3000 incidentes mensuales, 1000 son de los organismos hacia nosotros, que es algo que antes no sucedía.

¿Qué conclusiones sacamos del análisis de todos estos 26 000 o 27 000 incidentes? Pues como le daré a la Mesa la presentación, aquí dejo las definiciones porque para nosotros los conceptos son muy importantes. Muchas veces oímos hablar de ciberterrorismo, y parece que todo es ciberterrorismo, pero nosotros distinguimos, por un lado, ciberterrorismo, y por otro, uso de internet por parte de los terroristas. Yo todavía no he visto ningún caso de ciberterrorismo; será cosa de que mañana tengamos un caso, pero hoy por hoy no ha habido ninguno. Cada vez que han atacado una infraestructura crítica o han atacado a otros países, ha sido otro Gobierno, ha sido el crimen organizado o ha sido alguien que quería hacer daño, pero no han sido los terroristas, a los que todavía no se considera con la capacidad técnica suficiente.

Así, nosotros establecemos que nuestra principal preocupación es el ciberespionaje; la segunda, el ciberdelito; la tercera, la ciberguerra, el ciberconflicto, la guerra híbrida, el ataque a infraestructuras críticas o la desinformación, que ha crecido muchísimo porque estaba en quinto lugar el año pasado y ha pasado al tercer lugar; la cuarta, el uso de internet por los terroristas, sobre todo las comunicaciones entre ellos, la obtención de información, la propaganda o los procesos de erradicación; la quinta, el ciberactivismo; y, la sexta, el ciberterrorismo.

En tendencias con respecto a este año, han crecido muchísimo, sobre todo, los casos de ciberguerra, los casos de ciberespionaje y los casos de uso de internet por los terroristas. El ciberactivismo bajó en su

cve: DSCG-12-CM-105

día, pero ahora, con todos los asuntos de la operación Cataluña en España, hemos sufrido un repunte. El ciberterrorismo sigue estable, en unos niveles por ahora, gracias a Dios, bajos.

Siempre hago una alerta especial a los usuarios internos. Todos estos actores pueden utilizar a los usuarios internos. Manipulados adecuadamente, los pueden utilizar para atacar el sistema. Si a mí me infectan las redes de dentro es muy difícil que yo pueda determinar cuál es el origen de la infección, con lo cual el organismo tiene que aplicar muchas medidas de seguridad.

Dicho eso, y deteniéndome en los incidentes muy altos o críticos, esto es lo que vimos el año pasado: lo de abajo son incidentes esponsorizados por Estados, los famosos casos de ciberespionaje. Lo de arriba son otros incidentes que en un principio pueden tener o no tener valor. Ahí hay un error, porque eso de LexNet y la bandera de Rusia no es verdad. Eso se ha colado, se ha ido de un sitio para otro.

Nos vamos a los incidentes de arriba. Muchos tuvieron bastante eco mediático. Tenemos ahí el caso de WannaCry, el caso del NotPetya. Nosotros sufrimos muchos en marzo de 2017 con un incidente que se llama Struts. ¿Por qué? Porque esa tecnología la utilizan casi todas las páginas web de las administraciones públicas y nos hicieron un ataque por una falta de actualización que derribó bastantes páginas web. Y luego tuvimos el caso de la operación Cataluña.

Dicho eso, aquí tenemos muchas de las cosas que he ido comentando antes: desinformación en el caso de Grizzli Steppe. En el caso de elecciones USA, ¿por qué hemos plasmado aquí este incidente? Porque hubo cinco IP españolas de ayuntamientos y pequeñas empresas que utilizaron el ciberatacante para filtrar información del Partido Demócrata. Tenemos casos de demostración de fuerza, casos de sabotaje y muchos casos, por desgracia, de espionaje. En el caso de operación Cataluña, tenemos un caso de desinformación y también de potenciación de un relato.

Me voy a parar en dos de ellos. El más mediático fue WannaCry. ¿Qué pasó en WannaCry? Pasó que se publicaron dos vulnerabilidades —hay que reconocerlo— especialmente graves, dos vulnerabilidades que nos permitían progresar por la red corporativa prácticamente sin conocimiento de los administradores, y esas vulnerabilidades se publicaron en marzo. En abril, el atacante publicó la manera de atacar usando esas vulnerabilidades y el 12 de mayo apareció el caso de WannaCry. Tuvimos dos meses para actualizar y no actualizamos con la debida diligencia. Eso nos lo tenemos que poner, tanto las empresas como las administraciones, en el debe. También es verdad que Microsoft, que es el caso de esta tecnología, cuando actualiza lo hace sobre las últimas versiones, en este caso sobre Windows 7 y sobre Windows 10, y hay muchas administraciones y empresas que todavía están soportando sistemas operativos, que le llaman *legacy,* que son antiguos y que no pueden actualizar porque el fabricante no les proporciona la actualización.

La secuencia de hechos es la siguiente: el 12 de mayo nos llegó el aviso de Telefónica, que nos mandó la muestra. Nosotros la comprobamos en los motores antivirus y más del 60 % de los antivirus no lo detectaban. A media tarde generamos la primera vacuna y empezamos a alertar a las administraciones públicas y a mandarles los informes pertinentes. Durante todo el sábado se mejoró esa vacuna y se le puso hasta nombre, NoMoreCry, y a partir de ahí estuvimos informando a las administraciones y dándoles soporte sobre cómo instalarla y sacando versiones para Windows XC, para Windows 2000, para Windows 98, para que se pudiera parar. A partir del lunes, martes y miércoles, que eran los días 15 y 16 —el día 15 era fiesta en Madrid, San Isidro, por lo que en la Administración general no se trabajaba—, trabajamos con el resto de administraciones autonómicas y locales y el día 16 estuvimos centrados en la Administración General del Estado, que era la que entraba a trabajar en Madrid.

¿Cómo infectaba este *malware*? Infectaba haciendo un escaneo en internet y, cuando veía un equipo vulnerable, lo atacaba con el programa y lo infectaba. No mandaba correos y el usuario no tenía que abrir nada. Por desgracia, era así de letal. El organismo que tenía un equipo expuesto caía. ¿Qué les pasó a los hospitales británicos? Los hospitales británicos tenían muchos servicios expuestos en internet y, además, entre ellos se intercambiaban los expedientes clínicos utilizando los protocolos de Microsoft. Pero eso hay que usarlo en las redes internas, no en las redes externas. Por eso, infectaron varios con el suficiente impacto: cambia enfermos o urgencias que vienen a los hospitales a otros hospitales, con lo cual el daño pudo ser muy grande. En España tuvimos cuatro o cinco incidentes muy localizados en alguna ambulancia o en algún ordenador aislado, pero no tuvimos ningún impacto de consideración en el sector público. No podemos hablar del sector privado, porque ya conocemos el caso de Telefónica.

El segundo caso —aunque a nosotros no nos afectó, en España no afectó al sector público, pero sí afecto a algunas partes de España— fue de cibersabotaje. ¿Cómo fue la infección? Un atacante manipula un software de contabilidad, lo coloca en el repositorio, todo el mundo se lo descarga y cuando lo instala

cve: DSCG-12-CM-105

se queda infectado. ¿Qué hacía? Sacaba un pantallazo, pero, además, era un *malware* completamente destructivo, no quería pedir rescate, no quería pedir nada, lo único que quería el *malware* era destruir o dificultar el reinicio de todos los ordenadores. Tenemos aquí el caso de este centro comercial, donde todos los cajeros estaban infectados por este *malware* y el dato más característico fue el de la empresa Maersk. La naviera Maersk, conocida por su logística, tiene una terminal entera en el puerto de Barcelona, con lo cual se vio afectada y en el Foro Económico Mundial el CEO de Maersk reconoció el error y la llamada de atención, porque perdió bastante dinero en todos estos procesos.

Dicho eso, ¿a qué nos enfrentamos? Nos enfrentamos a una sensibilización de autoridades, a mejorar las capacidades de vigilancia, a mejorar el intercambio, a forzar a las administraciones a certificarse en el ENS, y ya le unimos la protección de datos, al uso de productos certificados y a una cooperación público-privada mucho más extensa.

Muchas gracias.

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

Iniciamos ahora el primer turno de intervenciones de los portavoces. Empezamos por el Grupo Mixto. Tiene la palabra le señor Yanguas.

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

Quiero agradecer al señor Candau, jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional, sus explicaciones y el PowerPoint que ha proyectado en esta comisión. Creo que serán aportaciones valiosas para el documento que esta comisión, en el marco de la ponencia sobre ciberseguridad, tiene que redactar y después aprobar. Simplemente intervengo para mostrarle mi agradecimiento, pero tengo una pregunta: a la vista de todas las empresas públicas e instituciones que protege el Centro Criptológico Nacional, quería saber, ya que mi partido es Unión del Pueblo Navarro, si en la Comunidad Foral de Navarra tienen ustedes adscrita, por llamarlo de alguna manera, alguna empresa pública o la propia Administración foral o tienen alguna empresa de la Comunidad Foral de Navarra. Quiero decirle que en mi grupo, Unión del Pueblo Navarro, estoy yo solo y tengo ahora otra comisión, por lo que tendré que leer su respuesta después en el *Diario de Sesiones*, si tiene a bien usted responderme.

Muchas gracias. Buenos días.

El señor **JEFE DEL DEPARTAMENTO DE CIBERSEGURIDAD DEL CENTRO CRIPTOLÓGICO NACIONAL** (Candau Romero): Muy bien. Con respecto a las comunidades autónomas…

El señor **PRESIDENTE:** Perdón, señor Candau, vamos a dejar que hablen los portavoces, toma usted nota y contesta luego a todos. Si no se hace así, esto se eterniza.

Por el Grupo de Esquerra Republicana de Cataluña, tiene la palabra el señor Castellana.

El señor **CASTELLANA GAMISANS:** Gracias, presidente.

Hoy en día en que la ciberseguridad es un fenómeno global, una necesidad global, quería preguntarle por la cooperación con otros países de la Unión Europea, así como por la cooperación con la Agencia de Ciberseguridad de Cataluña y el cos de Mossos d'Esquadra. Y también, aunque parcialmente ya ha respondido, querría preguntarle sobre los actores que protagonizan los ataques. De su presentación se deduce que básicamente son actores estatales y crimen organizado, ¿no sería interesante hacer más publicidad de los objetivos que tienen esos ataques? ¿Qué margen tiene la diplomacia para atajar estas cuestiones? Cuando el régimen sirio utiliza armas químicas contra su población, se publicita y hay acciones diplomáticas. El problema de los ciberataques es que los ciudadanos perciben que la principal amenaza es el terrorismo cuando, en el fondo, la principal amenaza de seguridad en nuestro mundo hoy en día son los organismos estatales.

No quería entrar en este tema, pero usted ha mencionado la operación Cataluña, y me gustaría que me diese más detalles sobre qué es eso de la desinformación y la creación de relato, porque cuando técnicos, por ejemplo, del Real Instituto Elcano, han ido al Reino Unido a explicarse, han hecho el ridículo ante la Cámara británica, o cuando un ministro de Exteriores del Reino de España se va a la BBC, le enseñan fotos y dice que esas fotos son falsas, le dicen: no, no, son fotos de nuestros reporteros. De hecho, aquí mismo, en esta misma sala, el ministro del Interior del anterior Gobierno nos enseñó una foto que también era falsa; la foto era cierta, pero estaba descontextualizada. Por tanto, le pregunto si el tema de desinformación y creación de relato no se debe a una visión sesgada, porque, al final, yo, como

cve: DSCG-12-CM-105

parlamentario, no tengo ninguna información ni datos fehacientes de ninguna institución estatal que me lleven a pensar que hay una campaña de desinformación y creación de relato a favor de la constitución de la república catalana y que no sea precisamente al revés.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.

Tema interesante este del *storytelling*.

Tiene la palabra ahora el representante de Ciudadanos, señor Salvador.

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

Señor Candau, bienvenido a esta comisión, aunque ya se lo han dicho el presidente y el resto de los comparecientes. Me han parecido muy interesantes sus aportaciones y el trabajo que está realizando el organismo que usted dirige.

Como ya hemos tenido bastantes comparecencias y cada una con representantes de distintos organismos y con distintas visiones que están aportando mucho al posicionamiento final de la ponencia, quiero resaltar que toda la estructura de organización de la seguridad en este momento está bastante bien encaminada dentro de las respuestas que hay que dar a los retos que tenemos por delante. Esa es una cuestión que usted ha explicado, cómo estamos funcionando con esa estructura y la coordinación que ustedes también asumen, y en ese sentido estamos tranquilos porque el camino es el adecuado para responder a esos retos. Pero me gustaría que nos ilustrara un poco más, pues casi todos los temas que ha mencionado, aunque realmente son importantes, se quedan fuera de esas notificaciones de incidentes. El hecho de que la gente tenga que notificar los incidentes que reciben nos da las acciones concretas que se están realizando y que están afectando para poder hacer un seguimiento, hacer la trazabilidad para ver de dónde proceden y cómo se puede actuar con las personas que están haciendo esos ataques. Todo eso estaría recogido en su intervención, pero todos los comparecientes han relatado, y usted también, que no existen especialistas, dentro de la flexibilidad que entendemos que tiene que tener todo esto, porque si se diera una formación muy concreta probablemente quedaría desfasada y habría que estar actualizando permanentemente a esos especialistas. ¿Qué medidas cree usted que tendría que adoptar el Estado? Porque todo el mundo detecta que hay falta de especialistas y ustedes están haciendo su cuota para intentar dar formación a técnicos de la Administración del Estado y reconvertirlos, pero ¿qué cree que tendrían que hacer las universidades y la política educativa del país? Hay que ver cómo lo público-privado puede funcionar para garantizar esos especialistas de futuro, porque en un momento en el que la automatización va a provocar la pérdida de empleos, esos especialistas pueden constituir una fuente de empleo de alta calidad. ¿Qué ideas tiene sobre eso?

Ha hablado de que nuestro esquema facilita el que se aporten medidas para defender a la Administración, para defender a las empresas, para defender a las infraestructuras críticas, para defender todo aquello que es cuestión de Estado, pero tendríamos que avanzar un paso más, dentro de que lo que se está haciendo, por prioridad, seguramente es lo posible. ¿Qué tendríamos que hacer para pasar al siguiente paso, que sería proteger a las personas? ¿Qué compromisos hay que adquirir con las operadoras de telefonía, con los suministradores? Porque los grandes olvidados, por la magnitud de esta comunicación total en la que estamos viviendo, terminan siendo las personas que también están recibiendo ataques, cambios en su reputación o problemas derivados de los que estamos viviendo a nivel macro. ¿Cuál sería su visión sobre eso?

Ha dicho también —y creo que es muy significativo, lo han dicho otros comparecientes y de ello somos plenamente conscientes— que cuando hablamos de ciberterrorismo, de actividades que se podrían entender como de agresión a otros Estados y a determinados niveles, una parte importante son producidas por Estados. Eso lo sabemos todos, es algo que se publica sin ningún pudor porque es normal, pero después no tiene ningún tipo de repercusión. ¿Usted cree que tendría que existir en Naciones Unidas, en el organismo correspondiente a nivel de la Unión Europea, algún tipo de convención o de conferencia en la que se adopten acuerdos para dar respuesta a lo que el mundo digital nos está exigiendo? Ya he dicho en alguna ocasión que la Convención de Viena regulaba qué hacer en caso de conflicto bélico, pero ¿qué se hace cuando un Estado está agrediendo a otro Estado, está intentando debilitar sus defensas, robar información o cualquier otra cuestión? Entiendo que es más difícil declarar una guerra por uno de estos motivos, pero la comunidad internacional tendría que adoptar unas normas éticas, unas normas mínimas. ¿Cuál es su opinión al respecto?

cve: DSCG-12-CM-105

Para terminar, en relación con la intervención anterior, noticias falsas han existido toda la vida, eso está más claro que el agua, siempre han existido noticias falsas, lo que no ha existido nunca es la capacidad que hay hoy para que esas noticias falsas se conviertan en el relato definitivo de cualquier historia. Siempre ha habido ataques a la reputación de empresas, ataques a la reputación de personas, pero en este momento la capacidad tecnológica ligada a la comunicación permite que se pueda alterar el comportamiento electoral dentro de una democracia o el comportamiento de la Bolsa en un momento determinado haciendo circular bulos. Todos hablamos de eso, de noticias falsas, *fake news,* por tanto, ¿qué cree que habría que hacer para atajar algo que es muy complicado pero que tiene unas consecuencias graves? Usted ha descrito varios ataques a escala mundial, la importancia que han tenido y su repercusión económica, pero el gobernar un país como Estados Unidos tiene una repercusión para el planeta mucho más grande que cualquiera de los ataques que hemos mencionado, y exactamente igual podríamos poner ejemplos en cualquier punto del mundo. Es un tema de primerísimo nivel, porque solamente nos preocupamos de hacer algo cuando el río suena, pero a nivel macro, ¿qué cree usted que hay que hacer incluso a nivel de los Estados para intentar que ese relato no pueda ser tergiversado por unos cuantos especialistas en la red con una intencionalidad aviesa?

Muchas gracias.

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

Quisiera aprovechar la intervención del señor Salvador para anunciar algo que pensaba decir después. Como ustedes saben, en el anterior periodo de sesiones se creó un grupo de trabajo sobre noticias falsas en el Congreso de los Diputados. El Ministerio de Defensa ha dicho que no tiene interés en ese grupo y, por tanto, la comisión parlamentaria correspondiente tampoco. Por ello, los grupos parlamentarios deberían pensar si quieren hacer algo al respecto. No obstante, el señor letrado ya está realizando las gestiones necesarias para traer a alguna persona. Ya hablaremos de ello.

Siento haber interrumpido la comisión, pero me pareció necesario señalar esta cuestión al hilo de la importante intervención del señor Salvador, a quien doy las gracias por sus palabras.

A continuación, tiene la palabra el senador Comorera.

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

Muchas gracias, señor Candau, por la interesante exposición que ha realizado en la mañana de hoy.

En casi todas sus intervenciones en diferentes foros hemos visto que insiste en poner el énfasis en la ausencia de precaución de muchas empresas a la hora de prevenir ataques informáticos y de destinar recursos suficientes. Se gastan mucho en la seguridad tradicional y no hacen lo mismo en esta materia, insistiendo siempre en la necesidad de incrementar la capacidad defensiva.

En cuanto a la inversión —y esta es una pregunta que acostumbramos a realizar a todos los comparecientes, más aún si nos comparamos con países como el Reino Unido y Estados Unidos—, ¿tenemos un problema grave por la falta de inversión en ciberseguridad? Además, dado el alcance que tiene hoy en día la utilización de las redes en el ámbito social, y al hilo de la ciberseguridad, así como del hecho de que entre sus funciones se encuentra la formación del personal especialista en seguridad de la Administración, ¿cree que es suficiente lo que se dedica presupuestariamente a esa formación o que es necesario aumentar la formación a las fuerzas y cuerpos de seguridad del Estado y a la Administración en general en el desarrollo de nuevas tecnologías para que puedan alcanzar los conocimientos, las habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad?

Por otra parte, dado el modelo mixto de protección que tiene España ante los ciberataques, y teniendo en cuenta que aproximadamente el 80 % de las infraestructuras críticas corresponden al sector privado y que usted siempre señala la necesidad de compartir información, tanto de ciberamenazas como de ciberincidentes, ¿cómo valoraría la cooperación actual entre el sector público y el privado en el intercambio de esa información? En general, ¿cómo valora la implantación del esquema nacional de seguridad y qué cree que debería hacer el Poder Legislativo para potenciar esa cooperación —si es que hay que hacer algo—, como, por ejemplo, las certificaciones del esquema nacional de seguridad?

Leía esta semana que, según un informe sobre amenazas informáticas a través del correo electrónico —hecho público por la compañía de seguridad informática FireEye—, dos tercios del tráfico mundial de *emails* está infectado. ¿Hay realmente más ciberataques o ciberincidentes o es que se están reportando actualmente más ciberataques que antes? ¿Han perdido el miedo o las reticencias las empresas por la

cve: DSCG-12-CM-105

pérdida reputacional que supone el reporte de este tipo de ciberataques? Me gustaría conocer su opinión al respecto.

La semana pasada leía también un tuit del Centro Criptológico Nacional sobre el *cryptojacking,* que definen como la amenaza basada en la utilización de forma ilegítima de un equipo por parte de los cibercriminales para realizar el proceso de obtención de criptomonedas y obtener el total de las ganancias. En el tuit se hace referencia a un nuevo informe de amenazas, a cómo funciona, cuáles son los fundamentos que hay detrás, qué procedimientos siguen los ciberdelincuentes para propagar la infección y las medidas que es necesario tomar para protegerse. En definitiva, del tuit y del informe se desprende que se califica el *cryptojacking* de ciberdelito. Sin embargo, según me consta, la fiscal de sala en materia de delitos informáticos no lo tiene claro todavía. No obstante, algunas páginas lo advierten en su tipo de servicio. La pregunta es por qué se deja a la justicia, y en concreto a la Fiscalía, fuera de la colaboración en un ámbito tan importante como la ciberseguridad. Al menos, esa es la impresión que a nosotros nos da. En este sentido, nos podríamos plantear preguntas como, por ejemplo, si es relevante la ralentización de la máquina afectada para considerarlo un delito, conforme al artículo 264.bis del Código Penal, que castiga la obstaculización o interrupción del funcionamiento de un sistema informático ajeno. Lo mismo ocurre con el llamado *hacking* ético y las dudas que surgen sobre su castigo, sobre lo que también me gustaría conocer su opinión. En definitiva, lo que nos preocupa —y me consta que a miembros de la judicatura y la fiscalía también— es que el CCN-CER se convierta un poco en juez, jurado y ejecutor en temas de ciberseguridad.

Y para terminar, una última pregunta: si el reto fundamental de la ciberseguridad estatal es el de proporcionar servicios horizontales mucho más proactivos, ¿qué supone la implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado ante este reto?

Muchas gracias.

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

Por el Grupo Parlamentario Socialista, tiene la palabra el senador Raffo Camarillo.

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

En primer lugar, como no podía ser de otra manera, quiero agradecerle al señor Candau su presencia. Me gustaría que les trasladase a los profesionales del Centro Criptológico Nacional nuestra felicitación por el trabajo que realizan.

En nuestra opinión, en un periodo relativamente corto de tiempo, España ocupa un lugar importante en cuanto al desarrollo en relación con el resto de países de la comunidad internacional. Esto es fruto de decisiones políticas, que establecieron en su momento la prioridad de desarrollar este campo y, cómo no, al trabajo de mejora continua y de implicación diaria realizado por los propios profesionales, labor por la que les tenemos que felicitar, pues podemos decir que estamos en buenas manos. Muchas gracias.

Como intervengo en penúltimo lugar, ya han surgido en las intervenciones de mis compañeros cuestiones por las que yo le iba a preguntar, por lo que me voy a centrar en dos o tres aspectos que aún me quedan pendientes. En primer lugar, según su experiencia en cuanto al recorrido de la organización y su visión estratégica sobre lo que se aventura a corto y medio plazo, ¿cuáles serían los dos o tres aspectos organizativos y de desarrollo de nuestras estructuras y capacidades más importantes que habría que potenciar? En segundo lugar, me gustaría que nos dijera cuáles son los elementos que habría que mejorar en la coordinación con la Unión Europea, considerándola como un todo único, para trabajar de forma conjunta en alianza con el resto de Estados. Finalmente —y teniendo en cuenta una de las diapositivas que ha expuesto—, he leído que es importante el papel de los Estados en relación con las ciberamenazas, ciberataques o la desinformación, pero no que estos ataques ocuparan con diferencia la primera posición en relación con los que se producen por otro tipo de agentes. En este sentido, existe cierta dificultad a la hora de establecer alianzas, consensos, cooperación, etcétera, para hacer un frente común, como ocurre, por ejemplo, con el terrorismo o el crimen organizado en el ámbito internacional. Por tanto, me gustaría que valorase cuál es el nivel de desarrollo de las alianzas de los organismos internacionales con otros Estados de la comunidad internacional a la hora de mantener una defensa común respecto a algunos aspectos relacionados con la ciberseguridad mundial.

Por último —creo que ya se lo han preguntado, pero es mejor insistir—, me gustaría preguntarle por la coordinación, la colaboración y las alianzas con el sector privado, que tiene una vinculación directa con lo que se consideran infraestructuras críticas. ¿Qué aspectos serían mejorables desde su punto de vista?

Muchas gracias.

cve: DSCG-12-CM-105

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

Para terminar este turno de portavoces, tiene la palabra la diputada señora Vázquez, del Grupo Parlamentario Popular.

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

Quiero dar la bienvenida a esta comisión al señor Candau. Sin lugar a dudas, la suya ha sido una explicación y una comparecencia importante, en la que hemos tomado buena nota de todo cuanto ha dicho y que va a complementar mucho los trabajos de esta ponencia.

En cuanto a la propuesta de estudio por parte de esta comisión de noticias falsas, a la que se refería el señor presidente de la comisión, quiero señalar que el Grupo Parlamentario Popular está totalmente de acuerdo y así lo ha transmitido el portavoz adjunto de esta Comisión de Seguridad Nacional, que hasta hace poco fue el portavoz de Defensa y gran defensor de que se creara esta comisión de estudio que, finalmente, no se ha creado. No obstante, nosotros sí la apoyamos.

La ciberseguridad, como saben, es un asunto prioritario para la Unión Europea, y así lo ha puesto de manifiesto el presidente Juncker en el discurso de ciberseguridad para el Estado de la Unión de 2018, donde señaló que era una cuestión prioritaria para los Estados y manifestó la obligación de los Estados de crear un centro nacional de coordinación entre los 660 centros nacionales que hay.

También hace un llamamiento de cara a las futuras elecciones al Parlamento Europeo y dice que hay coordinar y cooperar ante posibles injerencias o cualquier tipo de acontecimiento anómalo que suceda en ese proceso electoral. Por eso, me gustaría saber si en España ya existe o se va a poner en marcha algún instrumento de cara a esos procesos electorales. Y también le pregunto si, a raíz de los últimos acontecimientos sucedidos en Cataluña, se han producido o el Centro Criptológico Nacional tiene constancia de posibles injerencias de otros países.

Ahora está muy de moda hackear a sociedades abiertas a través de sociedades autoritarias, así que también me gustaría saber si el Estado tiene algún tipo de estrategia para frenar ese tipo de injerencias de esas sociedades autoritarias a nuestras sociedades abiertas y demócratas.

Y, dicho esto, voy a poner sobre la mesa una serie de datos que me hacía llegar el otro día una persona a través de internet, que ponen de manifiesto a lo que nos estamos enfrentando. Me decía: en el minuto en que llevo interviniendo ya se han subido cuarenta y ocho horas de vídeos a YouTube. Eso es tremendo. El 68,5% de la población española ya está conectada a internet. La segunda plataforma de anuncios ya es internet; ya nadie paga en televisión ni en prensa escrita, ahora ya todo es internet. Podríamos decir que el 96% de los jóvenes ya están conectados. Estamos en un ciberespacio que no tiene límites geográficos. Hay un catálogo de ciberamenazas que por primera vez usted ha clavado; y yo también hago una diferenciación siempre que se puede entre ciberespionaje, ciberdelito, ciberactivismo o ciberterrorismo, porque no podemos mezclar todas esas cosas.

El Grupo Popular también habla —y algunos se ríen en esta comisión— de amenazas de seguridad, que son tierra, mar, aire y espacio, y por eso hemos creado esta ponencia. Nosotros somos conscientes de que las nuevas tecnologías e internet producen competitividad y prosperidad, pero también dependencia y vulnerabilidad, y tenemos que reaccionar y hacer frente a esa vulnerabilidad. Recientemente —el 7 de septiembre— el Gobierno aprobó el Real Decreto 12/2018, de transposición de la Directiva NIS, y es importante que se ponga en marcha esa directiva. Nosotros creemos que las empresas deben estar obligadas a comunicar cualquier tipo de incidente a la mayor brevedad posible. Yo sé que desde el punto de vista de la publicidad a lo mejor a una empresa no le va bien porque supone que se la cuestione, pero de ese modo se pueden evitar males mayores. Por tanto, insisto en que el Grupo Popular considera que las empresas deben hacerlo.

Aunque aquí se ha hablado de si se invierte poco o se invierte mucho, en el mes de julio leía que el FBI ponía como ejemplo a España en materia de cooperación contra ciberataques, es decir, que lo estamos haciendo bien. Efectivamente, no tenemos los recursos que tiene Israel, que creo que es el país del mundo que más invierte en ciberseguridad, pero lo estamos haciendo bien cuando fuera de las fronteras españolas se reconoce que somos de los mejores. En cualquier caso, tenemos que ser todavía mejores: más eficientes y más eficaces.

Para finalizar, le voy a formular una serie de preguntas. En primer lugar, si considera que el nivel de cumplimiento de las administraciones públicas en el esquema nacional de seguridad es el correcto —y me refiero a todos los niveles de la Administración; ya he visto que hay comunidades y ayuntamientos que no están—. Repito que quisiera saber si usted considera que el cumplimiento está bien o no. Y aquí estamos

cve: DSCG-12-CM-105

para eso: no solo para que nos digan las cosas buenas que hacemos, sino también las malas, porque tenemos que aprobar una ponencia y unas conclusiones.

Por otro lado, me gustaría saber si cree que las administraciones públicas disponen del nivel de talento suficiente como para afrontar con garantías de éxito los retos a los que obliga a las administraciones el real decreto que acaba de aprobar el Gobierno. También, si considera efectivos los sistemas de reclutamiento de talento para los cuerpos TIC de la Administración General del Estado. Si cree que las actuales estructuras organizativas de las administraciones son las adecuadas para afrontar los nuevos retos estratégicos y objetivos de la ciberseguridad y la futura estrategia. Si considera valiosa la creación de algún canal de integración de la sociedad civil en defensa del dominio de ciberespacio como una ciberreserva. En este sentido, este grupo parlamentario, tanto en el Congreso como en el Senado, es defensor de una ciberreserva, pero queremos saber los pros y los contras y si usted estaría a favor de ella. Asimismo, si podría darnos razón del nivel de cumplimiento de los artículos 27 y subsiguientes de la Ley de seguridad nacional. En qué estado de desarrollo se encuentra el catálogo de recursos para la seguridad nacional. Y si considera suficientes y adecuados los posibles recursos humanos detectados e incorporados a los antedichos recursos.

Por mi parte, nada más. Le agradezco su comparecencia; y si no me puede responder ahora todas las preguntas lo puede hacer por escrito sin ningún tipo de inconveniente.

Muchísimas gracias.

El señor **PRESIDENTE:** Gracias, señora Vázquez.

Tiene la palabra el señor Candau para dar satisfacción a las preocupaciones de sus señorías.

El señor **JEFE DEL DEPARTAMENTO DE CIBERSEGURIDAD DEL CENTRO CRIPTOLÓGICO NACIONAL** (Candau Romero): Muy bien, contestaré por orden, siendo breve.

El representante de Unión del Pueblo Navarro me preguntaba si la Administración foral está adscrita al SAT de internet. He dicho que había trece comunidades; seis no están adscritas a él, pero tres comunidades de esas seis que faltan, que son Cataluña, la Generalitat Valenciana y Andalucía, tienen un CERT propio, con el cual estamos federados y compartiendo incidentes, por lo que en un principio recibimos de esos incidentes. Galicia y Navarra, que tampoco están federadas, no tienen un CERT reconocido pero sí un centro de operaciones de seguridad, al igual que Madrid, con los cual también federamos incidentes. Así pues, en un principio tenemos aceptablemente cubiertas todas las comunidades autónomas y ciudades autónomas con respecto al intercambio de incidentes. Es cierto que en el Ministerio de Política Territorial y Función Pública hay un grupo de trabajo *ad hoc*, el grupo de trabajo de seguridad, que preside el Centro Criptológico Nacional, compartido con la Secretaría General de Administración Digital, y en principio estamos bastante coordinados con las comunidades autónomas. Allí asisten también la Federación Española de Municipios y Provincias y la Conferencia de Rectores. Así pues, al menos ponemos las cosas en común; otra cosa es que tengamos recursos para resolverlas.

El representante de ERC me preguntaba por la cooperación con otros países de la Unión Europea. La cooperación se hace de manera fluida, pero en los veintiocho países de la Unión Europea hay diferentes niveles de madurez en la capacidad de respuestas. A nosotros nos gusta intercambiar con los que realmente cuando intercambias los dos ganan; no puedes intercambiar y estar dando tu información y que sea como tirar cosas a un pozo y que además no se oiga si la piedra cae o no en el agua. Como uno de los objetivos de la Directiva NIS es tener la red de C SIRT con los veintiocho países, tenemos que trabajar mucho en que los países con menos madurez ganen madurez para que en algún momento el intercambio sea fluido y en los dos sentidos; si no, es bastante desalentador.

Con respecto al Cesicat, creo que ya he respondido antes. Nosotros hemos trabajado bastante bien con Cesicat, y la última actuación fue la vigilancia conjunta del proceso electoral en Cataluña el 21 de diciembre.

También me ha preguntado por las acciones diplomáticas y los ataques de Estados. Esto —lo han preguntado varios grupos— es un asunto controvertido porque en el ciberespacio, primero, la atribución es muy difícil. Aunque creamos o estemos seguros de que puede ser de un país, es muy difícil demostrar que el ataque es de él. Y luego es muy difícil demostrar que son individuos los que nos están atacando o que nos está atacando el propio Estado, con lo cual, como es muy difícil la atribución, es muy difícil la respuesta. En la OTAN hay un debate continuo a costa del artículo 5 y sobre cuándo se ataca a un Estado y cuándo tenemos que responder, y la ciberseguridad entra en una escala de grises espectacular. Eso nos pasa también en otros foros. Algunos países están intentando un código de buenas prácticas en el

cve: DSCG-12-CM-105

ciberespacio a través de Naciones Unidas, la Unión Europea intenta dar un impulso en ese sentido, pero internet crece muy rápidamente, la presencia en internet, más aún, y todavía no se ha llegado a una estabilización y un acuerdo.

Por otro lado, cuando nosotros hablamos de la operación Cataluña la circunscribimos a los ataques que se reciben en las administraciones públicas. En ese caso, desde el 1 de octubre hasta el 21 de diciembre, por poner un marco temporal, se recibieron ataques en setenta y cinco organismos del Estado. Y cuando hablamos de desinformación y potenciación del relato decimos eso, porque nosotros de desinformación no hablamos. El CCN-CERT no habla de desinformación porque nosotros nos ceñimos a los ciberataques. No sé si la desinformación es de la *A*, de la *B* o de en medio. No hablamos de eso, pero es cierto que tenemos una demanda creciente de vigilancia de procesos electorales. Ahora, un montón de países iberoamericanos —por ejemplo, estuvimos desplegados en Colombia hace dos meses— nos piden que les ayudemos a auditar sus sistemas de recuento electoral e incluso vigilar que el sistema de recuento electoral no reciba ataques. Nosotros hacemos eso normalmente en todas las elecciones generales y en algún momento, cuando se nos apoya, en otro tipo de elecciones, aquí, dentro de España; pero ahora se nos está pidiendo fuera. Nosotros vigilamos e intentamos que al menos el proceso electoral no reciba ataques. De lo que no podemos opinar —y pasó en las elecciones americanas— es de lo que se llama *hack a link:* te hackean la página web del partido político, muestran datos y pueden orientar —o no— la intención de voto de los ciudadanos. Ahí mi recomendación para los partidos políticos es que hay que protegerse y recibimos muchas llamadas de todos los partidos políticos de la Cámara. Y es que esa persona que ahora mismo es jefe del partido va a ser luego el presidente del Gobierno; si te han hackeado antes y tienen información que luego pueden filtrar, pues la cosa... En fin, creo que las medidas de seguridad también se aplican a los grupos políticos.

Ciudadanos ha hablado de la estructura adecuada y ha preguntado si existen o no especialistas. Creo que las universidades están respondiendo rápidamente a una necesidad de ciberseguridad promoviendo másteres, asignaturas, etcétera, pero nos referimos a que nos hace falta un poco más de talento o un talento más especializado en cada una de las disciplinas. Nosotros lo intentamos cubrir con nuestros cursos, pero también es cierto que el especialista de ciberseguridad actualmente está muy cotizado. Las mismas empresas técnicas que nos dan los servicios de ciberseguridad están sufriendo una fuga de talentos importante, entre ellas y hacia fuera. Y, claro, cuando me hablan de la Administración digo que la Administración paga lo que paga, con lo cual, competitivos competitivos no podemos ser; tenemos que admitirlo y nos tenemos que mover al respecto ¿Cómo podemos corregir esto? Dando una formación especializada —que existe tanto en cursos propios como en cursos externos— que vincule a la persona durante un cierto tiempo con cada uno de los organismos; dotra manera, si alguien es bueno siempre vendrá una empresa que multiplique por dos el precio que nosotros podemos pagar.

Ha dicho también que nos centramos en infraestructuras críticas en los organismos del Estado y ha preguntado cómo podemos proteger a los ciudadanos. En eso nuestra capacidad es limitada porque esa misión es de Incibe y no del CCN-CERT. Nosotros publicamos unas buenas prácticas que utilizan la Agencia de Protección de Datos y el Incibe, y nuestra actuación va en ese sentido. Bastante trabajo tenemos con este asunto como para también desplegarnos en otros.

Ha vuelto a preguntar sobre ciberterrorismo y las acciones en la Unión Europea y la ONU. Creo que ya he contestado al referirme al código de conducta en el ciberespacio.

Y en cuanto a las noticias falsas —las *fake news*— y todos los atentados a la democracia, creo que también he respondido hablando de nuestra misión, que es evitar que haya ciberataques en los sistemas que monte el Gobierno de España o en donde nos pidan que les apoyemos. A mí las *fake news* me preocupan mucho, porque considerar cuándo una noticia es falsa o no es falsa es un terreno demasiado pantanoso en el cual yo, como técnico, no quiero entrar.

Y paso a contestar al representante de Unidos Podemos, que quiere saber si tenemos o no suficientes recursos cíber y el nivel de inversión en ciberseguridad en España comparado con otros países. Bien, en España ha habido una legislación que ha acompañado, pero España no es un país de estrategias. En España funcionan el *BOE* y la normativa que se publica en los diarios oficiales, y eso es lo que vincula. La estrategia de ciberseguridad es un documento muy importante que nos marca el norte, pero no es un documento como pasa en el Reino Unido, donde la estrategia de ciberseguridad va acompañada de presupuestos. Aquí normalmente las estrategias no vienen acompañadas de presupuestos; se da la misión a los organismos, y luego los Presupuestos Generales del Estado dan una serie de dinero, con lo cual contabilizar el dinero que se dedica a ciberseguridad en España como lo puede contabilizar el Reino

cve: DSCG-12-CM-105

Unido es muy difícil, porque ellos contabilizan los capítulos 1, 2 o 6 y aquí a lo mejor solo contabilizamos el capítulo 6. Como digo, es un asunto difícil. Lo que puedo decir es que, si nos comparamos con países homólogos, por lo menos tenemos el mismo nivel de madurez. ¿Que nos hace falta dinero? Nos hacen falta bastante dinero y bastantes recursos, pero es cuestión de ir dotando a los organismos en los Presupuestos Generales del Estado y dotar a las plantillas del número suficiente.

En cuanto a si el número de especialistas es suficiente o no, eso lo dejo abierto; siempre hacen falta más —el Grupo Popular también ha preguntado si tenemos suficientes—. Yo creo que nos tenemos que restructurar. La ciberseguridad es un servicio que se puede dar en modo horizontal, y aquí el número no es importante, porque yo puedo tener diez buenos especialistas que hagan mucho más que un equipo de cincuenta que haya reclutado donde haya hecho falta. Por tanto, es mejor tener un buen servicio horizontal bien dotado que un montón de equipitos de respuesta mal dotados y mal instruidos. Y así como en otros sitios hay que matizar mucho el servicio horizontal, dependiendo del organismo y de la Administración, en ciberseguridad es bastante exportable.

Han hablado del modelo mixto, de infraestructuras críticas, de cómo colaboramos con el sector privado, etcétera. Quiero matizar que estamos todavía determinando qué infraestructuras críticas son del sector público y cuáles del sector privado. Pero hay sectores que son eminentemente públicos: salud, agua, transportes —por ejemplo, casi todo el transporte ferroviario está soportado por el sector público—… Hay más sector público del que nos podemos imaginar en las infraestructuras críticas. En el sector privado puro, cuando las empresas hablan de la cooperación público-privada están pensando: ¿qué me vas a dar? ¿Cuánta información me vas a dar y cómo vamos a colaborar?, cuando la información viene de los organismos públicos a las empresas. Tenemos que superar esa barrera y ganar la suficiente confianza para que ellas no tengan reparos en notificar los incidentes y además deseen intercambiarlos porque van a recibir valor añadido. Ese es un asunto que para nosotros debe ser crítico en el futuro.

Con respecto a si se potencian las certificaciones en el modelo de ciberseguridad, creo que hay que potenciarlas tanto en infraestructuras críticas como en GDPR. Y ya que tenemos el modelo del esquema nacional de seguridad, mi recomendación para la Cámara es potenciar una certificación conjunta ENS-GDPR y para lo que toque con el incremental necesario, infraestructuras críticas.

También preguntaban sobre los informes de FireEye y Cryptojacking. Nosotros no tenemos ninguna intención de ser juez ni parte de nada, pero estamos obligados a informar de los problemas de seguridad que van saliendo. Hace dos años estaba de moda el *ransomware*: te infectaban el ordenador y te pedían un rescate. Eso es claramente un delito porque es una extorsión. El *cryptojacking* consiste en que yo infecto tu ordenador y utilizo todo lo que tú no utilizas, el 90 % —normalmente utilizamos el 10 % de la CPU—, en minar criptomonedas. ¿Eso es delito? No lo sé. Lo tiene que decidir la Fiscalía, que tiene el informe, como tiene otro informe de Incibe u otro de la Policía. Yo veo que hay bastante picaresca, pero es cierto que el *cryptojacking* es el ataque por excelencia de este año. Se infecta, y no es un delito; ahora bien, con ese exceso de trabajo de la CPU se puede calentar y quemar un móvil. Ayer hubo bastantes noticias acerca de que los portátiles o móviles se queman; se pueden quemar porque la batería está mal o porque la estemos haciendo trabajar en exceso. Eso está en una escala de grises, y yo no me atrevo a determinar si es delito, falta o qué es, pero, desde luego, no nos piden permiso para utilizarlo, con lo cual, bien del todo no debe de estar.

También me han preguntado por los servicios horizontales, cuestión que ya he comentado, por lo que paso a las preguntas del representante del PSOE. Pregunta también sobre la coordinación con el sector público en infraestructuras críticas. Creo que el CNPIC está haciendo muy buen trabajo y que está teniendo bastante paciencia, porque aproximarse al sector privado con una normativa que obliga y que encima nos vean como un aliado es un asunto complejo.

Y ha hablado de potenciar dos o tres aspectos. Yo vuelvo a insistir en los retos actuales y, sobre todo, en mejorar las capacidades de vigilancia en la Administración General del Estado. Y, por supuesto, en el intercambio. Cuando hablo de intercambio de incidentes y amenazas hablo de un intercambio real basado en la confianza entre el sector público y el sector privado. Y tanto para el sector público como para el sector el privado, ya que tenemos el esquema nacional de seguridad, utilicémoslo, sobre todo por los sellos de certificación. La GDPR habla de unos códigos de conducta y de unos esquemas de certificación. Estamos trabajando con la agencia para que haya un sello conjunto ENS-GDPR, y estamos trabajando con el CNPIC para que determinemos cuál es el incremental que necesita una infraestructura crítica sobre las medidas de seguridad establecidas en el ENS. Vamos a trabajar en eso, de tal manera que tengamos unas auditorías programadas y unos sellos reconocidos aquí y en Europa, porque lo que va a decir la

cve: DSCG-12-CM-105

Unión Europea es que el estándar internacional va a aplicar la 27001, que realmente es de bastante menor calidad... No voy a decir de menor calidad, de menor exigencia que el esquema nacional de seguridad.

Ya he hablado de coordinación, por la que también me han preguntado. En cuanto a los niveles de madurez, he comentado que cuando nos movemos en el contexto internacional los CERT de todos los países escandinavos, los de Holanda, Alemania, Francia, Reino Unido o Suiza son espectacularmente maduros; y del resto de CERT no puedo decir lo mismo. Entonces, tenemos unos grupos informales para que esos CERT intercambien información. Y ahora el reto será que en la red C SIRT establecida en la Directiva NIS también se intercambie información.

Por último, me queda contestar las preguntas de la representante del Partido Popular, que ha hablado de que este es un asunto prioritario para la Unión Europea y también se ha referido a posibles injerencias, asuntos sobre los que ya he contestado.

Les diré que el porcentaje de penetración de internet en España es de más del 80 %. La media de uso del móvil en España es de 5,5 horas; cinco horas y media nos pasamos mirando el móvil, consultando noticias o contestando el malísimo wasap —malísimo o buenísimo. A mis hijos solo les puedo mandar usando el wasap, de otra manera es imposible porque no me hacen caso. Les llamo por teléfono y no me lo cogen; les mando un wasap, y me contestan—. Ese es el reto que tenemos ahora: todo está en internet y tenemos que evolucionar en ese sentido. Y tenemos que ser más seguros como país evitando los ataques que nos vienen por internet y que no tienen tiempo ni espacio.

Ha hablado de la trasposición de la Directiva NIS con el Real Decreto 12/2018, de que el FBI nos pone como ejemplo y se ha vuelto otra vez al debate de la inversión. Como ya he dicho, es difícil para nosotros medir cuánto estamos gastando en ciberseguridad y si todos los gastos que estamos haciendo en ciberseguridad son eficientes, porque si invertimos en capítulo 6 equis millones de euros deberíamos saber cuál es el retorno de inversión del que se están beneficiando los organismos públicos. En el Reino Unido hemos visto que se habla mucho del gasto, pero no de la eficiencia o del retorno de la inversión del gasto.

Y sobre las últimas preguntas de la representante del Partido Popular, en cuanto a cómo considero el nivel de cumplimiento del esquema nacional de seguridad, le diré que el esquema nacional de seguridad tiene un problema con respecto a la Directiva NIS o la GDPR: estas vienen con sanciones, pero el ENS no. Por tanto, es un esquema cuyo cumplimiento por parte de los organismos públicos, aunque sea obligatorio, depende del tiempo y de los recursos. El nivel de cumplimiento está en un 50 %, así que, como dicen ahora los cursis, creo que tenemos un amplio margen de mejora. Pero también les digo que en la página web del Centro Criptológico Nacional están publicadas tanto las empresas del sector privado con sello de certificación como las empresas y organismos públicos que también lo tienen. Hay que impulsar que en ese listado de empresas y organismos públicos con sello de certificación, en el que ahora no habrá más de 20, aparezcan 800 como mínimo. No voy a exigir a un ayuntamiento de 5000 habitantes un sello de certificación —aunque debe tenerlo porque está escrito en el ENS—, pero vamos a ayudarlos, a facilitar que les llegue el servicio horizontal de seguridad a través de las diputaciones. En estos momentos para nosotros es un reto que den el salto para poder certificarse y que un auditor externo les diga que cumplen todo el ENS.

Otra pregunta se refería a si tenemos el talento suficiente para aplicar la Directiva NIS. Bien, los responsables de seguridad de las administraciones públicas —incluyo a todas: autonómicas, locales y general— se han tenido que enfrentar al ENS, a la GDPR y ahora al real decreto. Creo que tienen talento, aunque a lo mejor faltan recursos e impulso político.

En cuanto al sistema de reclutamiento, creo que en las administraciones públicas se detecta el talento porque los procesos selectivos para entrar en las administraciones son duros, por lo que no entra cualquiera. Lo que hay que hacer es seleccionar o por lo menos marcar un itinerario de ciberseguridad, que no tenemos actualmente en las administraciones públicas, y unos puestos específicos. Ahora el ENS establece al responsable de seguridad y la Directiva NIS establece una figura, pero no está definida una figura como un puesto de trabajo con un currículum dentro de la Administración.

Con respecto a si las actuales estructuras organizativas de las administraciones son adecuadas para afrontar los objetivos de la Estrategia de ciberseguridad nacional, incido en lo que he dicho antes: creo que tenemos bastante personal, aunque a lo mejor está ubicado en grupos demasiado aislados, y tenemos que ir a servicios horizontales de ciberseguridad. El trabajo que hizo el anterior Gobierno, intentando racionalizar con el estudio de CORA y con la creación de la Secretaría General de la Administración Digital

cve: DSCG-12-CM-105

creo que es el camino. Hay muchos servicios TIC, y creo que todos los ministerios podrían tener el mismo correo electrónico. Poniendo como ejemplo a Israel, todas las páginas web de todos los ministerios tienen el mismo *look and find,* y cuando un ciudadano va a la página web de los ministerios de Fomento, Agricultura o Sanidad sabe dónde están las cosas porque todas tienen los mismos criterios; y esto se aplica igual en ciberseguridad.

Con respecto a si considero la creación de un canal de integración con la sociedad civil, vamos a aislar la palabra ciberreserva, que suena a reserva militar. La ciberreserva como detección del talento me parece una idea magnífica, y la podemos llamar ciberreserva o lo que estimen ustedes conveniente. Es cierto que llegará un momento —nos pasa ya— en el que el Centro Criptológico no pueda abordar solo cualquier ataque, por lo que tenemos que rodearnos de empresas y de profesionales independientes con talento. Pero cuando ellos trabajen, hay que pagarles; lo que no puede ser es que les digamos que, por amor a España, —que hay que tenerlo— trabajen tres, cuatro o cinco días de su vida para resolver un incidente. Son servicios profesionales y hay que pagarles. Esa es nuestra aproximación. Vamos a tener una ciberreserva con un talento muy bien identificado y cuando nos hagan falta cuatro especialistas de base de datos tiraremos de esa ciberreserva.

En cuanto a la última pregunta, referida al artículo 27 de la Ley de seguridad nacional, se establece para situaciones de crisis una provisión de recursos, que creo que en ciberseguridad no se aplica por lo que he explicado antes, porque tenemos el talento identificado. Normalmente a mí me va a hacer falta movilizar a 10, 15 o 20 personas de empresas o profesionales independientes, y ya los tenemos identificados o estamos en proceso de identificarlos. En caso de crisis por inundación o por incendio hacen falta una serie de recursos humanos que no se aplican a la ciberseguridad.

Y creo que con esto he contestado a todos, señor presidente.

El señor **PRESIDENTE:** Muchas gracias, señor Candau, por el esfuerzo que ha hecho y por la claridad de su exposición.

Vamos a abrir un segundo turno. Ruego a sus señorías que sean lo más breve posible en su intervención.

El señor Yanguas no está, así que le doy la palabra al señor Castellana.

El señor **CASTELLANA GAMISANS:** Gracias, presidente.

Muchas gracias, señor Candau, por las respuestas dadas y por contextualizar la cuestión de la operación Cataluña.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Castellana.

Tiene la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Solo quiero hacer una pequeña puntualización, señor Candau. Le he felicitado por su exposición, que ha sido superdetallada y ha demostrado el trabajo tan importante que realizan y la enorme coordinación que tienen. Con mis preguntas quería aprovechar, no al técnico Candau, que ha descrito magníficamente el trabajo que están realizando, sino a la persona que, conocedora de este mundo, puede aportar algo más. Cuando le he dicho lo de la protección de las personas, no trataba de echarles a ustedes esa carga. Sin embargo, creo que en este momento es un eslabón perdido que no estamos acometiendo como sociedad y que es fundamental; tenemos que empezar a pensar en ello y qué mejor sitio para ello que el Parlamento.

Por tanto, aprovechando su experiencia en este mundo, le he preguntado qué piensa usted respecto a la carencia de profesionales —y no lo he dicho yo, lo ha dicho usted— y también qué cree usted que tenemos que hacer para resolver el déficit que tenemos, teniendo en cuenta, sobre todo, una cuestión: que en el futuro, uno de los grandes problemas que vamos a tener por la automatización —también lo ha mencionado— es la creación de empleo. Y precisamente aquí, en un mundo digital que va a necesitar protección, seguridad, seguimiento, coordinación, etcétera, si lo sabemos racionalizar bien, podemos tener un nicho de empleo importante en una sociedad que lo va a demandar a corto plazo.

Muchas gracias.

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

Tiene la palabra el senador Comorera.

cve: DSCG-12-CM-105

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

Intervengo nuevamente para agradecer sus respuestas a las preguntas que le hemos formulado. Únicamente me gustaría insistir en la pregunta sobre si es necesaria una mayor colaboración entre la Fiscalía de Delitos Informáticos y el Centro Criptológico Nacional o si cree que de la manera en que está ahora ya es suficiente. Me gustaría que me concretara esto.

Muchas gracias de nuevo.

El señor **PRESIDENTE:** Muchas gracias, senador Comorera.

Tiene la palabra el señor Raffo.

El señor **RAFFO CAMARILLO:** Quiero darle las gracias de nuevo y hacer un comentario que no tiene que ver con ninguna pregunta, y es que el Senado, como organismo público, está en línea con lo que hemos estado hablando. Tiene su propia comisión interna y un consejo que preside un miembro de la Mesa, con técnicos relacionados con los distintos departamentos, haciendo un trabajo horizontal, y hay aspectos técnicos que ha mencionado el compareciente que ya se han puesto en marcha también aquí en el sistema de comunicación, a través de un convenio de colaboración con el sector.

Nada más y muchas gracias.

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

Tiene la palabra la senadora Vázquez.

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

Intervengo simplemente para agradecer la valentía que ha tenido el compareciente a la hora de dar respuesta a las preguntas que le he formulado, porque sé que eran complicadas, y, sobre todo, por dejar constancia de ellas en sede parlamentaria. Como he dicho, se agradece este tipo de respuestas, porque nosotros tenemos que elevar un informe, y la ponencia no puede aplaudir lo que ha hecho el Gobierno anterior del Partido Popular, ni lo que hace el Gobierno socialista, sino que tenemos que analizar la realidad de la ciberseguridad en España. Creo que es la mejor manera de ayudar a la sociedad, a los padres, a las empresas y a las administraciones. Por tanto, muchísimas gracias por la valentía de sus respuestas, porque, sin lugar a dudas sé que eran complicadas y usted las ha respondido.

Muchas gracias.

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

Tiene la palabra el señor Candau.

El señor **JEFE DEL DEPARTAMENTO DE CIBERSEGURIDAD DEL CENTRO CRIPTOLÓGICO NACIONAL** (Candau Romero): Estoy totalmente de acuerdo en lo que respecta a la protección de las personas, creo que tenemos que dar a nuestros ciudadanos un ciberespacio seguro y hay que concienciarlos, porque tienen que ser conscientes de que se enfrentan a un territorio en el que se hacen cosas que no se suelen hacer en el mundo físico. Proporcionan datos en una serie de páginas web que cualquiera que se acercara a una puerta no los proporcionaría. Por tanto, tenemos que trabajar mucho esa concienciación.

Por otro lado, en la parte que a nosotros nos compete, tenemos que darles la completa seguridad de que cuando visitan una página web desde un organismo público, dicha página web es segura y no van a recibir ninguna infección.

Estoy totalmente de acuerdo con usted en lo que respecta a la sensibilización. Me atrevería a decir que actualmente la Policía lleva a cabo acciones parciales en las escuelas, pero creo que en el currículum de primaria y de secundaria, igual que hay seguridad vial, debería haber algún componente de ciberseguridad, y todavía no está contemplado. Esto respecto a los ciudadanos.

Respecto a los profesionales, creo que lo he contestado, pero igual no ha quedado claro. Tenemos que hacer una aproximación de la ciberseguridad como un servicio horizontal, pero a varios niveles. No podemos contemplar que un ayuntamiento de 5000 habitantes, que tiene un secretario y un informático, pueda aplicar el ENS a satisfacción. Tenemos que establecer estructuras en diputaciones, en comunidades autónomas o donde se decida, pero eso no está escrito. Las diputaciones ofrecen servicios y los ayuntamientos los cogen o no, y en el caso de ciberseguridad tendríamos que ser especialmente vehementes.

cve: DSCG-12-CM-105

Y lo siguiente que tendríamos que hacer es definir los perfiles de ciberseguridad. Ahora mismo en la Administración pública tenemos perfiles TIC y no tenemos perfiles cíber. Si tenemos huecos de perfiles cíber, seguramente podremos generar la demanda que esperan las universidades.

Al Grupo Podemos, que ha insistido en la colaboración con la Fiscalía, le diré que yo con la fiscal hablo muchísimo y mi jefe más. Otra cosa es que sus unidades de trabajo son las fuerzas y cuerpos de seguridad del Estado, por lo que los grupos de delitos telemáticos y la unidad de información tecnológica de la Policía Nacional son sus instrumentos de trabajo. No obstante, nosotros colaboramos. Es verdad que el centro, en algunos procesos judiciales aporta labores periciales cuando nos las piden, y en algún momento, análisis criptológicos, o cuando hay algún disco duro que no se puede descifrar y el juez ordena que se intente descifrar, lo que no quiere decir que lo descifremos todo; unas veces acertamos y otras veces no podemos.

Creo que he respondido a todas las preguntas, presidente.

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

Creo que así ha sido, por las intervenciones de los distintos ponentes.

Antes de levantar la sesión quisiera volver a la idea inicial. Hay dos constataciones fácticas: la primera, que el tiempo es escaso, y la segunda, que la naturaleza tiene horror al vacío, y el que nosotros no ocupemos lo ocuparán otros, como sabemos por propia experiencia. Constataciones que vienen al caso por el tema de las noticias falsas, de las *fake news*.

Me dice el letrado que probablemente el método más práctico y operativo sería que la ponencia que está analizando la ciberseguridad asumiese también el tema de las noticias falsas dentro de su trabajo, con el compromiso de dedicar un capítulo a este tema. Si eso les parece bien —estamos en democracia directa, ni siquiera en junta de portavoces—, el letrado se encargará de investigar quiénes son las personas que pueden ilustrarnos en estos primeros pasos y les haríamos comparecer. Los senadores y diputados, como es obvio, pueden hacer las sugerencias y presentar a los comparecientes que consideren oportuno. **(El señor Raffo Camarillo pide la palabra).**

El señor **PRESIDENTE:** Tiene usted la palabra, señor Raffo.

El señor **RAFFO CAMARILLO:** Si la Presidencia y el resto de grupos tienen a bien, pedimos aplazarlo para la próxima reunión de la Junta de Portavoces y que esta se celebre pronto, con la idea de intercambiar opiniones y de que podamos hacer una valoración de cómo encajar ese tema, porque es complejo, es delicado y sería bueno consultarlo y analizarlo un poco más profundamente. Como tenemos que discutir también el tema de los plazos de la Ponencia, podemos ver de qué manera contemporizar ambos aspectos.

El señor **PRESIDENTE:** Dada la volatilidad de los tiempos que tenemos, me parece bien la sugerencia. Asimismo sugiero que la Junta de Portavoces se reúna a la mayor brevedad posible para que nuestros trabajos puedan seguir de forma ordenada.

¿Alguna otra observación? **(Denegaciones).**

Agradezco al compareciente y a todos ustedes su presencia.

Se levanta la sesión.

Eran las once horas y cuarenta minutos.

cve: DSCG-12-CM-105