DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 97 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 16

celebrada el jueves 24 de mayo de 2018 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

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

---

cve: DSCG-12-CM-97

Se abre la sesión a las doce y treinta minutos del mediodía.

COMPARECENCIAS. POR ACUERDO DE LA COMISIÓN MIXTA DE SEGURIDAD NACIONAL:

— DEL SEÑOR PÉREZ GARCÍA (CEO UNIDAD CIBERSEGURIDAD TELEFÓNICA, ELEVEN PATHS), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 219/001245 y número de expediente del Senado 715/000513).

El señor **PRESIDENTE:** Buenos días, señorías.

Comenzamos la sesión, escasamente con dos minutos de retraso. Tenemos un cronograma muy apretado si es que queremos disponer de media hora para un almuerzo. Celebro ver que después del debate presupuestario todas sus señorías están o.k., que, como saben, quiere decir cero muertos en inglés. Vamos a ver si en esta sesión también hay supervivientes.

En primer lugar, tenemos la comparecencia de don Pedro Pablo Pérez García, de la unidad de ciberseguridad de Telefónica, para informar sobre diversas cuestiones relativas a la ciberseguridad en España.

Tiene la palabra.

El señor **PÉREZ GARCÍA** (CEO unidad ciberseguridad Telefónica, Eleven Paths): Muchas gracias.

Voy a presentar una serie de *slides,* explicando, sobre todo, cómo vemos la ciberseguridad y cómo esta pasa a ser una oportunidad en la actualidad; básicamente, el escenario actual y cómo visualizamos el mundo desde el punto de vista tecnológico. **(Apoya su intervención con una presentación en Power Point).** A mí me gusta comentar una historia en la que un rey tuvo un determinado problema con su hija. Un sabio consiguió arreglar su problema. El rey le dijo: ¿Cómo quiere que le recompense? El sabio dijo: Quiero un tablero de ajedrez y que vaya poniendo granos de arroz, es decir, 1, 2, 4, etcétera, de manera exponencial en cada una de las casillas. El rey accedió porque no se dio cuenta de lo que significaba realmente, porque un mundo exponencial implica que no hay granos sobre la faz de la tierra para cubrir lo que tendría que poner en la última casilla. Eso es lo que estamos viviendo a día de hoy desde el punto de vista tecnológico. Tenemos crecimientos exponenciales y el mundo tecnológico no es lineal. Como ven en esta curva de usuarios, y cómo de alguna manera el acceso a Internet se está disparando a nivel mundial, más de cuatro mil millones tendrán acceso durante el año 2020. Es decir, no estamos hablando de crecimientos lineales, sino exponenciales.

Estos crecimientos exponenciales han provocado que en el mundo en el que estamos la tecnología sea algo clave. Vemos que la moneda que actualmente tiene mayor crecimiento, el *bitcoin*, no está regulada y no tiene un banco central asociado; que la compañía más grande del mundo, desde el punto de vista de tecnología, que se dedica al *software,* vive de vender publicidad; que la compañía que gestiona más llamadas a nivel intencional no tiene ni una sola línea de comunicaciones; que la compañía de fotografía más grande del mundo es simplemente una *app;* que la compañía de taxis más grande del mundo no tiene un solo coche; que la compañía de hospedaje más grande del mundo no posee ni un solo hotel; que la compañía de ventas más grande del mundo no tiene ningún almacén; que la compañía más grande del mundo de vídeo no dispone de ningún cable; y que la compañía más grande en el sector de los medios no dispone de un solo periodista. Vemos cómo todas estas compañías están liderando sus sectores.

La seguridad en este punto es un disruptor terrible. De hecho, durante el año 2013 todos los ciudadanos vivimos en nuestras carnes un caso por una *fake news.* Enviaron una determinada información en Twitter, robaron el usuario y la contraseña, y mandaron: *breaking two explosions in the White House and Barak Obama is injured*. Mandando este simple tuit a millones de usuarios, el New York Stock Exchange se desplomó por valor de 280 000 millones —estamos hablando del PIB de Portugal—; y todo simplemente porque a alguien le han robado un usuario y una contraseña. Esto está ocurriendo en la actualidad. Hace apenas dos meses nos enteramos de cómo un grupo de ciberterroristas había cifrado todos los documentos del Ayuntamiento de Atlanta y pedían un rescate de 50 000 dólares para poder recuperar toda esta información. Esto que veíamos antiguamente en las películas de Superman o similares, que parecían supervillanos, está ocurriendo en la actualidad y cada día nos levantamos con noticias similares. Por no hablar de lo que ocurrió recientemente con Facebook, cuando una filtración de determinada información provocó una caída en bolsa de la compañía de más de 90 000 millones de dólares. Al final, como Wired expresa, la siguiente guerra fría está aquí y es todo acerca de los datos.

cve: DSCG-12-CM-97

Hay un reporte tremendamente interesante que publica Microsoft sobre el año 2025, cuando se prevé que habrá tres escenarios: el escenario peor, el escenario valle y el escenario óptimo. Aquí el uso de la tecnología puede crear un trillón de productividad en el mundo. El principal factor para que esta productividad pueda ser implementada es la ciberseguridad. Si el mundo al que vamos en el año 2025 no es ciberseguro, el ciudadano no confiará en la Administración, no hará determinadas transacciones *online*, no tendrá determinados procesos de *onboarding* digital. La ciberseguridad es un punto clave dentro de los escenarios que expresa Microsoft en este documento sobre el futuro de la seguridad en el año 2025. Vemos cómo estos escenarios, ya estemos en los escenarios pico, plató o cañón, hacen que la productividad de los países crezca o decrezca en función de la ciberseguridad. Este es un punto que en España está siendo debidamente abordado. En la Agencia de Seguridad Nacional están identificadas las determinadas vulnerabilidades y las amenazas tecnológicas y vemos claramente cómo estos puntos, tanto desde la perspectiva tecnológica como de las infraestructuras críticas, a día de hoy se toman en consideración y están priorizados.

La palabra de moda en seguridad no es simplemente entender la seguridad como la prevención. De alguna manera, en todos los documentos que vienen de Europa en general y de Estados Unidos el sinónimo de la seguridad es la resiliencia. La resiliencia implica que básicamente seremos ciberseguros si prevenimos, detectamos, respondemos y recuperamos adecuadamente. Es decir, la seguridad no es entender que vamos a ser cien por cien seguros y que vamos a prevenir el cien por cien de las ocurrencias, sino que seremos capaces de garantizar que detectamos en tiempo real y que podemos responder de manera adecuada.

El último Foro de Davos y los informes que vienen del World Economic Forum, como pueden ver destacan la ciberseguridad. Todos los riesgos que aparecen en morado son los tecnológicos, los que aparecen en otros colores son los derivados de catástrofes naturales, etcétera. En el cuadrante superior derecho aparece la ciberseguridad como uno de los puntos con mayor probabilidad y con mayor impacto. La ciberseguridad está considerada por todos los Estados como uno de los tres potenciales riesgos a gestionar, no solo desde el punto de vista de Estado, sino de presidentes y de CEO de compañías.

En relación con la seguridad actual, mucha gente piensa que estamos hablando de proteger un castillo para tener muros más altos, más cocodrilos en el foso o más agua. A día de hoy, la ciberseguridad en el mundo digital es totalmente diferente de este concepto, ya que se basa en garantizar que identificamos, protegemos, detectamos, respondemos y recuperamos. Ninguna nación ni ninguna compañía están a salvo de ser *hackeadas;* el Gobierno americano y múltiples empresas que a día de hoy gastan cientos de miles de millones han sido vulneradas. La garantía de la ciberseguridad se obtiene por identificar, proteger, detectar, responder y recuperar. Hay varios informes de Gartner y de múltiples consultoras que hablan de que el 90 % del gasto en ciberseguridad estaba solo en la protección, pero que a partir de 2020 la protección será apenas el 30 % y el 70 % del gasto será detección y respuesta, dado que es imposible cubrir el cien por cien de los escenarios.

La Estrategia de Seguridad Nacional, evidentemente, entiende a día de hoy la dimensión tecnológica, y tenemos un punto clave por el cual el ciberespacio es tremendamente complejo, dado que la seguridad en un entorno en el que no hay fronteras y la atribución es tremendamente compleja garantiza que estos puntos sean tomados en consideración de manera muy especial. La Estrategia de Ciberseguridad Nacional, como todos saben, entiende las ciberamenazas, entre las cuales están los ataques de negación de servicio, los ataques de *ransomware* y similares, que están debidamente identificadas.

Para Telefónica, la ciberseguridad no solo es la protección de la operadora, sino que es un punto de crecimiento para la misma. Es una unidad que se creó hace ya bastante tiempo e inició su periplo con una facturación de 5 millones de euros, terminando el año pasado con un importe superior a los 500 millones de dólares a nivel mundial. Es una de las áreas de más crecimiento en la operadora Telefónica en la actualidad. Adicionalmente se han inaugurado centros de seguridad, no solo en Madrid, sino en Londres, en Centroamérica, en México, en Argentina, en Brasil, en Colombia, en Perú y en Chile. Telefónica dispone actualmente de más de mil quinientos profesionales en ciberseguridad para proteger tanto sus infraestructuras como las de sus clientes; además, mantiene alianzas con otras telecos líderes en el sector, como son Etisalat, Turtelecom, Sintel y SoftBank, a nivel mundial, principalmente en Asia, para proteger donde no tenemos cabida como red y no somos operador incumbente.

Desde el punto de vista de oportunidad, la clave es que vemos que la ciberseguridad, al mismo tiempo que se presenta como uno de los principales riesgos en la actualidad, es un área de alto crecimiento, es un sector que a día de hoy ha superado los 100 000 millones en gasto e inversión a nivel mundial. Es un

cve: DSCG-12-CM-97

sector que permite la exportación, en el cual, mediante los *managed security services*, servicios de seguridad gestionados, que superan con creces los 20 000 millones a nivel mundial, permite que empresas como Telefónica puedan prestar servicios de ciberseguridad desde España a empresas que están en Japón o en Estados Unidos, siendo uno de los puntos más importantes en la operadora para la creación de empleo.

Cuando vemos el crecimiento, observamos que no solo se trata de la inversión o el gasto en seguridad que hacen las empresas, sino los fondos de inversión, que el año pasado invirtieron más de 20 000 millones en la creación de *startups* a nivel mundial. Estas *startups* están principalmente localizadas en Estados Unidos, con principal presencia en Silicon Valley y en Texas, y en Tel Aviv, en Israel, mientras que en España, como Telefónica hemos invertido en los últimos años en cerca de 700 *startups,* de las cuales aproximadamente unas 20 son de ciberseguridad. Una de las naciones que a nivel mundial está tomando esto como una oportunidad y gestionándolo desde un punto de vista más proactivo, es Israel, que teniendo apenas una cuarta parte del PIB de España invierte del orden de diez veces más, manteniendo un liderazgo para conseguir que la ciberseguridad sea uno de los motores de crecimiento del país en la actualidad.

Cuando se hacen las valoraciones, se ve que los múltiplos de las empresas en ciberseguridad son de los más altos del sector. Actualmente, en ciberseguridad las empresas están valoradas normalmente entre cuatro y cinco veces su facturación; es decir, empresas que ni siquiera tienen beneficios, con facturaciones de 100 o 150 millones, llegan a valoraciones por encima de los 600 o 700 millones, dado que es un área de alto crecimiento. Esta es una gran oportunidad para determinadas naciones que están apostando por la ciberseguridad. Está cifrado que en el año 2015 hacían falta más de 1,5 millones de profesionales en el mercado, según Symantec, y en el año 2016 el crecimiento fue, según Isaca, de hasta 2 millones de ciberprofesionales a nivel mundial. Este dato crece hasta los 3,5 millones en el año 2021, según determinadas estimaciones. En Estados Unidos, el salario medio de un profesional de la ciberseguridad ronda los 110 000 euros, y cuando estas personas son mánager, como pueden ver, los salarios llegan a los 200 000 o 225 000 dólares a nivel mundial. Es decir, estamos hablando de un sector de alto crecimiento, en el que los ciberprofesionales están tremendamente bien pagados, y en el que adicionalmente hay una capacidad exportadora tremenda, dado que los servicios de ciberseguridad pueden viajar y desde España, Argentina, Brasil, etcétera se pueden prestar determinados servicios en múltiples países.

Cuando vemos la comparación de los centros de ciberseguridad a nivel mundial, observamos cómo Tel Aviv, en Israel, o Silicon Valley, en Estados Unidos, son los puntos principales que atraen la inversión extranjera y la local. Mientras tanto, determinadas zonas como China, Corea o Singapur están realizando durante los últimos años fuertes inversiones. La inversión de Israel en ciberseguridad, atendiendo a determinadas estadísticas, se cifra en más de mil millones. Si hacemos una comparación, en España tocaría invertir más de 4000 si quisiéramos hacer algo similar a lo que están gestionando ahora mismo en ciberseguridad en Israel.

Quedo a la espera de sus preguntas.

El señor **PRESIDENTE:** Muchas gracias.

Quiero hacerle dos precisiones. Cuando habla de trillones, ¿habla de *billions* americanos?

El señor **PÉREZ GARCÍA** (CEO unidad ciberseguridad Telefónica, Eleven Paths): *Billions* americanos. Correcto.

El señor **PRESIDENTE:** La inversión a la que se ha referido, ¿es en términos de flujo o de *stock?* ¿Es inversión anual?

El señor **PÉREZ GARCÍA** (CEO unidad ciberseguridad Telefónica, Eleven Paths): Es inversión anual.

El señor **PRESIDENTE:** Gracias.

Vamos a dar ahora la palabra a los portavoces. Les ruego otra vez que se atengan a los cinco minutos.

Tiene la palabra el señor Llanguas. **(Pausa).** No va a intervenir. Gracias.

Tiene la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Gracias, señor presidente.

En primer lugar, quiero dar la bienvenida al representante de Telefónica. Comparto los datos que nos ha dado en relación con el crecimiento de negocio que tiene la ciberseguridad y sobre la necesidad de los

cve: DSCG-12-CM-97

Estados y los propios modelos productivos de protegerse para poder garantizar incluso —como usted mismo ha dicho— su propia productividad.

Esperaba de su comparecencia que hubiera entrado un poco más en detalle sobre la solución que Telefónica está adoptando en este sentido. Se ha publicado recientemente la creación de este consejo asesor, formado por personas ilustres, incluso algún excongresista estadounidense experto en ciberseguridad, y máximos responsables de la Unión Europea en temas de seguridad. Para nosotros, Telefónica es un gigante del sector a nivel mundial, por tanto, nos interesa mucho ese organismo que están creando, pero también queremos saber cuál es el sistema que están utilizando. Ha dado datos cuantitativos del número de empleados, de la inversión, pero nos gustaría conocer con más detalle cómo están enfocando el tema de la ciberseguridad.

Ha mencionado una palabra clave, que es la palabra clientes, y luego ha hablado del tema de la confianza, de la necesidad de que la sociedad tenga confianza, de que los clientes tengan confianza y que en este mundo se pueda competir digitalmente sabiendo que solo estás hablando del modelo de negocio y del objetivo, pero no de que tienes unos riesgos y de qué empresa los soporta.

Independientemente de pedirle que profundice un poquito más en la explicación del caso concreto de Telefónica, que despierta nuestro interés, como estamos hablando de proveedores como ustedes y al mismo tiempo de clientes, que también pueden ser empresas, y de ciudadanos que utilizan y consumen servicios de esas propias empresas, quisiera preguntarle cómo cree que se va a valorar la confianza, si va a ser general en el conjunto de la red, lo que me produce confianza o desconfianza, hago transacciones o no las hago, o vamos a llegar a un punto en el que los ciudadanos van a confiar más en unas empresas que en otras, es decir, que unas están más protegidas que otras. Me gustaría que descendiera a la letra pequeña. ¿Hablamos de confianza en genérico? Si vamos al sector de la banca, vemos que lleva mucho tiempo invirtiendo para intentar garantizar que esos servicios sean seguros, pero también estamos hablando de que Telefónica tiene empresas que son clientes y que ustedes van a trabajar para apoyarles en su ciberseguridad. Si otras empresas que compiten con ellos no tienen los mismos modelos de ciberseguridad, van a ser más vulnerables, y sin son más vulnerables generarán menos confianza. Por tanto, esa reputación puede tener un valor en las propias empresas y en los propios usuarios.

Me gustaría aprovechar su experiencia, para hacerle una serie de preguntas, porque he visto que lleva bastante tiempo en el apostolado de esta cuestión; no se ha incorporado ahora, en la ola de la moda de la ciberseguridad, sino que es un experto y un profesional que lleva bastante tiempo en esto y que ha ido viendo el desarrollo de todo el sistema de ciberseguridad que se ha ido produciendo en España. Quiero preguntarle si considera que estamos desarrollando adecuadamente la estrategia; si considera que esa estrategia de país que se está desarrollando está suficientemente coordinada con todos los actores que tienen intereses en la ciberseguridad, públicos, privados, ciudadanos; si considera que en un mundo globalizado gran parte de nuestra información está en medios sociales y en medios de comunicación que utiliza el conjunto de la ciudadanía, estilo redes sociales, etcétera; si cree también que la política que se está llevando a cabo es la adecuada y si debieran ser precisamente esas empresas, como Facebook, Twitter o Instagram las que, por su reputación, tendrían que garantizar la seguridad de los datos de sus clientes, el uso no fraudulento de sus datos, en vez de tratar de instar, como se suele decir, a que sean los propios usuarios los que configuren bien sus sistemas de seguridad para no tener esa pérdida. Es verdad que con el tema de la protección de datos los operadores están actualizándose, pero quiero saber si entiende que los Estados debieran exigir a esos grandes proveedores de comunicación más responsabilidad con respecto a ese tipo de información, porque si de repente desaparece la información de muchos usuarios no tenemos noticias de que suceda nada, de que se pida alguna responsabilidad o de que se compense a la persona a la que le han desaparecido sus datos.

Espero que profundice un poco más en el modelo Telefónica y que nos hable de este entramado de empresas, operadores y ciudadanos.

Muchas gracias.

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

Tiene la palabra el senador Comorera.

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

Señor Pérez, gracias por su comparecencia y por las explicaciones que nos ha dado en esta primera intervención. Directamente le voy a formular unas cuantas preguntas. En primer lugar, me gustaría que nos dijera qué supone para Telefónica la alianza con las grandes operadoras de comunicaciones, Etisalat,

cve: DSCG-12-CM-97

Sintel, SoftBank, en su lucha contra las amenazas de la red. En segundo lugar, ante el aumento de riesgos en seguridad cibernética, en la medida en la que la seguridad de la información será cada vez más compleja, ¿cuáles son las expectativas de esta alianza en la protección de los intereses de las empresas? En tercer lugar, desde su punto de vista, ¿qué supone el desarrollo de nuevas tecnologías tales como el análisis predictivo mediante *machine learning* y la seguridad cibernética avanzada para el Internet de la cosas? Al hilo de ello, ¿de qué manera considera que se debe abordar la creciente expansión del llamado Internet de las cosas?

Hemos tenido conocimiento de que Telefónica ubicará en Valencia su centro de I+D en ciberseguridad, orientado precisamente al Internet de las cosas y *smart city*. Siendo este el único centro de este tipo que se pondrá en marcha en España, me gustaría saber qué nos puede contar al respecto.

Siendo usted de Telefónica, quisiéramos que nos comentara algo sobre el aumento del *malware* en los dispositivos móviles, porque según las últimas noticias ha crecido bastante. Nos gustaría que nos dijera qué datos manejan ustedes.

En cuanto a la inversión, le haré una pregunta que acostumbramos a hacer a la mayoría de los comparecientes. Nos ha dejado claras en el cuadro las diferencias que tenemos con países como Estados Unidos o Israel. ¿Cree que la inversión que se está haciendo en ciberseguridad en España es suficiente o tendríamos que mejorarla?

Finalmente, se desprende de los datos del Ministerio del Interior que ha habido más ciberataques o ciberincidentes en los últimos meses; de hecho, en los dos primeros meses de este año se produjeron 125 ciberincidentes en infraestructuras críticas, 53 en enero y 72 en febrero. ¿Realmente hay más ciberataques o es que se están reportando más que antes? ¿Cree usted que las empresas han perdido el miedo o las reticencias por la llamada pérdida reputacional que supone el reporte de este tipo de ciberataques?

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.

Tiene ahora la palabra, el señor Luena.

El señor **LUENA LÓPEZ:** Gracias, señor presidente.

Señor Pérez García, gracias por sus palabras y enhorabuena por la creación del Consejo Mundial de Seguridad. Después de haberle escuchado, nuestra tarea es un poco ímproba o difícil, porque es que haya granos de arroz, como usted decía al principio. Por eso le digo que la tarea de esta Comisión es aprovechar la enorme experiencia privada que tienen ustedes para que nosotros, como representantes del pueblo, podamos hacer un buen trabajo y que dicha experiencia privada pueda redundar en el servicio público y en las políticas públicas de ciberseguridad, que son claramente deficientes. Ese es el motivo de que tengamos tanto interés en escucharle.

Hay cuestiones de actualidad. Por ejemplo, esta semana ha estado en Bruselas el presidente de Facebook. No sé qué nos podrá contar usted sobre la garantía de la privacidad de los datos, si eso existe. Hoy el diario *El País,* publica una noticia sobre el negocio de la manipulación digital en España. Se viene hablando con muchísima insistencia sobre la injerencia de países como Rusia —no pasa nada por decir las cosas— en procesos electorales, como, por ejemplo, aquí en España, en Cataluña. Como usted ha dicho que hay que dedicar el 70 % de los recursos a la detección y respuesta, mi pregunta es de qué forma podemos anticiparnos, en esa dinámica de la que habla de detección y respuesta, a los ataques, a la prevención más que a la protección, y si se pueden anticipar estos comportamientos en la red.

En segundo lugar —por ir rápido, como nos pide el presidente—, no sé si en su opinión es suficiente con la legislación, con los sistemas de protección, con la directiva que todavía está en trasposición, con la Ley Orgánica de Protección de Datos, con la Ley de Seguridad Privada, y con el Reglamento europeo, que precisamente entra en vigor mañana.

En tercer lugar, ¿conciencia de riesgo o cultura de ciberseguridad? Nuestro portavoz decía en la anterior sesión de la Comisión que existe más sensación de seguridad en el ciberespacio de la que realmente hay. ¿Cómo evalúa usted el grado de concienciación de los usuarios respecto a la ciberseguridad y al uso seguro de los diversos dispositivos y herramientas que utilizamos? Le hago la misma pregunta para el mundo empresarial, ¿hasta qué punto la seguridad de los sistemas, redes, herramientas, es valorada por los solicitantes de los servicios? Para terminar, ¿qué papel puede jugar el sector privado a la hora de extender la concienciación sobre esa cultura de ciberseguridad? También quiero preguntarle, para que sirva de ayuda a los trabajos de esta Comisión, qué podemos hacer, como sociedad, para tener una conciencia sobre la importancia de nuestra independencia tecnológica en materia de ciberseguridad.

cve: DSCG-12-CM-97

En cuarto lugar, en cuanto a la colaboración público-privada, sobre la eficacia de la integración de nuestros sistemas, capacidades públicas y privadas, ¿cómo ve usted los niveles de cooperación? ¿Echa usted en falta estructuras de coordinación público-privadas? Si no es así, ¿es necesario reforzarlas?

En quinto lugar, referencia internacional. El señor Picatoste, representante de Deloitte, en la última sesión de la Comisión nos habló de Estados Unidos y de Israel. Si no he entendido mal, creo que usted ha dicho lo mismo y ya nos ha situado, por lo que no le pido que nos haga un escalafón. Lo que sí quiero es que nos detalle cuáles son, a su juicio, las principales fortalezas y vulnerabilidades del sistema, hasta donde se pueda, porque esta Comisión es en abierto y seguramente ahora mismo por el canal del Parlamento nos estarán viendo. En cualquier caso, dada su experiencia, que fundamentalmente es global —se ha preguntado ya, pero se lo tengo que decir, porque, como he dicho, nuestra misión es aprovechar su experiencia privada para hacer propuestas públicas—, quisiera saber qué le parece el presupuesto que se dedica en España, sobre todo si lo comparamos con los de otros Estados y con el del sector privado, nacional y global o internacional. Asimismo, me gustaría conocer el nivel de inversión en I+D+i en ciberseguridad realizada por el sector privado con relación a la que se hace también en I+D+i en otros ámbitos.

Termino, señor presidente. Usted ha llamado a la formación y al empleo la oportunidad. Estamos absolutamente de acuerdo. La oportunidad, que finalmente será la necesidad; pero usted ha dicho la oportunidad. Hoy terminan unas jornadas de ciberdefensa que ha organizado el Mando Conjunto de Ciberdefensa. Se ha hecho hincapié en la necesidad de la detección y promoción del talento. ¿Cuál es su opinión? ¿Qué hoja de ruta —como se dice a menudo— debiéramos tener? Se ha hablado también del itinerario formativo para hacer esas reformas y de los voluntarios de la ciberreserva. ¿Qué opinión le merece a usted, como representante del sector empresarial?

Por terminar, una pregunta con relación a la eficacia de los sistemas de cooperación. ¿Cree usted que hay la suficiente colaboración, asociación público-privada, o lo único que tenemos es una mera relación cliente-proveedor? En caso de que exista, ¿cómo funciona?

En todo caso, señor Pérez García, gracias por haber venido, por su información y las respuestas que nos pueda dar. Enhorabuena por la creación de este consejo mundial. Y le puedo asegurar que, al menos por parte de las Cortes Generales y esta Comisión, trataremos de que, si no llega a haber del todo arroz, sí la mayor cantidad posible.

Gracias.

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

Termina este turno el señor Cosidó.

El señor **COSIDÓ GUTIÉRREZ:** Muchas gracias, señor presidente.

Una de las desventajas que tiene ser el grupo mayoritario —las ventajas son muchas— es que buena parte de las preguntas las han formulado ya el resto de los portavoces. Intentaré repetir lo menos posible, aunque algo va a ser inevitable.

Nos ha hablado usted de la estrategia y ha señalado la resiliencia como concepto fundamental. Ya tenemos esta palabra en el Diccionario de la Real Academia, que hasta hace muy poco no existía. Usted la ha definido sobre la base de cinco aspectos: identificar, proteger, detectar, responder y recuperar. ¿Es posible anticipar? Da la sensación de que todas nuestras estrategias de ciberseguridad son esencialmente reactivas, y no sé si tecnológicamente es posible tener capacidad de anticipación sobre los ataques y saber por dónde nos van a llegar en el futuro las amenazas, para ser capaces de neutralizarlas, incluso antes de que puedan desarrollarse.

Querría felicitarle no solo por su intervención, que ha sido claramente la de un ingeniero pero muy concisa, sino también por la labor que están realizando. Tener una empresa como Telefónica entre las grandes compañías de telecomunicaciones del mundo creo que nos debe hacer sentir a todos orgullo. Pero que además esta gran empresa se encuentre en estos momentos en una fase tan expansiva en el ámbito de la ciberseguridad nos hace albergar buenas perspectivas sobre las posibilidades de crecimiento que tiene el sector en nuestro país. Debería haber empezado por ahí, pero vaya la felicitación antes que las preguntas.

Quería preguntarle por la evaluación desde el punto de vista de esta gran empresa del sector privado en la ciberseguridad en tres ámbitos. ¿Cómo evalúan ustedes la ciberseguridad en el ámbito de las administraciones públicas, cómo estamos? Sé que esta cuestión corresponde al Centro Criptológico Nacional, pero me gustaría tener la perspectiva desde el punto de vista del sector privado. ¿Cómo evalúa

cve: DSCG-12-CM-97

la ciberseguridad en nuestro sector empresarial, en nuestras empresas? Y de manera muy particular, porque creo que es una de las áreas principales de negocio que en estos momentos desarrolla Telefónica —comparecerá después el director del Centro de Protección de las Infraestructuras Críticas—, desde su punto de vista, ¿España tiene razonablemente garantizada la ciberseguridad en sus infraestructuras críticas? Si puede hacer una valoración, se lo agradecemos.

También me gustaría preguntarle qué es lo que más le demandan sus clientes —el concepto de ciberseguridad es muy amplio— y por dónde va la demanda de futuro, qué es lo que más preocupa a las empresas, y a raíz de ello, cómo estima usted el sector. Indudablemente, la evaluación de la propia empresa es buena, como hemos visto en la presentación, pero quisiera saber qué valoración hace de las capacidades del sector para dar respuesta a esa creciente demanda de ciberseguridad que vemos que tenemos en España.

Sobre el marco regulador ya le han preguntado y, por tanto, no voy a insistir en ello, aunque tenemos interés en escucharle. Quizás tenga usted alguna demanda o propuesta en este ámbito.

También le han preguntado ya por la cooperación público-privada, pero quisiera conocer dos cuestiones: en primer lugar, cuáles son los procedimientos de comunicación y de cooperación que tienen con los distintos organismos que hay en España responsables de ciberseguridad en el ámbito público, y, en segundo lugar, si las empresas denuncian o no. En referencia a cuando se produce un ataque, un incidente o actividad delictiva, la experiencia es que las empresas eran bastantes renuentes a denunciar, porque eso ponía también de manifiesto sus vulnerabilidades. Creo que está cambiando la cultura, pero me gustaría que usted me dijera si la tendencia es que las empresas son cada vez más transparentes y denuncian más este tipo de casos.

Usted ha dicho que para parecernos a Israel deberíamos invertir cuatro veces más que aquel país porque tenemos una economía cuatro veces más grande. Aparte de invertir, ¿hay algo más que podamos hacer para ser un poco el Israel de Europa, para convertirnos en un país realmente puntero en nuestro entorno en el ámbito de ciberseguridad, en cuanto al número de *startups*, inversión y facturación? ¿Cuáles serían las claves que a usted le parece que hacen que Israel tenga esos mil millones de dólares de inversión al año y que nuestra inversión sea menor? ¿Cuál es la inversión privada y cuál es la inversión pública, con referencia a las cifras globales o mundiales, incluso de Israel o Estados Unidos?

Y casi una curiosidad personal, aunque creo que escapa del ámbito de su competencia. Siempre hemos hablado de la necesidad de concienciar y de educar en el ámbito de la ciberseguridad. Hubo una iniciativa de Telefónica —para mí, muy exitosa—, junto con la Dirección General de la Policía y la Fundación Cibervoluntarios, para dar en las escuelas el carné de ciberexpertos. Quisiera saber si Telefónica sigue apostando por ese proyecto y si siguen creyendo que la mejor medida preventiva en el ámbito de la ciberseguridad es la educación y, de manera particular, la educación de nuestros niños y jóvenes en las escuelas.

Gracias.

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

Tiene la palabra el señor Pérez García. Me permito sugerirle que agrupe las respuestas por grandes temas, porque ha habido preguntas que se han repetido.

El señor **PÉREZ GARCÍA** (CEO unidad ciberseguridad Telefónica, Eleven Paths): Intentaré responder a todas.

La primera pregunta es relativa a cómo funciona Telefónica en la parte interna y, sobre todo, en referencia al reciente anuncio que hicimos. Ayer sacamos una nota de prensa según la cual hemos creado un consejo asesor, en el que está don Javier Solana, también Mike Rogers, asesor del Gobierno americano, y otras personalidades. Tenemos un equipo que asesora al presidente y asesora en ciberseguridad, dado que entendemos que es una cuestión clave. En principio, se reúne dos veces al año y sirve para tener un punto de entrada de información adicional a los que existen en la actualidad, dado que la seguridad es tremendamente importante. De hecho, ayer también inaugurábamos el centro de ciberseguridad en Galicia, en la Ciudad de la Cultura, creado conjuntamente por Telefónica y Gradiant, en el que inicialmente se dará empleo a unas veintiocho personas dedicadas a I+D+i en esta materia. Es decir, toda esta información se refiere a la apuesta de Telefónica, porque entiende que la ciberseguridad es clave, y por eso se crean consejos asesores, se invierte en determinados territorios y se llevan a cabo casos y ciberejercicios. Este año participaremos en no menos de tres a nivel europeo, estatal y con determinadas entidades privadas.

cve: DSCG-12-CM-97

Explicaba anteriormente que la seguridad externa de los clientes es un ámbito en crecimiento. Pero, evidentemente, la seguridad de la operadora Telefónica en cuanto a protección de una infraestructura crítica está alineada para tener el *compliance* necesario con toda la normativa actual.

Sobre la confianza digital, las ratios y cómo se aplica a la seguridad, hay que entenderla como resiliencia, es decir, con estos componentes de identificación, prevención, detección, respuesta y recuperación, de manera que la confianza digital va aumentando cuanto más resilientes somos de cara a los ciudadanos.

Desde el punto de vista del desarrollo de las estrategias, si son adecuadas y cuál es la colaboración público-privada, antes de responder primero hace falta saber qué queremos ser de mayores, es decir, Israel decidió que quería liderar el mundo de la ciberseguridad a nivel mundial y por eso tiene ese apetito por la inversión en ciberseguridad. Otros países libremente han decidido no liderar este segmento, sino el del turismo, etcétera. Por tanto, que no se entienda, por favor, que estoy reclamando una inversión, sino que, básicamente, hay que decidir qué queremos. Pero, como ingeniero —como antes comentaban—, diré que si queremos liderar algo no nos podemos hacer trampas al solitario, es decir, los líderes están invirtiendo una cantidad de dinero y, si queremos liderar algo, evidentemente hay que tener cantidades de inversiones similares.

Desde el punto de vista de cómo se está compensando y al hilo de lo que ha ocurrido con Facebook, evidentemente a día de hoy las empresas privadas están invirtiendo en ciberseguridad. De hecho, el propio presidente y consejero de Facebook explicaba que iba a acometer inversiones de importante magnitud para asegurar que no volviera a ocurrir en su empresa. En mi opinión, es el camino, es decir, determinadas compañías, como Facebook, han sido valientes a la hora de reconocer determinados fallos y problemas. Ese es el primer punto para mejorar, reconocer un determinado fallo y acometer las inversiones. Otras compañías fueron *hackeadas* o vulneradas hace dos, tres, cuatro años y nos informan de los problemas a posteriori. Creo que lo valiente es lo que ha hecho Facebook con el problema que ha tenido, incluso con pérdidas en bolsa, etcétera. Podemos entrar en otro tipo de valoraciones sobre el uso legítimo o no de los datos, pero hoy estamos hablando de ciberseguridad, y, desde este punto de vista, lo que ha hecho Facebook ha sido tremendamente valiente, asumiendo el problema y poniendo la inversión o el gasto adecuado para erradicar el problema en el futuro.

Acerca de la alianza de las operadoras, las amenazas son globales. Como han podido observar, los logros de las empresas con las que mantenemos las principales alianzas están en Asia, y las amenazas llegan de todo el mundo, de América, Europa, África y Asia. Eso nos ha permitido tener visibilidad y poder llegar a lugares donde antiguamente estábamos más ciegos. Evidentemente, los intereses empresariales son tremendamente importantes. Hablamos de un sector que crece a doble dígito a nivel mundial y que a día de hoy —insisto— tiene un *gap* de más de dos millones de profesionales, es decir, estamos hablando de una de las áreas de mayor crecimiento a nivel mundial.

Desde el punto de vista del análisis predictivo, del *machine learning* y el IoT, entiendo que la mayoría sabe distinguir lo que es la inteligencia artificial y cómo se aplica a determinados mecanismos, y, al final, las herramientas tecnológicas permiten el progreso, de modo que básicamente es el uso que hagamos o cómo lo devolvamos a la sociedad lo que hará que sean buenas o malas herramientas. Hoy día el *machine learning* está siendo ampliamente utilizado en ciberseguridad para poder detectar y prevenir determinados casos, como antes se comentaba. Pongo un ejemplo muy simple, que además hace referencia a múltiples casos que constantemente aparecen en prensa. Uno de los más conocidos es el ataque referido a denegación de servicio. Se da la orden a un ejército de bots de conectarse a una determinada web, todos al mismo tiempo, provocando un desbordamiento. Lo que ocurre es que, evidentemente, la tubería recibe más agua de la que puede llevar, y, al haber tanto tráfico, la percepción del usuario es que realmente esa página o ese servicio deja de funcionar, porque está saturado y no es capaz de cursarlo. Pero hoy día este tipo de ataques son tremendamente fáciles de parar en determinada escala gracias a algoritmos de aprendizaje automáticos. Si una determinada empresa, banco equis, recibe habitualmente el 99 % de su tráfico desde España, pero resulta que el 10, 20, 30, 40 % del tráfico empieza a llegar de China, Estados Unidos, etcétera, hay una anomalía, y esa detección de anomalía se puede ver en red y de manera automática provocar un bloqueo. Por tanto, este tipo de tecnologías ya están implantadas. No obstante, como la legislación europea sobre protección de las infraestructuras y, especialmente, protección de información se gestiona de manera particular, es verdad que determinados Estados, singularmente Singapur, China, etcétera, están creando los *cyberdrone*, escudos de protección digital a nivel estatal para protegerse de determinados ataques.

cve: DSCG-12-CM-97

Internet of things es uno de los puntos que están explosionando a nivel mundial. Actualmente existen más dispositivos conectados a Internet que personas en el mundo, más de 6000 millones de dispositivos, y la cifra no para de crecer; como comentaba al inicio, estamos hablando de un aumento exponencial. No debemos pensar que es lineal sino exponencial, de modo que probablemente en 2030 estemos en 6500 millones de ciudadanos y 30 000 millones de dispositivos. No nos resulta ajeno que cada uno tiene en su casa una consola, un rúter, el móvil de la mujer, los de los hijos, los de gente que viene, es decir, el número de dispositivos en el hogar está creciendo de manera exponencial; no hay menos de cinco dispositivos por casa, al igual que la media de cuentas de una persona en Internet llega a ser hasta de veinte ciberidentidades. Pero el principal problema en el *Internet of things* es que consideramos la seguridad desde un punto de vista tradicional, y, sin embargo, hay elementos accionables que pueden provocar la pérdida de vidas humanas, ya sea, por ejemplo, en relación con la seguridad de un coche, en un determinado puerto o en un determinado entorno industrial, lugares que han de estar debidamente protegidos. Exactamente igual, en el *Internet of things* se aplican los mismos parámetros de resiliencia, como respecto a determinadas compañías que pueden ser *hackeadas* y sufrir ciertos problemas, y una detección temprana y respuesta adecuada hacen que se mitigue el riesgo. Nosotros solemos comentar el caso de Tesla, que además es uno de nuestros mejores clientes a nivel mundial, porque uno de sus vehículos eléctricos tiene una SIM de Telefónica en toda su composición a nivel mundial, de modo que todos esos coches están conectados. Hace ya algún tiempo tuvieron un determinado problema de seguridad acerca de su vulnerabilidad, lo vimos, se consideró, se apretó un botón y en menos de veinticuatro horas se actualizaron todos los coches, a nivel mundial. Esto ocurrió también en otra compañía, pero a día de hoy tiene más del 70 % de la planta sin parchear. Es decir, hay que entender que los coches tienen que ser seguros y que el *Internet of things* —entendiendo por ello coches o cualquier otro elemento— requiere de esa ciberseguridad, especialmente cuando hablamos del que va ligado a los dispositivos personales, como son, por ejemplo, las cámaras para vigilar bebés en los hogares o que constantemente estamos emitiendo datos en Internet sobre nuestra salud, como cuántos pasos damos, etcétera.

Hablando de los centros, se publicó la noticia de que en un futuro inauguraremos el centro de Valencia, y lo que estamos haciendo va en dos direcciones. La ciberseguridad está creciendo notablemente y por eso ayer inauguramos el centro en Galicia, como también se abrirán otros en el futuro o el año pasado inauguramos uno en Buenos Aires. Por otra parte, la búsqueda de ciberprofesionales es tremendamente compleja, por lo que se hace en todo el territorio nacional y también a nivel mundial, porque así se crean centros de expertos que lideran su área en materia de seguridad.

Con respecto a la pregunta sobre el *malware* en los dispositivos móviles, es verdad que está aumentando tanto su adopción como los problemas de seguridad, que hoy día se refieren especialmente a Android y iOS, el sistema operativo que tiene Apple. A nivel mundial, los datos sobre este tipo de infecciones indican que en los dispositivos Android superan el 3 % y que en los dispositivos de iOS están por debajo del 0,1 %. Estos son los datos a nivel mundial, en general, pero no podemos dar las cifras exactas de Telefónica.

En cuanto a la parte de la inversión y si es suficiente, creo que lo más importante es saber para qué, como comentaba antes. Si lo que básicamente queremos es proteger el país y clasificarnos para estar en el número 20, 30 o 10 a nivel mundial, evidentemente la inversión es suficiente. Si queremos pasar a liderar en ciberseguridad, como están haciendo algunos países, evidentemente la inversión es a todas luces insuficiente.

Con respecto a los ciberataques, creo que la pregunta estaba muy bien hecha, porque así ocurre en la actualidad. En primer lugar, estamos invirtiendo más en detección, de modo que vemos más cosas que antes. Y, evidentemente, hay un punto clave, que es el tiempo de detección, que antiguamente estaba casi en 180 días de media a nivel mundial, y, sin embargo, hoy ya está bajando a los 90 días en muchos países. Por tanto, esa inversión en detección también hace que veamos más ataques, de esos que antes también ocurrían. Pero, al mismo tiempo, hay que considerar su proliferación, es decir, están creciendo, al tiempo que tenemos más visibilidad. Por eso sabemos que los crecimientos son de tal magnitud.

Sobre la comparecencia en Bruselas, Facebook y este tipo de ataques electorales, soy un experto en ciberseguridad, y, evidentemente, no voy a hacer valoraciones sobre si un Estado ataca a otro, etcétera, porque no es mi función. Desde el punto de vista tecnológico, evidentemente, las *fake news* están causando una serie de problemas a nivel mundial y por ello hay una inversión importante en su detección.

cve: DSCG-12-CM-97

El propio Facebook ha anunciado que está pensando en crear cerca de 2000 empleos solo para poder acotar el tema de las *fake news* en su red social. En definitiva, es algo tremendamente importante y tecnológicamente tiene solución.

Desde el punto de vista legislativo, Europa y también España están trabajando bastante fuerte en el tema, tanto con la transposición de la Directiva NIS y la reciente normativa sobre protección de datos de GDPR como en múltiple legislación aplicable para protección de infraestructuras críticas. Creo que lo estamos haciendo bien, y la nota que pondría sería un notable. Para el sobresaliente, el problema es que aún tenemos que entender que el mundo del que hablamos es digital pero constantemente creemos que seguimos en un mundo analógico o que de alguna manera crece linealmente, de manera que continuamente aparece normativa en la que se clasifica a las empresas así. Por ejemplo, por ser una empresa de telecomunicaciones, consideramos que solo hace telecomunicaciones, o, por ser una empresa de servicios digitales, que solo presta servicios digitales. Sin embargo, en el mundo en que vivimos muchas empresas digitales son a su vez proveedores de comunicaciones y hacen *mobile banking*, o también son empresas de taxis, o tienen una app y son la empresa más grande del sector turístico, es decir, los sectores y los hipersectores están tremendamente mezclados, y, sin embargo, desde el punto de vista legislativo seguimos considerando que son sectores estancos. Hay una que sin tener almacenes es la empresa de *retail* más grande del mundo, y otra que sin tener un solo taxi es la empresa de transportes más grande del mundo, y seguimos aplicando determinadas leyes para los propietarios de determinados vehículos, porque creemos que si alguien está en transportes ha de tener vehículos, pero resulta que la principal compañía de transportes del mundo no tiene ninguno.

Acerca de la cultura del riesgo, creo que es una pregunta muy buena, sobre todo porque considero que nos falta concienciación en ciberseguridad. Me gustaría poner un ejemplo. La mitad de mi tiempo lo paso en un avión, viajando por el mundo, porque, evidentemente, Telefónica tiene cobertura mundial. Hace apenas tres años, en un evento en Colombia pregunté a cuánta gente conocían que hubiesen hecho un paseíto millonario. Entiendo que se sabe qué significa esta expresión por su propio nombre, y es que se lleva a la persona por todos los cajeros hasta que sus tarjetas dicen basta —evidentemente, se le roba todo el dinero—. Ante esta pregunta frente a una audiencia de unas doscientas personas, apenas levantaron la mano tres que dijeron que en los últimos años habían conocido a alguien a quien habían hecho un paseíto millonario. Después pregunté cuántos conocían a gente a la que hubieran robado con ransomware trescientos euros o cantidades similares y más de la mitad de la sala levantó la mano. Este simple ejercicio, que se puede comprobar en las estadísticas, hace referencia a que es más probable que estando en Bogotá alguien nos robe trescientos euros en el hotel infectándonos el PC o que nos pidan dinero por un secuestro que alguien nos atraque por la calle. Es decir, la sensación de inseguridad la tenemos en el mundo físico, y no en el mundo digital, cuando la inseguridad en el mundo digital a día de hoy es tremendamente mayor, dado que no se han tomado las medidas adecuadas. Por tanto, creo que nos falta concienciación en estos aspectos, pero no porque se esté haciendo mal. Suelo decir que estamos en la Edad del Bronce en ciberseguridad, es decir, es algo muy nuevo, y, si sigue habiendo asesinatos después de miles de años de historia, pensar que fuera perfecto algo que apenas tiene treinta años sería inaudito. Por tanto, hay que hacer una labor de concienciación, y creo que INCIBE, en España, es uno de los organismos que mejor lo están haciendo a nivel mundial. De hecho, determinadas prácticas se están replicando en Latinoamérica. Por eso, mi reflexión en este punto es que lo estamos haciendo bien pero queda mucho camino por recorrer. Como decía, estamos hablando de la Edad del Bronce de la ciberseguridad.

Desde el punto de vista de la colaboración entre el sector privado y el sector público, hay colaboración pero es manifiestamente mejorable si la comparamos con países líderes, como Estados Unidos o Israel. Si bien esa colaboración existe, se fomenta y hay grandes iniciativas en el territorio nacional, como la existente con el INCIBE, con el CCN, con las Fuerzas y Cuerpos de Seguridad del Estado, con los distintos organismos que se dedican a la ciberseguridad en las comunidades autónomas y organismos como el CNPIC, todavía debe crecer más.

Desde el punto de vista de fortalezas y vulnerabilidades internacionales, creo que tenemos una fortaleza tremenda en España desde el punto de vista tecnológico. España siempre ha sido una nación en la que se ha utilizado la tecnología, y hay campeones nacionales y mundiales, como la propia Telefónica, Indra y similares, y, dentro del mundo de las *startups,* algunas están liderando en esta materia a nivel mundial. Lo que falta es garantizar una mayor inversión si queremos que llegue al siguiente término.

En cuanto a la inversión estatal en ciberseguridad y si es adecuada o no, permítanme que no haga valoraciones, dado que no dispongo del dato exacto al respecto. Sí le puedo hablar del sector privado,

cve: DSCG-12-CM-97

donde la inversión y el gasto en seguridad ligada a la tecnología aparece en las compañías de telecomunicaciones, en los bancos, etcétera, que en general invierten por encima del 10 % del total invertido en tecnología en materia de ciberseguridad. Luego tenemos compañías logísticas, de *retail*, etcétera, con una inversión que ronda aproximadamente el 5 %, y después aparecen sectores con apetito inversor en ciberseguridad, especialmente en las pymes, donde la inversión en tecnología es inferior al 2 %. Respecto al nivel de I+D+I en el sector público y privado, a día de hoy, en Telefónica, que es el ámbito que más conozco, en la parte de ciberseguridad hemos invertido más de cien millones durante los últimos años. Como comentaba, tenemos más de veinte *startups* ciberacelaradas. Recientemente, trabajamos con el Programa General Communications Headquarters en Inglaterra, por el cual estamos ciberacelerando cada año diez *startups* en materia de ciberseguridad, y la colaboración y la inversión es alta. De hecho, en el caso concreto de Telefónica, aproximadamente el 15 % de las patentes que generamos todos los años son en materia de ciberseguridad.

En cuanto a la pregunta sobre empleo, que hacía referencia a las Jornadas de Ciberdefensa 2018 que se están celebrando durante estos días, sin duda alguna, la clave es fomentar el talento. Insisto, en un país como el nuestro, la posibilidad de creación de empleo, el entrenamiento y la formación sobre todo en lo que se refiere a Security Education, Training and Awareness, es decir, la educación de la seguridad, el entrenamiento y la concienciación, requiere una hoja de ruta que no es fácil. Esta hoja de ruta implica planteamientos —como están haciendo en Israel o en determinados países— que requieren planes a cinco y diez años para poder conseguirlo. No son planes que se puedan hacer de la noche a la mañana ni en cuestión de seis meses; implica formar a determinada gente, entrenarlos y hacer que campeones nacionales o determinadas empresas sean capaces. Y esta empleabilidad, repito, no es solo la que pueda tener un país como España, porque los ciberprofesionales desde el punto de vista de servicios de seguridad gestionada viajan. Es decir, se puede gestionar desde Madrid un determinado elemento de seguridad que está en China o en cualquier país. De hecho, como muchos sabrán, ese es el éxito principal de Bangalore en la India, donde tienen millones de profesionales dedicados a la tecnología gestionando redes y sistemas a nivel mundial.

Respecto a la anticipación, es un tema clave y es verdad que es el mantra que debemos conseguir, pero a día de hoy la anticipación se consigue en no más del 10 % de los casos. La anticipación no es posible en todos los casos y, evidentemente, la inteligencia artificial que tenemos a día de hoy no es la que veremos en el año 2030 ni en 2050. Es decir, estamos haciendo distintas cosas, como comentaba, hay algunas aplicabilidades como el escudo contra ataques de denegación de servicio o cómo detectar determinado *malware* —*software* malicioso— en base a determinados comportamientos. Esto permite determinadas anticipaciones, pero el hecho de que falten tres millones de ciberprofesionales para el año 2021 o los dos millones que faltan a día de hoy, es un síntoma de que no hemos conseguido la anticipación de tener un robot o un *software* que automáticamente nos proteja en materia de ciberseguridad. Es uno de los campos de mayor crecimiento, todo lo referente al *machine learning* en la ciberseguridad y cómo con algoritmos aplicados al *big data* podemos ser capaces de prevenir determinados casos, que se está utilizando actualmente para ataques de denegación de servicio o detección de determinados comportamientos, pero no puede ser aplicado a todos los campos.

En cuanto a la evaluación del sector privado y público y la protección de las infraestructuras críticas, hoy en España tenemos múltiples organismos que se dedican a la seguridad. Creo que somos bastante punteros a nivel mundial con organismos como el Centro Criptológico Nacional, Incibe y los CERT que existen en la Policía y la Guardia Civil, los distintos centros de ciberseguridad que existen en las comunidades autónomas o el Mando Conjunto de Ciberseguridad dentro del Ministerio de Defensa. Creo que todos estos grupos nos posicionan a nivel mundial y tenemos una inversión adecuada para poder proteger nuestras infraestructuras. Desde el punto de vista privado, a día de hoy hay una inversión bastante adecuada en las grandes empresas y una falta de concienciación de las pymes, especialmente de las pequeñas empresas, que en muchas ocasiones no se pueden permitir la ciberseguridad, sobre todo porque no lo entienden o se lo explicamos de una manera muy compleja. Desde el punto de vista de los ciudadanos, pasa algo parecido a lo que sucede con las pequeñas empresas. De hecho, nuestra apuesta es cada vez más que los sistemas de seguridad vayan embebidos por defecto en los múltiples productos disponibles, con una política de *security by default* en los distintos entornos. Adicionalmente, las pequeñas empresas y los particulares más que seguridad están buscando un concepto que normalmente se utiliza en inglés, *peace of mind*, es decir, tranquilidad. Igual que cuando uno compra un seguro busca estar protegido, se busca este concepto *peace of mind,* puesto que no se le puede explicar a alguien una

cve: DSCG-12-CM-97

determinada vulnerabilidad en las redes wifi del algoritmo WPA2 con intercambio de clave PSK, que son los anuncios que aparecen en los distintos sistemas, porque no los entiende ni el 0,1 % de la población. Por tanto, hay que hacer una seguridad para todos, que sea entendible, no es necesario ser ingeniero para poder aplicarla. Simplemente, igual que abrimos el grifo y sale agua potable, las redes de comunicaciones en el futuro deberían ser exactamente igual; es decir, nos conectamos y debería ser limpio, no debería salir barro.

Desde el punto de vista de las demandas, entre el consumo, las pymes y las grandes cuentas, el consumidor y las pequeñas empresas lo que más nos demandan es *peace of mind;* es decir, necesitamos que alguien nos haga todo y que de alguna manera nos dé la seguridad y la certeza; y en las grandes cuentas evidentemente hay trajes a medida. No es lo mismo la seguridad que requiere un gran banco, una empresa de transporte o una empresa energética, cada uno tiene sus distintos factores. Es verdad que tienen determinados puntos en común, pero muchas particularidades. Desde el punto de vista del sector, como comentaba, está creciendo a doble dígito y las capacidades de que disponemos en la actualidad hacen que España como país, desde el punto de vista tecnológico, pueda estar debidamente contento. Es uno de los puntos en los que se está invirtiendo cada vez más con determinados organismos públicos, ya sea a nivel estatal o de las comunidades autónomas, con lo que la ciberseguridad ha entrado en la agenda de todas las administraciones públicas. Desde los últimos tres años se ha hecho un trabajo tremendo para que esto de alguna manera tenga sus frutos en los próximos años.

En cuanto al marco regulatorio, he hablado con anterioridad del GDPR que entra en vigor mañana, día 25, y nosotros y múltiples empresas nos llevamos preparando desde hace tiempo. Es una regulación que está para ayudar y que está haciendo que las inversiones en seguridad crezcan, pero, como siempre, para poder sacar el sobresaliente tenemos que asegurarnos de que estamos entendiendo la regulación del mundo digital en una regulación de 1980. Nos falta entender el mundo digital que se mueve exponencialmente y que las empresas son transnacionales y operan en no menos de veinte actividades tecnológicas, con lo cual cumplir la regulación para una multinacional con determinada regulación en ciberseguridad a nivel estatal, de comunidad autónoma, por ser protección de infraestructura crítica, por esta en España, por estar en Argentina, Brasil, Estados Unidos, etcétera, supone cumplir no menos de 250 leyes internacionales y es tremendamente complejo. Siendo esto muy positivo porque, como decía, podríamos calificar con un notable la regulación en ciberseguridad porque estamos haciendo un buen trabajo; para sacar un sobresaliente necesitamos entender más que el mundo digital tiene menos fronteras de las que pensamos.

Respecto a la coordinación, ya he comentado antes que entre Incibe, CCN, CNPIC, Policía, Guardia Civil y los distintos organismos hay colaboración. Y respecto a las denuncias, que es un punto de los más importantes sobre todo en la transposición de la Directiva NIS y con la llegada del GDPR, la obligatoriedad de la denuncia y de explicar este tipo de casos van a hacer un buen favor a la transparencia de cara a los ciudadanos. La última pregunta se refería a formación, inversión y concienciación, nosotros seguimos trabajando con la Policía en la formación. De hecho, también trabajamos con Incibe con uno de los organismos de cibervoluntarios, y damos cursos de ciberseguridad, *ciberbullying,* etcétera, desde el equipo de Telefónica conjuntamente con Policía y con los cibervoluntarios de Incibe en múltiples colegios y asociaciones.

El señor **PRESIDENTE:** Muchísimas gracias. Llevamos diez minutos de retraso. De todos modos, vamos a abrir un segundo turno en el que cada portavoz tendrá tres minutos. Yo les rogaría que se limitasen a hacer las preguntas que consideren oportunas.

Tiene la palabra el señor Comorera Estarellas.

El señor **COMORERA ESTARELLAS:** Seré muy breve, intervendré únicamente para agradecer sus contestaciones y preguntar una simple curiosidad en relación con Telefónica. El 1 de septiembre de 2017, según el Ministerio de Justicia, el servicio de Internet proporcionado por Telefónica para el acceso a LexNET sufrió una oleada de ciberataques. No sé si usted sabe algo al respecto, si estaba ya dentro de Telefónica; si conoce lo que pasó y nos pudiera contar algo sobre este ataque, se lo agradecería porque soy miembro de la Comisión de Justicia y me interesa el servicio LexNET.

Muchas gracias.

El señor **PRESIDENTE:** Tiene la palabra el señor Luena.

cve: DSCG-12-CM-97

El señor **LUENA LÓPEZ:** Intervengo únicamente para agradecerle de nuevo, en nombre del Grupo Parlamentario Socialista, sus aportaciones, ha cumplido las expectativas que teníamos puestas en su comparecencia; y recordarle, como a todos los comparecientes, que esta es una tarea colectiva; que recuerde en su trabajo las tareas de esta Comisión porque finalmente no solamente tenemos que llenar el granero, sino que me quedo con la última metáfora que es mejor, y es que si queremos llegar a la Edad de Hierro y superar la Edad de Bronce, tendremos que seguir trabajando. Dice usted que estamos en un notable, el Grupo Parlamentario Socialista como somos el principal partido de la oposición es más modesto en esa calificación, pero en todo caso como se trata de construir entre todos una estrategia de política pública en torno a la ciberseguridad, le reitero nuestro agradecimiento por sus respuestas.

El señor **PRESIDENTE:** Muchas gracias, señor Luena. Espero que lleguemos a la edad de oro.
Tiene la palabra el señor Cosidó.

El señor **COSIDÓ GUTIÉRREZ:** Muchas gracias, señor presidente.
También intervendré brevísimamente, primero, para agradecer todas sus respuestas. Creo que ha contestado todo, lo cual no era nada fácil. El departamento que usted dirige en Telefónica es un proveedor de servicios de ciberseguridad, y no me ha quedado nada claro si la ciberseguridad dentro de la compañía tiene un departamento diferenciado o su departamento hace prestación al exterior y al interior de la compañía. En segundo lugar, hemos hablando del déficit de ciberprofesionales, de expertos en ciberseguridad, y me gustaría que hiciese algún comentario sobre cómo está respondiendo la universidad española y en general cómo estamos respondiendo a esa demanda o necesidad de formación tan clara. Nosotros, como estamos en el Gobierno, no solo aspiramos a mejorar el notable, sino que optamos a la matrícula honor.
Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señor Cosidó.
Le traslado dos preguntas para responder.

El señor **PÉREZ GARCÍA** (CEO Unidad Ciberseguridad Telefónica, Eleven Paths): En cuanto a la primera pregunta sobre el incidente de justicia, permítame que no la conteste porque es un tema sobre el que ya se hizo una nota pública. En cualquier incidente el que tiene que dar la explicación oportuna es el afectado. Respecto a la organización en materia de ciberseguridad de Telefónica, yo dirijo toda la unidad de negocio de ciberseguridad que, como comentaba con anterioridad, factura a día de hoy más de quinientos millones, siendo Telefónica uno de sus clientes. La unidad interna de ciberseguridad está dirigida por Miguel Sánchez, anterior miembro del centro. En cuanto a la pregunta sobre las universidades desde el punto de vista de la formación, antes no he hecho excesivo hincapié en este aspecto y creo que es muy importante matizar que la ciberseguridad no es solo para ingenieros. Es decir, cuando hablamos sobre cumplimiento del GDPR hay múltiples personas que son abogados o con formación jurídica; cuando hablamos de ciberseguridad aparecen matemáticos para hacer algoritmos, o cuando hablamos del mundo de Internet de las cosas y seguridad aparecen ingenieros industriales, etcétera. Es decir, es una actividad tremendamente diversa en la que no solo hacen falta expertos que vengan de la universidad, sino también personas con formaciones en otro tipo de grados, incluso gente que no tiene un título universitario tiene cabida en los puntos de la ciberseguridad, de tal manera que la formación tiene que ir en 360 grados y sobre todo de una manera holística para garantizar que formamos no solo a los ingenieros, sino también a la gente que proviene del ámbito legal. Desde el punto de vista de ciberseguridad, lo que veremos en el futuro es que, igual que explicamos la seguridad vial o la seguridad en determinadas materias a nuestros hijos en los colegios, aparecerán asignaturas sobre ciberseguridad para explicar cómo hacer un buen uso de las tecnologías. Si los menores pasan no menos de dos o tres horas conectados a Internet, habrá que explicar y de alguna manera tutelar y educar en cómo se deben utilizar estos nuevos medios digitales.
Gracias.

El señor **PRESIDENTE:** Muchísimas gracias, don Pedro Pablo Pérez, por su intervención.
Tenemos ya aquí al siguiente compareciente, pero su intervención está prevista a las dos y cuarto. Aquellas señorías que no se sientan obligadas por el ramadán cuentan con media hora para comer y estar aquí a las dos y cuarto. **(Pausa).**

cve: DSCG-12-CM-97

— DEL SEÑOR DIRECTOR DEL CENTRO NACIONAL DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS, CNPIC (SÁNCHEZ GÓMEZ), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 212/001636 y número de expediente del Senado 713/000970).

El señor **PRESIDENTE:** Hay un cambio de planes, en este régimen cuasiasambleario que tenemos en la Comisión, las inscritas y los inscritos han decidido que adelantemos la siguiente comparecencia. Y es exactamente lo que vamos a hacer dando la palabra a don Fernando Sánchez Gómez.

El señor **DIRECTOR DEL CENTRO NACIONAL DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS, CNPIC** (Sánchez Gómez)**:** Muchas gracias, señor presidente.

Voy a aprovechar para cargar una presentación que puede ser algo más visual. **(Apoya su intervención con una presentación en Power Point).** Señorías, buenas tardes. Comparezco ante la Comisión y ante esta sede para informar de las actividades que el Centro Nacional de Protección de Infraestructuras y Ciberseguridad, conocido como CNPIC y que depende del Ministerio del Interior, realiza en un ámbito de tanta trascendencia como es el de la ciberseguridad, que es vital no solo para nuestra seguridad nacional, sino también para nuestra economía y, me atrevería a decir, que para el desarrollo de nuestro estilo de vida y para la garantía de nuestros derechos y libertades. A tal fin estructuraré mi intervención en dos partes, una primera dedicada a cuestiones generales, en la que trataré de identificar los principales rasgos de la ciberseguridad en lo concerniente a mi departamento y al Ministerio del Interior; y una segunda parte en la que voy a procurar ahondar en las labores concretas que el CNPIC desarrolla incardinándolas en el esfuerzo común de nuestra seguridad.

Lo primero que quisiera comentar es que, como pueden ver en pantalla, los avances tecnológicos están revolucionando la forma en la que trabajamos y en la que vivimos, pero este adelanto viene acompañado ineludiblemente de un aumento de las ciberamenzas. Ya hay numerosos expertos que han alertado de que los ataques van a tener un alcance cada vez más amplio y de que el cibercrimen y otras conductas van a continuar profesionalizándose. Y esto supone una afección sobre nuestra propia seguridad nacional, como reconocen tanto la Estrategia de Seguridad Europea de 2016 como la Estrategia de Seguridad Nacional de 2017. Según refleja el informe del Foro Económico Mundial sobre los Riesgos Globales 2018, que pueden ver en pantalla y cuya lectura recomiendo, por orden de importancia los ciberataques aparecen ya como la tercera amenaza más probable y como la sexta con efectos potenciales más negativos a nivel mundial, tan solo detrás de amenazas tan graves para la propia humanidad como las armas de destrucción masiva, los efectos climatológicos extremos, las catástrofes naturales, el cambio climático o las crisis de agua. Esto da idea de la dimensión del problema al que nos enfrentamos. Según este mismo informe, el impacto de Internet y de las redes sociales es imparable. Globalmente, se calcula que en 2017 había cerca de 8400 millones de dispositivos con conexión a Internet, superando ya en más de mil millones el número de habitantes del planeta cifrado en 7600 millones. Pero es que en el año 2020 se estima que los dispositivos con conexión a Internet van a ser alrededor de 20 400 millones. No obstante, la aproximación a la ciberseguridad, si bien de nuevo cuño, conceptualmente hablando, no debería ser tratada de forma distinta al concepto de seguridad con mayúsculas, que es el concepto superior que le da cobertura.

Como pueden ustedes observar en este diagrama, *grosso modo,* este es el ecosistema de amenazas al que nos enfrentamos en el ciberespacio. Pueden ver en rojo la tipología de acciones más comunes y en blanco los actores que las pueden originar, pero en el momento en el que el prefijo ciber es suprimido, volvemos otra vez al mundo físico, a un contexto mucho mejor conocido, con amenazas dimensionadas y al menos estudiadas y, por supuesto, con los mismos actores que, como ven, no varían en absoluto. Por lo tanto, la ciberseguridad no debe ser considerada como un elemento ni ajeno ni distinto al concepto global superior de seguridad, como bien reconoce nuestra propia Estrategia de Seguridad Nacional. La aproximación a la ciberseguridad requeriría así de la aplicación de una estrategia integral, y cualquier estrategia relacionada con la seguridad debe abarcar de manera transversal cuatro pilares básicos de actuación: prevención, protección, respuesta y persecución. De esta manera, la ciberseguridad debería ser abordada, por supuesto, con herramientas y con metodologías propias de las nuevas tecnologías, pero siempre sin perder de vista la perspectiva integral innovadora y aglutinadora de acciones en los cuatro pilares que acabo de mencionar, que permitan conectar las políticas y acciones que se implanten con otros campos ya existentes en nuestra Estrategia de Seguridad Nacional.

cve: DSCG-12-CM-97

En el aspecto técnico las acciones destinadas a dotar a nuestro país de la ciberseguridad adecuada son los centros de respuesta a incidentes cibernéticos o CSIRT —en este caso pueden ver en pantalla los nacionales—, así como otros organismos con capacidades de ciberseguridad, que son competentes en estos pilares de prevención, protección y respuesta. Destacan el Centro Criptológico Nacional, competente en lo referido a ciberseguridad de administraciones públicas, el CERT de Seguridad e Industria en lo relativo al sector privado y al ciudadano, el Mando de Ciberdefensa en materia de ciberseguridad de redes y sistemas militares y las unidades del Ministerio del Interior en el ejercicio de sus propias atribuciones. A todos ellos se deben añadir otros protagonistas que cada vez son más importantes para nuestra seguridad, precisamente las organizaciones privadas, que tienen sus propias capacidades tecnológicas para salvaguardar sus activos y, de paso, los servicios que proporcionan. Sin embargo, este último ámbito, el cuatro, el de la persecución, es exclusivo del Ministerio del Interior, ya que desde el momento en que se produce un ciberataque estamos hablando ya de una cuestión que en principio puede ser judicializada y, por lo tanto, el resto de actuaciones estarían condicionadas al concepto de Policía Judicial que, como saben, es cuestión exclusiva de la Fuerzas y Cuerpos de Seguridad del Estado. De esta manera, es importante resaltar que en España el único ministerio presente en todo el ciclo de vida de la ciberseguridad es precisamente el Ministerio del Interior. Y como trataré de explicar más adelante, el pivote sobre el que gira la coordinación de estos cuatro pilares es precisamente el Centro Nacional de Protección de Infraestructuras y Ciberseguridad, CNPIC.

A grandes rasgos y sin tener en cuenta la infinidad de factores y matices que intervienen en su parametrización, podrían esbozarse tres grandes bloques de amenazas para y desde el ciberespacio, que se diferencian tanto por su motivación como por sus capacidades. En cuanto a su motivación, como pueden ver están encarnadas, en primer lugar, por la delincuencia y los delincuentes que actúan con un móvil fundamentalmente económico, que ocupan en cuanto a número de actividades, con mucha diferencia, el primer puesto entre todos los agentes de la amenaza. Su impacto sobre la seguridad es muy heterogéneo, pudiendo abarcar desde delincuentes individuales y pequeños fraudes hasta delitos a gran escala realizados por grandes redes criminales. En 2017 la estadística del Ministerio del Interior refleja que la cifra de ciberdelitos se disparó a más de 81 000, de los cuales, como pueden ver en pantalla, casi las tres cuartas partes, el 74 %, se referían a fraude informático. El segundo de los actores, por llamarlos de alguna forma, es el *hacktivista,* de carácter preferentemente ideológico, antisistema, organizado en torno a pensamientos o ideas más o menos radicales.

Y un tercer ejemplo es el de los Estados y Gobiernos, cuya motivación es de carácter política o estratégica. El ciberespionaje es posiblemente la actividad más desarrollada a día de hoy, pero tampoco son infrecuentes las acciones de sabotaje o incluso la ciberguerra. Una derivación de todo esto es precisamente lo que está tan de moda, que son las amenazadas híbridas. Lo realmente importante no es tanto la motivación como las capacidades que hay detrás, la participación de servicios de inteligencia de algunos Estados, de unidades cibernéticas de sus Fuerzas Armadas, de grandes compañías multinacionales o de grandes organizaciones criminales, confiere a todo una especial gradación al estar dotados de grandes medios y recursos técnicos y de una gran capacidad de acción y estas son con diferencia las acciones potencialmente más peligrosas.

Pues bien, de forma transversal a todos estos grupos que acabo de mencionar, y con posibilidades de ser realizadas por cualquiera de ellos con una u otra motivación, están las posibilidades de ataques terroristas valiéndose de la Red. La peor de las hipótesis es precisamente un ataque contra nuestras infraestructuras críticas y los servicios esenciales que trataré de esbozar a continuación. Como ya saben en España, según determina la Ley 8/2011 de protección de infraestructuras críticas, existen reconocidos doce sectores estratégicos que pueden ver en la pantalla. Se definen estos sectores estratégicos como cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva nacional que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o la seguridad del país. La caída de uno o de varios de estos servicios esenciales puede provocar graves impactos que desde el CNPIC son valorados conforme una serie de parámetros: victimización, impacto económico, impacto sobre el medio ambiente e impacto público y social con deterioro de servicios y bienes.

Esta mezcla de servicios esenciales, por un lado, y de tecnología, por otra, es la que nos ha llevado a una serie de conclusiones desde el centro. En primer lugar, que nuestro país como toda sociedad hipertecnificada es extremadamente dependiente de esto que denominamos infraestructuras críticas, o mejor dicho, de los servicios esenciales que proporciona. Hoy en día no hay actividad de Gobierno económica, social o humana que no se encuentre vinculada o dependa de una u otra forma de algunos de

cve: DSCG-12-CM-97

estos servicios que hemos visto en esos doce sectores antes en pantalla. La parte negativa de todo esto es que nos hace enormemente vulnerables, porque somos muy dependientes.

La segunda reflexión se refiere a que los servicios esenciales y las infraestructuras críticas que lo soportan son también dependientes entre sí, es el concepto de interdependencia. El correcto funcionamiento de una infraestructura o de un servicio condiciona la prestación del otro y desarrolla una cadena, cuya protección global lógicamente es la del eslabón más débil.

Por último, transversal a todo esto y como nexo de unión cada vez más importante, se encuentran las tecnologías de la información y las comunicaciones, las TIC, a través de las que se dirigen, se gestionan y se explotan la mayoría de las infraestructuras críticas y sus procesos productivos. Las perspectivas de futuro, como ya hemos podido apreciar anteriormente, son que las TIC serán responsables en un horizonte ya muy próximo del funcionamiento global de una sociedad en la que la conectividad de sistemas y de elementos se contabilizará por billones. Debo decir también llegados a este punto que en España alrededor del 80 % de nuestras infraestructuras, y lógicamente los servicios que proporcionan, están en manos del sector privado y esto hace vital una interlocución de estos con las autoridades en materia de seguridad.

En cuanto a la evolución de ciberincidentes, al igual que lo he introducido anteriormente con los ciberdelitos, los últimos cinco años han sido dramáticos. Estos datos que facilita el CERT de Seguridad e Industria que cogestiona el Ministerio del Interior, por un lado, y el Ministerio de Energía, Turismo y Agenda Digital, por otro, a través del Incibe y del CNPIC muestran cómo los ciberincidentes conocidos por este centro tecnológico han aumentado exponencialmente, de 12 000 en 2013 a 123 000 en 2017. Además, los incidentes en sistemas y redes gestionadas por operadores críticos, que son estos últimos que aparecen, han pasado de 18 a 885, en tan solo cinco años. Es un incremento muy superior a la media, casi se multiplica por veinte y esta proporción que evidentemente es muy baja respecto al total supone, sin embargo, el tramo más peligroso potencialmente. Entre estos casos se encuentran los ya bien conocidos WannaCry o NotPetya que afectaron a nuestro país y a otros el año pasado.

En cuanto a afección por sector estratégico destacan fundamentalmente los ataques contra el sistema financiero, contra el sistema energético, contra el transporte y contra el agua. Visto esto parece claro que garantizar la seguridad de las redes y de los componentes tecnológicos es clave y con esa idea en mente está configurado el CNPIC en la parte que le compete.

Paso ya a la segunda parte de mi intervención que se refiere a cómo estamos trabajando, qué es lo que hacemos y lógicamente incardinados en el esfuerzo de seguridad nacional. El CNPIC, como acabo de comentar brevemente, tiene por tanto una doble orientación claramente definida. La primera, que es la más tradicional, está dirigida a la protección de las infraestructuras críticas y de los servicios esenciales y tienen un carácter de seguridad integral y, por tanto, engloba también la necesidad de dotar de ciberseguridad a nuestras infraestructuras, nuestras redes y nuestros sistemas. La segunda, que es más reciente, está dedicada a las funciones de coordinación de los cometidos de ciberseguridad encomendados al Ministerio del Interior y esta segunda función se realiza a través de la conocida como Oficina de Coordinación Cibernética que está en nuestro centro.

El primero de nuestros cometidos, que es el del sistema PIC, es disponer de un sistema coordinado —somos un ente fundamentalmente de coordinación— entre las instituciones del Gobierno, por un lado, y la empresa, por otro, para una mejor protección de las infraestructuras críticas y de los servicios esenciales del país con tres objetivos estratégicos: en primer lugar, que los operadores públicos o privados tomen medidas para optimizar la seguridad de sus infraestructuras, redes y sistemas; en segundo lugar, garantizar la seguridad y derechos de los ciudadanos y fundamentalmente su acceso a los servicios esenciales, como bien básico sobre el que se apoya nuestra vida y también nuestro sistema de convivencia, y finalmente, la evolución de este sistema PIC al cambio tecnológico y al cambio de modelo de seguridad nacional que estamos viviendo. Por eso este sistema que nació siendo eminentemente físico hace diez años ha evolucionado hacia un concepto de seguridad integral que prioriza los servicios y los sistemas sobre las infraestructuras concretas.

El servicio de protección de infraestructuras críticas está compuesto por ocho departamentos ministeriales, por otros tantos organismos de la Administración General del Estado y las administraciones autonómica y local y a esto se le deben añadir los operadores críticos, es decir, aquellos que gestionan y operan las infraestructuras y los servicios esenciales. La figura del operador crítico es una figura creada por primera vez por la Ley 8/2011, que ya mencioné anteriormente, y en su momento fue un hecho sin precedentes, ya que se dio la oportunidad por primera vez en nuestro país a actores del sector privado

cve: DSCG-12-CM-97

para participar en la propia seguridad nacional. El sistema PIC está presidido por el secretario de Estado de Seguridad, con el apoyo del CNPIC, y como ya he subrayado los operadores de los doce sectores estratégicos —estos son los diferentes planes que elaboramos respecto a estos sectores estratégicos— juegan un papel clave, donde las relaciones se basan principalmente en la confianza, en el intercambio de información y en la confidencialidad de los datos intercambiados por ambas partes. Actualmente, el sistema PIC está compuesto por más de 200 actores, de los cuales 150 son operadores críticos y constituye todo ello la mayor comunidad de cooperación público-privada de España en seguridad. En un momento en el que en materia de ciberseguridad se aboga de forma constante por la necesaria cooperación público-privada debe tenerse en cuenta este caso de éxito para extenderlo, como ya está haciendo el CNPIC, también al ámbito de la ciberseguridad.

La segunda de las misiones del centro se dirige exclusivamente a la ciberseguridad, pues el rol que el Ministerio del Interior ha querido dar a este centro es el de constituirlo en correa de transmisión de los diferentes agentes, participando en todo el ciclo de vida de la ciberseguridad. Todo ello se realiza, en primer lugar, a través de la integración, coordinación y contacto técnico con los Csirt nacionales, con los centros tecnológicos, en las fases de prevención, protección y respuesta. Aquí cabe recordar que el CNPIC participa de forma activa en el CERT de Seguridad e Industria de León y tenemos contacto y coordinación permanente con los otros dos; en segundo lugar, a través de la transmisión de información e inteligencia a nuestras Fuerzas y Cuerpos de Seguridad del Estado para la persecución del ciberdelito; y en tercer lugar, de cara a nuestros clientes originales que son los operadores críticos que en su mayor parte son privados, esta misma información puede ser trasladada, lógicamente en la medida que deba conocerse, para prevenir nuevos ataques, responder a los asistentes y recuperarse mejor de ello.

Para ello, como les decía, está la Oficina de Coordinación Cibernética (OCC), que fue creada mediante una instrucción del secretario de Estado de Seguridad en 2014, pero que no se reguló y se empezó a desarrollar hasta muy recientemente, a través del Real Decreto de regularización del Ministerio del Interior de 2017. ¿Cómo funciona esta Oficina de Coordinación Cibernética? Aquí pueden ver el esquema de ámbitos de actuación de los diferentes Csirt nacionales, el CCN sobre el sector público, el Csirt sobre la empresa privada y los ciudadanos, las capacidades militares y de defensa para el Mando de Ciberdefensa, los CERT privados para multitud de industrias y de empresas y los Csirt autonómicos. Este es un poco el mapa tecnológico de responsabilidad de nuestro país en materia de reacción, prevención y protección ante ciberataques. Pues bien, sobre esta estructura en aquellos casos en que los servicios esenciales o las infraestructuras críticas resulten o puedan resultar afectadas por un ciberincidente será el CNPIC, a través de esta oficina, quien coordine las actuaciones a seguir y muy especialmente con los actores de los operadores críticos y de las Fuerzas y Cuerpos de Seguridad del Estado.

Quiero mencionarles también que la OCC ha sido recientemente designada como punto de contacto español para la comunicación entre los Estados miembros con la Comisión Europea de aquellos ataques contra los sistemas de información previstos por la Directiva 2013/40/UE, que como consecuencia de esta directiva se traspusieron una serie de nuevos tipos a nuestro Código Penal. El artículo 13 de esta directiva establece la necesidad de constituir un punto de contacto permanente para facilitar la comunicación e investigación de esta serie de tipos y este punto de contacto ha recaído precisamente en nuestro centro.

Acabo ya mi intervención haciendo un pequeño resumen. Aquí pueden ver un diagrama de debilidades, amenazas, fortalezas y oportunidades respecto a la situación actual de la ciberseguridad en general y el sistema PIC en particular, desde mi humilde punto de vista. En cuanto a las fortalezas, como ya indiqué a lo largo de mi intervención, posiblemente nuestra mayor fortaleza reside en el tremendo potencial que supone coordinar el mayor sistema de colaboración público-privado en materia de seguridad de nuestro país y es también de los mayores de Europa. En los próximos años esperamos contar con más de 200 operadores trabajando con nosotros. Además, gozamos de una alta confianza del sector porque contamos con cierto prestigio nacional e internacional contrastado, ya que somos referencia en Europa y en muchos países de Iberoamérica que están copiando el modelo. Asimismo, nos basamos en un sistema legal, sólido y equilibrado nacido de la Ley 8/2011. Pero sin duda el mayor valor añadido que tiene el CNPIC es el que he mencionado anteriormente, que es el enlace natural con las Fuerzas y Cuerpos de Seguridad del Estado, con los operadores críticos y lógicamente con los CERT nacionales, con lo cual participamos en todo el ciclo de vida de la ciberseguridad.

En cuanto a debilidades, nuestra mayor debilidad —esto lo hago extensivo a la ciberseguridad de nuestro país— es la escasa cultura de seguridad existente. Es más patente si cabe a nivel ciudadano, pero sobre todo más preocupante a nivel directivo de nuestras organizaciones, ya sean públicas o

cve: DSCG-12-CM-97

privadas. Esto se refleja en muchas ocasiones en escasez de medios humanos y materiales, con los que se tiene que hacer frente a las responsabilidades en todos los ámbitos, así como también en la deficitaria formación en ciberseguridad de nuestro sistema educativo, o en el escaso impacto de las nuevas tecnologías en nuestra industria.

Preparando esta intervención topé en Internet con esta estadística que les voy a proyectar a modo de ejemplo: trabajadores técnicos en Europa. Como ven están proliferando en Irlanda. Hay un listado de diez países, entre los cuales no está España, que va desde Irlanda hasta Portugal. Esa es una de las carencias fundamentales que yo me atrevería a resaltar.

Pasando al capítulo de amenazas básicamente he de volver a decir todo lo que ya dije al principio de mi intervención. Como amenazas principales, si no damos los pasos adecuados, tenemos que ser conscientes de que el adversario, ya sean terroristas, delincuentes o Estados, sí se están preparando en este campo. También como hemos visto nuestra sociedad es cada vez más dependiente de las tecnologías y esto constituye un verdadero talón de Aquiles, si no segurizan los medios con los que nos proporciona. Es evidente también que la inseguridad genera un impacto subjetivo a nivel económico que puede afectar directamente a la competitividad y a la prosperidad económica de cualquier país.

Finalmente, termino con el capítulo de oportunidades porque creo que tenemos muchas e importantes. En primer lugar, a nivel sistema de protección de infraestructuras críticas estamos a punto de culminarlo, esperamos culminarlo en el plazo de dos años. Para esto es necesario enlazarlo con otras normativas legales, como puede ser el caso de la Directiva NIS que se va a trasponer en nuestra legislación próximamente. Es vital tener una coherencia normativa sobre ambas normas.

Como ya he dicho a lo largo de mi intervención tenemos acceso a gran cantidad de información y generación de inteligencia y eso se puede y se debe hacer llegar a todos aquellos que tienen necesidad de ella para explotarla, no solo a las Fuerzas y Cuerpos de Seguridad sino también a los operadores y a otros agentes que deben ser capaces de explotar esta información para prevenir y para protegerse ante ciberataques. Lógicamente nuestra capacidad de apoyo a la industria nacional, la generación de puestos de trabajo, y cómo no, a la protección de derechos ciudadanos creo que es algo que es importante resaltar.

Para finalizar termino con tres conclusiones. Hoy en día es imposible garantizar la seguridad de un país tan solo desde los organismos de Gobierno y más en un escenario como el ciberespacio, donde actores no estatales tienen un protagonismo indiscutible. Si hay un terreno donde David puede derrotar a Goliat es precisamente este. Por tanto, la colaboración entre la Administración pública, empresa y ciudadanos es clave, ya que se necesita de una sinergia entre nosotros para hacer frente a las nuevas amenazas. La segunda conclusión se refiera a las políticas de ciberseguridad y la implantación de acciones en este campo que no son gratuitas. Las normas y las estrategias aprobadas y las que están por aprobarse necesitan de recursos y de medios para que puedan ponerse en marcha. En este sentido, nada mejor que este foro, el Parlamento, para trasladar esta idea de que las capacidades que necesitamos para llevar a cabo nuestro trabajo deben de tener un respaldo presupuestario. La tercera conclusión es que esto puede esperar poco porque el avance de la tecnología es tan rápido que las decisiones que puedan tomarse un día, pueden estar desfasadas al día siguiente. Uno de los inconvenientes de la revolución tecnológica en la que estamos inmersos especialmente es precisamente la inmediatez, lo que no quiere decir ni mucho menos improvisación. En cualquier caso, como colofón, el abordaje de la ciberseguridad debería tener el rango de política de Estado al mayor nivel, ya que es algo transversal a todos los dominios en los que hoy se mueve un país moderno.

Con esta reflexión acabo mi intervención. Me someto a sus preguntas, a las cuales contestaré en la medida en que sea capaz o pueda.

El señor **PRESIDENTE:** Muchísimas gracias, por su intervención.

Damos un primer turno de cinco minutos. Por el Grupo Mixto, señor Yanguas. **(Denegación).** Por el Grupo Ciudadanos, tiene la palabra el señor Salvador.

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

Quiero decirle que me ha encantado su intervención, por su estructura y por la capacidad de poder ver en la misma el fantástico trabajo que están haciendo con los recursos de los que dispone. Por lo menos sabemos que estamos en buenas manos, así como que la forma de trabajar y cuáles son los objetivos se están desarrollando bien.

cve: DSCG-12-CM-97

Me ha gustado mucho el concepto, que comparto plenamente, de seguridad integral. Digo esto porque siempre existe una confusión sobre este tema, al cual quiero referirme y preguntarle. Cuando uno cree que la seguridad presencial es distinta a la seguridad digital, se piensa que no necesariamente hay que dotarlas de los mismos recursos. Se entiende que la seguridad presencial que tiene que acometerse para esas infraestructuras críticas o para los ciudadanos tiene que ser de una manera, pero que la seguridad digital al final se soluciona más o menos con tres ordenadores y con cuatro cosas más. El compareciente anterior que era representante de Telefónica —que está en el apostolado de todo esto— nos decía que en este momento hay más riesgo de inseguridad digital que física en Colombia, un país donde hay más de cuatro millones de personas que viven directamente de la violencia. Por tanto, ese es un dato muy a tener en cuenta.

Asimismo, el compareciente anterior se ha referido al igual que usted, aunque desde su perspectiva desde el Ministerio de Interior, aportación que me ha gustado, a que al final la inseguridad se traduce en falta de competitividad y en un perjuicio económico, es decir, en un intangible que no se está quizás valorando. Solo se tienen en cuenta los ataques que se producen, qué tipo de efectos provocan y a partir de ahí qué perdidas ha habido, pero no se está siendo plenamente conscientes de que esos ataques suponen unas pérdidas determinadas. Es decir, a veces sucede que el intangible es muchísimo mayor que lo que realmente han ocasionado, porque lo que está en juego es la credibilidad de todo el conjunto en este sentido del sistema. Por tanto, comparto su concepto de seguridad integral. Me han gustado mucho esas dos diapositivas en las que mostraba los mismos actores y las mismas amenazas, independientemente de que se hablara de seguridad digital o no, algo que ha sido absolutamente gráfico.

Creo que también es muy importante la labor didáctica, tanto la suya como la que podamos desarrollar en todos los ámbitos con todo tipo de jornadas, etcétera, para contribuir también a esa cultura. Entendemos que esa cultura de la seguridad se tiene que impulsar desde las escuelas. Tenemos que empezar ahora para que en un futuro esas generaciones que vayan entrando tengan perfectamente esos conceptos arraigados de serie. También es verdad que hay que dar este tipo de formación en empresas u organismos, que normalmente es donde más falta hace, pero también al conjunto de los ciudadanos. Hay que hacerles ver la importancia que tiene este tema, porque la vida de cada persona está metida en sus datos móviles y la distorsión o el cambio de tus datos móviles pueden cambiarte la vida. En este sentido, probablemente no estemos haciendo lo mismo para intentar divulgar este asunto a todo el conjunto de la sociedad. Hay un cambio de era que implica riesgos y que nos afecta absolutamente a todos. Tenemos muchísimas oportunidades que no queremos cercenar, pero al mismo tiempo tenemos que ser conscientes como sociedad de que tenemos que afrontar este tema. No se puede dejar esto al criterio de los ciudadanos, si tienen interés o nivel de formación suficiente para darse cuenta de que eso es así, porque estaremos dejando a mucha gente muy vulnerable ya que puede que no hayan llegado a ser conscientes de la importancia de este tema, que les puede cambiar su vida y su negocio.

Me ha gustado mucho que usted se haya referido al tema —lo echábamos de menos en la comparecencia anterior, pero era normal ellos no eran Interior— de la persecución, a todo ese sistema que es reactivo preventivo e intenta dotarnos de medidas para poder afrontar esos retos y poder actuar rápidamente. Yo creo que es muy importante esa parte de la persecución y por eso quisiera preguntarle sobre ese tema. ¿Cómo actúan? ¿Cómo funciona el procedimiento de denuncias y la coordinación que existe con otros sistemas? Voy a ponerle un ejemplo, ya que hemos tenido al compareciente de Telefónica. ¿Es Telefónica quien les dice los problemas que han tenido y ustedes a partir de ahí inician algún tipo de procedimiento de persecución de las personas que han intentado vulnerar o crear algún tipo de distorsión? En esa persecución hay que poner un tope a las personas que cometen esos delitos para que sepan que se la están jugando, porque si no uno puede ir probando, probando, y si sale, sale, y si no sale, puede seguir probando. Este asunto sería importante.

Para finalizar he de decir que resulta normal que todos los comparecientes que tienen que ver con la Administración sean muy disciplinados. Entendemos que los recursos son escasos, que se hace el máximo esfuerzo posible y que tampoco es su papel decir algo muy fuerte. Pero me ha parecido un grito cuando decía que hay que actuar. Yo he creído entenderle muy claramente, más aún cuando ha mencionado la palabra presupuestos. ¿Estamos invirtiendo lo suficiente? Decimos que no hay profesionales suficientes, que hay que incluir en nuestro ciclo formativo esta materia para que haya esos profesionales, para poder avanzar en ese camino. Sin embargo, fichan a profesionales cuando se detecta que tienen las cualidades necesarias y contribuyen a su formación. ¿Hay un plan adecuado de formación continua de esos profesionales para estar absolutamente a la última? ¿Hay un plan de actualización

cve: DSCG-12-CM-97

tecnológica en todos los sentidos? Ustedes tienen que estar dotados, ya que al igual que en cualquier concepto de seguridad tradicional como el armamento o las escuchas hay que actualizarlo tecnológicamente, ustedes también deben hacerlo, más que nadie. ¿Tienen cubierto que esa renovación tecnológica se va produciendo conforme avanza los tiempos? ¿Hay la suficiente inversión en I+D+i para tratar de avanzar lo máximo posible y no estar solamente en la etapa de la prevención, sino podernos situar en ese mundo que va a venir y que se va a multiplicar con el tema de los dispositivos, la inteligencia artificial o el Internet de las cosas? Díganos a los partidos políticos de esta Cámara, que estamos haciendo esta ponencia para recoger la realidad, las carencias reales que tengan en estos temas, porque nos afecta absolutamente a todos. Aquí no vamos a tener diferencias, ni por decir una cosa vamos a atacar al Gobierno, sino que vamos a ponernos de acuerdo para exigir todos juntos —también me imagino que el partido que apoya al Gobierno— que haya los medios que sean necesarios para conseguir que la seguridad de los ciudadanos y de nuestras empresas sea la adecuada.

Muchas gracias.

El señor **PRESIDENTE:** Por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea, senador Comorera.

El señor **COMORERA ESTARELLAS:** Muchas gracias, señor Sánchez, por su comparecencia y su exposición, que me ha parecido muy bien estructurada y muy clarificadora.

Le voy a hacer algunas cuantas preguntas. Aunque ha apuntado algunas impresiones, me gustaría que me dijera cuál cree que es el estado actual de las infraestructuras esenciales de España en cuestión de seguridad, o si al menos puede ponerme una nota de cómo estamos para tener una cierta idea. Dado el modelo mixto de protección que tiene España ante los ciberataques, y teniendo en cuenta que aproximadamente como ha manifestado el 80 % de las infraestructuras críticas corresponden al sector privado, ¿cómo valoraría la cooperación entre el sector público y el privado en el intercambio de información?

Recientemente el Incibe apostaba por ejercer un mayor control sobre los operadores de telecomunicaciones para evitar los ciberataques y se justificaban en que era más fácil controlar a los proveedores de Internet, cuyas redes son utilizadas para los ciberataques que no a las pymes, por ejemplo. ¿Qué piensa que deberíamos hacer —si cree que hay que hacer algo— desde el Poder Legislativo para potenciar esa cooperación o ese control?

Hay una pregunta que ya hemos formulado al anterior compareciente. Dada las cifras de ciberincidentes y ciberataques que han crecido enormemente, ¿están creciendo realmente más o es que se están reportando muchos más, teniendo en cuenta que ahora sabemos más y ahora se detectan muchos más ciberataques ya que antes se tardaba muchísimo más tiempo en ser detectados? Se ha perdido un poco el miedo, las reticencias que tenía desde el sector privado por lo que llaman la pérdida reputacional que supone el reporte de este tipo de ciberataques y más teniendo en cuenta si hablamos de infraestructuras críticas.

En cuanto al Internet de las cosas, ¿de qué manera considera que se debe abordar desde la Administración esa imparable expansión que está teniendo y qué implicaciones puede tener, sobre todo para cuestiones de infraestructuras críticas?

Respecto a la inversión no le preguntaré más porque ya el compañero de Ciudadanos ha hecho las mismas preguntas que tenía preparadas. Evidentemente, uno de los objetivos de la estrategia de seguridad es avanzar en el cumplimiento de la normativa sobre protección de infraestructuras críticas y en el proceso de planificación escalonada previsto en dicha normativa. ¿Cómo valoraría el estado actual de cumplimiento de la normativa por parte de las infraestructuras?

Dentro de las infraestructuras críticas está la salud. Me he quedado parado porque en el cuadro que nos ha mostrado —si no he visto mal— ponía el 0,11 % de los ciberataques. Pero mirando datos yo he visto que la industria sanitaria sufrió el 26 % de los incidentes de seguridad producidos durante el segundo trimestre de 2017, algo que en teoría es bastante preocupante, dada la naturaleza de los datos de pacientes y la dependencia de los sistemas informáticos para ejecutar correctamente los flujos de trabajo clínico. Me ha chocado esto. ¿Podría decirme con qué datos me quedo y si realmente puede afectar a las infraestructuras críticas?

Para acabar quisiera preguntarle cuál de las áreas estratégicas entre las que se dividen las más de 3500 instalaciones, infraestructuras críticas sensibles, es la que más le preocupa y por qué. Lo que nos pueda explicar, teniendo en cuenta en que estamos en una sesión pública, *grosso modo*.

cve: DSCG-12-CM-97

El señor **PRESIDENTE:** Por el Grupo Socialista, señor Hernando.

El señor **HERNANDO VERA:** Gracias, presidente.

Gracias, señor Sánchez Gómez, por su exposición. Quiero darle la enhorabuena por el trabajo que vienen desarrollando los hombres y mujeres que forman parte del centro que usted dirige y también por su propio trabajo.

No seguiré exactamente el hilo de su intervención, sino que iré haciendo preguntas que tienen relación con casi todo lo que ha dicho. Lo primero que me llamó la atención cuando entré estos días en la página del centro nacional, del CNPIC, es que seguimos en nivel de alerta 4, nivel de riesgo alto en materia terrorista. ¿Cómo influye eso en materia de ciberseguridad? ¿Qué se hizo y qué se está haciendo para prevenir ese nivel alto de riesgo terrorista? Nos podemos imaginar qué se hace en materia de seguridad física, en infraestructuras, pero qué se hace en materia de ciberseguridad. ¿Cómo actuaron ustedes y cómo siguen actuando? Me imagino que esto ha permanecido naturalmente en el tiempo como consecuencia del mantenimiento de este nivel 4.

En segundo lugar, ¿cuál es el nivel de interrelación —usted lo ha llamado interdependencia, seguramente sea más adecuado— entre la ciberseguridad dentro de la Estrategia de Seguridad Nacional 2017 y el resto de seguridad en los distintos sectores? Usted ha hecho mención a este tema. En el sector de la seguridad energética, en el sector de la seguridad económica y financiera, porque da la impresión de que la ciberseguridad o que ante supuestos ataques a esos sectores van a ser fundamentalmente a través del ciberespacio y no a través de ataques físicos. Por tanto, cuál es el nivel de interdependencia o de interrelación. Ha hablado de déficit de formación y de déficit de titulaciones. El anterior compareciente habló de un *gap* de 2 millones a nivel mundial me parece. En el año 2011 hay una importante incorporación de miembros de las Fuerzas y Cuerpos de Seguridad del Estado al CNPIC, tanto de guardias civiles como de policías. No sé si además de estos miembros ustedes captan personal que no sean exactamente de las Fuerzas y Cuerpos de Seguridad del Estado. Ya le digo que si el presidente y el resto de grupos lo consideran oportuno y ustedes tienen a bien invitarnos a conocer el centro del Pardo, estaríamos encantados, porque creo que es puntero y además sería muy interesante para ilustrar el trabajo de esta Comisión. Me gustaría conocerlo, pero le pregunto eso. Ustedes captan personas de fuera de las Fuerzas y Cuerpos de Seguridad del Estado y cuáles creen ustedes que son las necesidades formativas de los profesionales en este tema. Si hay titulaciones universitarias suficientes. Es necesario habilitar nuevas titulaciones y cuáles son las titulaciones óptimas para actuar en el mundo de la ciberseguridad. Estos días preparando la comparecencia hay másteres, especializaciones, determinados cursos, muchos ingenieros informáticos, pero cuáles son las titulaciones óptimas y si faltan. Si hay una necesidad regulatoria de nuevas titulaciones, más allá de las titulaciones en sí mismas.

En cuanto al marco regulatorio, tenemos la Ley 8/2011, el Reglamento 704/2011, antes se nos decía, esto supone un crecimiento exponencial y cambios también exponenciales. ¿Detecta usted la necesidad de alguna reforma, tanto en la ley como en el reglamento? En relación con la Directiva NIS, tenía que estar traspuesta desde el pasado 9 de mayo, cuál ha sido el papel del centro que usted dirige y cuál ha sido el papel del ministerio del Interior, creo que esto lo está desarrollando otra secretaría de Estado de otro ministerio. Si usted conoce cuál es el punto en que nos encontramos en estos momentos de desarrollo de la ley para tener un conocimiento.

En cuanto al catálogo de infraestructuras críticas, ya sé que es materia reservada, que es secreto. No pretendo que lo revele ni mucho menos, lo que pretendo es que digan cómo lo actualizan, cómo incorporan nuevos operadores críticos, cómo los detectan y a partir de ahí y más allá de cuáles son las obligaciones de los nuevos operadores críticos, aparte de lo que nos digan los artículos 13 y 14 de la ley y del reglamento. Si todas las obligaciones de los operadores críticos van a cargo de los operadores críticos, digo económicamente, porque esto supone una serie de obligaciones que tienen coste económico o hay algún tipo de ayuda y de aportación por parte de la Administración. No estamos hablando de cualquier operadores críticos, sino que son operadores críticos que tienen suficientes medios para afrontar esas obligaciones que establecen la ley y el reglamento, pero en cualquier caso me gustaría que nos dijese cuál es el nivel de apoyo por parte de la Administración.

Una última cuestión, siempre estamos hablando de prevenir, de vigilar dentro del concepto global de resiliencia, hay planes especiales, antes se nos ha hablado de escudos de protección digital ante determinados procesos de participación democrática por parte del CNPIC. Es decir, ante un proceso electoral se toman medidas por parte del CNPIC o de otras instancias dentro de la Administración General

cve: DSCG-12-CM-97

del Estado para prevenir ataques. No estoy hablando de *fake news*, estoy hablando por ejemplo de un ataque a la empresa que se dedica a hacer el recuento el día d. Ese es un momento pico, de ciberseguridad, de inseguridad en el ciberespacio. Hay planes especiales y hay escudos digitales para prevenir este tipo de ataques. Con esto por ahora basta. Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señor Hernando.
Termina este turno la portavoz del Grupo Parlamentario Popular, señora Vázquez.

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

Quiero darle la bienvenida al director del CNPIC a esta Comisión y agradecerle su exposición que ha sido brillante práctica y muy ilustrativa para el desarrollo de esta ponencia que estamos llevando a cabo en el Congreso de los Diputados y en el Senado. Me quedo con la última frase que aparecía en su exposición: política de Estado. Y debe ser la política de Estado la ciberseguridad, más conectados, más vulnerables. Esa es la realidad. Después, como usted ha expuesto aquí, son doce sectores esenciales, como en todas las guerras esto ya no es un descubrimiento nuevo, las infraestructuras críticas siempre ha sido el objetivo del enemigo. Es decir, lo primero que atentaban en una guerra era el agua, la electricidad y los alimentos para intentar desabastecer a la población, con lo cual el papel que tiene el CNPIC es fundamental. Más cuando lo enlazamos con la ciberseguridad. Con los datos que usted dio, que no sé si los copié mal, creo que dijo que había 8 100 millones de dispositivos en estos momentos. Más que población. **(El señor director del Centro Nacional de Protección de las Infraestructuras Críticas, CNPIC (Sánchez Gómez): 8 400).** Ya 8 100 me parecía mucho, esto me parece muchísimo más que tengamos más dispositivos que población. Estamos en un mundo interconectado y con unas carencias que tenemos que dar respuesta tanto a los Estados como a las empresas privadas. Ya han sufrido países como Ucrania en el año 2015 ciberataques a centrales eléctricas. Nosotros no sé si hemos sufrido alguno, pero en todo caso países de la Unión Europea han sufrido ataques y ciberataques a las infraestructuras críticas. A mí me gustaría hacerle una serie de preguntas, algunas ya han sido reiteradas por mis compañeros. Yo le traía aquí una en concreto si se ha articulado algún dispositivo extraordinario de ciberseguridad en los procesos electorales recientes, que enlaza con la del Grupo Socialista. Me gustaría saber de qué manera puede afectar la implantación de la Directiva NIS al funcionamiento propio del CNPIC, que está ahora en fase de trasposición. Le gustaría saber al Grupo Popular con qué recursos cuenta el CNPIC para el desarrollo de sus competencias. Es decir que nos informe del número de efectivos y las competencias desarrolladas por esos efectivos. Cuántos incidentes de ciberseguridad, porque usted aquí hizo el de todo el conjunto de ciberseguridad ha gestionado el CNPIC en el año anterior, por ejemplo, en el año 2017, conjuntamente con el Incibe, porque creo que algunos se llevan con Incibe y CNPIC.

¿Cómo valora la cooperación de las empresas, que sabemos que es fundamental, y cómo valora las empresas que forman parte del catálogo de operadores críticos a la hora de comunicar y gestionar incidentes de ciberseguridad? El anterior compareciente nos hablaba de la valentía que tuvo *faceboock* reconociendo que habían sufrido un ataque y eso les supuso unas consecuencias económicas muy graves. Aquí en España nos hemos enterado a posteriori, días o semanas después, que habían sufrido ataques. Muchas veces se ocultan para no tener unas pérdidas de prestigio empresarial o económicas. Me gustaría que usted nos informara sobre esa valoración sobre la cooperación. Cómo valora el uso del sistema Hermes por parte de los operadores críticos. ¿Dispone de los recursos necesarios para verificar la información aportada por los operadores críticos al sistema Hermes? Volveríamos a incidir en el tema. Qué nivel de cumplimiento se ha verificado por parte de los operadores críticos en la entrega de los planes de seguridad de los operadores y de los planes de protección específicos que tiene del CNPIC. ¿Se han realizado actividades de inspección para verificar de forma aleatoria el cumplimiento de estos planes? ¿Cuál es el cumplimento de los planes de apoyo operativo? Se han realizado en el último año ejercicios que permitan determinar la eficacia de estos planes operativos. Por último, aunque como decían aquí pertenece a la Administración, pero usted es un magnífico profesional, he visto en su currículum que prácticamente lleva muchos años ahí, cómo se encuentra en CNPIC comparativamente con otras organizaciones de su estilo en otros países y algún rasgo que a lo mejor se pudiera implantar aquí en España el CNPIC y que usted echa en falta respecto a otros ejemplos que existan en la Unión Europea. Muchísimas gracias.

El señor **PRESIDENTE:** Muchísimas gracias a usted, señora Vázquez.
Señor Sánchez Gómez, por favor.

cve: DSCG-12-CM-97

El señor **DIRECTOR DEL CENTRO NACIONAL DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS, CNPIC** (Sánchez Gómez): Intentaré contestar a todas las preguntas. Desde luego, aprovecharé algunas respuestas para contestar otras. Quisiera hacer una reflexión de inicio que es en primer lugar todo lo que es el ciberespacio se debe considerar tanto como un fin, cuando hablamos de seguridad. Es decir, el ciberespacio se puede utilizar por los delincuentes, grosso modo, como fin o como medio. Como medio es lo que estamos viendo que no es tan diferente a quitarle el prefijo ciber, prácticamente los móviles son los mismos lo único que la metodología varía. Ese común medio se está convirtiendo en una herramienta para atacar y eso es algo que todavía a nivel sociedad —y no solo en España, sino en la mayoría de los países que tienen diferente grado de madurez— no hemos digerido. Siempre pongo un ejemplo muy sencillo que es: ¿alguien dejaría la puerta de su casa abierta o alguien dejaría las llaves puestas en su casa y se va? En España y en muchos países en la parte cibernética sí, porque no cumplimos con los protocolos de seguridad. No tenemos esa mentalidad de que tenemos que asegurar también nuestro mundo virtual. Se han puesto muchos ejemplos. Imagino que en esta sede se habrá hecho por alguno de los ponentes alguna referencia a esto, a que precisamente los ciudadanos nos descargamos cualquier cosa que suena a tecnología, nos metemos en nuestro móvil y no pedimos los niveles mínimos de seguridad. La base es que no estamos maduros en ciberseguridad, como sociedad ninguna, ni siquiera la más desarrollada, la más puntera en materia de seguridad no estamos maduros. Seguimos viendo, si me permiten la expresión, como un becerro de oro todo lo que sea tecnológico. Eso está muy bien pero no se ve la cara b, que la cara b es que a través de esas herramientas y de esas metodologías nos pueden atacar y somos vulnerables. Eso lo tenemos que asumir a nivel ciudadano y a nivel de otro tipo de organización. Digamos que ese sería quizás el primero, contestando ya a las primeras preguntas, de los debes que tenemos. No tenemos suficiente cultura de ciberseguridad, no la tenemos. Como país, no solo aquí, sino en muchos otros países. Esto debe ser cuestión de tiempo, lluvia fina. Tenemos una estrategia de ciberseguridad nacional que efectivamente aborda la cuestión, por ejemplo, de formación, pero eso lleva un tiempo de implantación e insisto también lleva que esto es algo transversal a todos los departamentos de Gobierno, en este caso la parte del Ministerio de Educación tiene mucho que decir ahí para tener tramos formativos, nuevas carreras adaptadas a las necesidades y eso es algo que me consta que se está trabajando, pero el problema, ahí venían algunas de las reflexiones mías que hacía en la intervención, es que los que trabajamos que somos profesionales en este mundo vemos que este mundo es muy rápido, es muy ágil, y nuestros mecanismos no son tan ágiles. Es cuestión muchas veces de tiempos, pero sacar adelante, por ejemplo, una regulación, una norma, se ha comentado la Directiva NIS, sacar todo eso e implantarlo lleva un tiempo y este mundo varía de la noche a la mañana, y este es un problema con el que vamos a tener que convivir, porque va siempre más rápido este tipo de situaciones que nuestras propias capacidades para adaptarnos, pero en este sentido creo que sí que vamos haciendo a nivel país nuestros deberes con muchas carencias y con muchas ganas de mejora, pero sí que están bien planteadas las diferentes áreas, las diferentes ocho líneas de acción de la estrategia de ciberseguridad.

Preguntaba el representante de Ciudadanos sobre la persecución, cómo hacíamos para la persecución del ciberdelito, lógicamente el ciberdelito tiene una metodología totalmente diferente al resto de las otras tres fases. Es básicamente algo mucho más operativo, mucho más tecnológico para ir tras el delincuente, detenerlo y ponerlo a disposición judicial. Ahí tenemos problemas en primer lugar a la hora del sistema judicial que tenemos, es decir, tenemos un sistema judicial que es enormemente garantista, pero un ataque de este tipo en muchos casos necesita operativamente hablando de una reacción inmediata y rápida y esto en muchos casos cuando se llega al mandamiento judicial o a la acción punitiva el delincuente ya no está ni se le espera y en muchos casos está en otro país. Nosotros cómo queremos trabajar el CNPIC a la hora de mejorar esas capacidades de nuestras unidades, haciendo de correa de transmisión. Como digo, tenemos acceso a una cantidad ingente de información. ¿Por qué? Porque los operadores nos reportan incidentes y también porque los CERT, los centros tecnológicos, nos hacen llegar información. Esa información nosotros ni podemos ni queremos explotarle. Nosotros nos limitamos a mandarle a nuestras unidades para ver si son tipificables como delito se judicialicen y a partir de ahí perdemos de vista ese tipo de acción.

Me preguntaba si estábamos invirtiendo en Plan de información continua, plan de actualización tecnológica, hay una línea de la propia estrategia de ciberseguridad que va en ese sentido, es cierto que va más lenta de lo que quisiéramos y también esta por detrás que la estrategia de ciberseguridad nacional nuestra actual no está dotada económicamente, es decir, la dotación se hace a nivel departamental, son

cve: DSCG-12-CM-97

los departamentos ministeriales, Ministerio del Interior, Ministerio de Defensa, los que abordan esas líneas de acción conforme a sus propios presupuestos. Quizás esa sería un área de mejora importante. Sin ir más lejos, la ciberestrategia británica que es de 2016 o 2021, que es un quinquenio, está dotada con 1 900 millones de libras, pero es algo que dota a toda la estrategia y a partir de ahí de reparten en todos los ministerios para que se lleve a cabo la inhalación. En el caso español somos los departamentos los que identificamos y se invierte en consecuencia, pero no hay dotación para ciberseguridad. En lo referido a presupuestos iría por ahí, si se están dotando en presupuestos del Estado, como bien saben, a nivel departamental, no a nivel ciberseguridad. Creo que esa variación podría ser más interesante.

Me preguntaba el representante de Podemos sobre el estado actual de las estructuras críticas en seguridad. Lo enlazo con la reacción de los operadores, que ha habido varias preguntas en ese sentido. Creo que sin intentar ser demasiado optimista el nivel de seguridad de nuestras infraestructuras críticas es alto, por razones en muchos casos culturales. Hemos estado inmersos en una situación de terrorismo durante muchos años y se ha calado en nuestra sociedad y en nuestras empresas privadas para tener un nivel internacional. En la parte ciber es cierto que no estamos al mismo nivel que la seguridad como un todo, porque se ve como un concepto en muchos casos naíf, que no tiene una afección real, cuando todo lo contrario, sí que lo tiene. Efectivamente el miedo que tenemos, hablaba la representante del Partido Popular de ataques a Ucrania, el miedo que tenemos es que un ciberataque puede causar efectos físicos. No es una broma, se puede paralizar. En este caso en Ucrania se vino abajo el sistema eléctrico, porque las máquinas, el Internet de las cosas, las ot, las tecnologías de la operación, o a una máquina se le da una instrucción errónea, que es una tipología de ataque cibernético, a la máquina que gestiona operativa de lo que sea, en este caso, se le da una instrucción errónea y puede quemar la máquina, por tanto se va la electricidad. Es decir, puede haber y de hecho es nuestro principal miedo a día de hoy consecuencias físicas sobre ataques cibernéticos. El nivel es alto y hay concienciación de nuestras empresas. Hay diferentes niveles de madurez. Yo diría que más de un 80 % cumplen perfectamente y hay un 20 % que van un poco más retrasados por medios, por capacidades y por falta de concienciación. Pero son un buen porcentaje. La cooperación público-privada, me va a permitir que saque un poco de pecho a nivel España. A nivel internacional somos un ejemplo, un caso de éxito de cómo nuestras organizaciones incluidas las privadas colaboran con la Administración, por lo menos con el CNPIC. Tenemos una relación de entendimiento. Hay una figura que es el operador crítico, que es el responsable de seguridad de enlace, que es una persona designada expresamente con capacidad de reacción y conocimiento de su empresa en materia de seguridad para interlocutar directamente con nosotros. Es verdad que muchas organizaciones tienen intereses económicos. En ese sentido nosotros firmamos un NBA un acuerdo de colaboración y de confidencialidad saben lo que es también, en muchos casos, a nivel directivo, no a nivel responsable o de la seguridad de otras empresas es a nivel directivo, que todavía no acaba de calar esa situación, pero con el tiempo vamos a irlo logrando.

Los ciberataques crecen y se reportan. Cada vez hay más ciberataques, son más dañinos y más sofisticados, pero también es verdad que la cifra negra también va bajando. Nos reportan más ciberataques. Un debe, más allá del reporter de ciberataques, es la denuncia a nuestras unidades de las Fuerzas y Cuerpos de Seguridad del Estado, si no se denuncia en muchos casos no se puede investigar. A nosotros nos reportan ciberataques, pero en muchos casos no discernimos si pueden ser o no objeto de delito. Nos vamos a los tres primeros puntos de los que hablaba: prevención, protección y respuesta. Pero la investigación es el plus para nuestras unidades y que se judicialice y a partir de ahí investigar. En eso todavía estamos un poquito retrasados y es cuestión también de concienciación. El estado de cumplimiento del operador crítico de la normativa PIC es alto un 80 %. Hay operadores que van más lentos. Saben ustedes que no tenemos régimen sancionador. Posiblemente vaya a ser una de las mejoras y ya borro también en qué mejoraría las normativas a efectos de las críticas. La aproximación inicial, de tener un régimen sancionador.

Nos queda una cifra que es un poquito más complicada gestionarla y que tendríamos que tener algún tipo de aproximación diferente.

En el tema de la salud, es relativamente sencillo. Todavía no hemos llegado a la salud. En una de las presentaciones que había varias fotografías de planes. Este año, justo dentro de un mes, posiblemente, la comisión PIC que dirige el secretario de Estado, que es el máximo órgano político en protección de infraestructuras críticas, hemos propuesto para la aprobación a la Comisión el plan estratégico de la salud, que lo hemos realizado de la mano del ministerio competente y de las organizaciones que pueden tener algo que ver ahí. A partir de ahí, creo que alguien me ha hecho una pregunta en ese sentido, ¿cómo

cve: DSCG-12-CM-97

identificamos a un operador crítico? Tenemos una serie de planes. Ahora mismo de los doce sectores estratégicos tenemos quince planes. Me preguntaba por qué quince y no dieciocho. Porque la electricidad, el gas y el petróleo son suficientemente potentes como para que hiciera un plan diferente de cada uno de ellos, aunque son parte del mismo sector que es el energético. Vamos a ir a dieciocho, ahora tenemos quince, que son los que ven en pantalla. El dieciséis va a ser el de la salud. A partir de ahí identificamos cuáles son las vulnerabilidades a las que nos enfrentamos como país, cuáles son los servicios estratégicos y esenciales que proporcionan estos sectores. Cuáles son los actores fundamentales, dentro de estos habrá algunos que son críticos y algunos que no son críticos y sobre estos sacamos las infraestructuras que tienen que gestionar, las redes y los sistemas y empezamos a planificar un sistema que es lento pero que está dando buenos resultados. Llegaremos al de la salud en breve, posiblemente las estadísticas crezcan a la hora de reportar incidentes.

En cuanto a los niveles de alerta, cómo influyen en materia de ciberseguridad. Como yo avanzaba al inicio de mi intervención, la ciberseguridad es una parte de seguridad. Como saben ustedes estamos en nivel 4 de alerta terrorista y esto tiene un plan, el plan contraterrorista, que nos dice donde nos encontramos. El hermano de ese plan es el plan nacional de protección de infraestructuras críticas y está hermanado en el nivel de la amenaza. ¿Qué significa esto? Que nosotros trasladamos estas prevenciones y estas obligaciones que el plan contraterrorista exige a las Fuerzas y Cuerpos de Seguridad del Estado y a las Fuerzas Armadas en un momento determinado y que mucha de esa información es lógicamente clasificada, trasladamos la parte que podemos a los operadores, para qué, para que ellos empiecen también a trabajar en la prevención de su sistema para que evidentemente un ataque, en este caso terrorista, tenga menor éxito. Es un escenario de colaboración público privada. A partir de ahí hay una parte de ciberseguridad en la cual nosotros le pedimos a los operadores que lleven a cabo una serie de medidas. Del 1 al 5, dependiendo en qué nivel nos encontramos y del reporter. Hay incidentes que no llegan a ser importantes, que en una ocasión normal no se nos reporta, pero cuando estamos en un determinado nivel pedimos que se nos reporte. A lo mejor no significa nada para el operador ni incluso para nosotros, pero si eso lo trasladamos a la unidad de inteligencia pueden sacar información que conecte con otra información y que pueda abordar mejor el riesgo terrorista que es alto que es nivel 4.

En cuanto a la interrelación con otros sectores, la ciberseguridad es un elemento que es transversal a todo. Hoy día prácticamente es imposible separar defensa o seguridad ciudadana o seguridad energética o seguridad en el transporte de lo que es la ciberseguridad, porque es transversal a todo ello. Por poner un ejemplo de seguridad energética, que también tenemos una estrategia, lógicamente ahí de qué forma afecta la ciberseguridad, por ejemplo en la gestión de las *smart grids*, de las redes inteligentes. Las redes inteligentes son las redes eléctricas que nos permiten tener una energía de calidad mucho mejor gestionada, pero esa gestión se lleva a cabo a través de máquinas, redes inteligentes. Por tanto, la ciberseguridad ahí es crítica y esencial, porque se puede llegar incluso a un contador mediante un *hackeo*. Nos pueden dejar sin energía eléctrica. Por tanto, impacta totalmente sobre la ciberseguridad. En estos planes que ven en pantalla precisamente hay un capítulo dedicado a la ciberseguridad. Es decir, identificamos qué riesgos cibernéticos existen sobre todos estos sectores para trasladarlo tanto a los operadores como, lógicamente, a los ministerios competentes. Es decir, estamos enlazando la ciberseguridad con todos estos planes y con el resto de sectores que puedan estar afectados.

En cuanto al déficit de personal, creo que tenemos un déficit de personal con talento a nivel país, no porque carezcamos de personal con talento sino por las vías para reclutarlo. Es algo que reiteradamente en cualquier organismo en que tenemos responsabilidad en materia de ciberseguridad estamos reclamando de alguna manera. También creo que es cuestión de mentalidad y de tiempos. Hemos evolucionado en muy poco tiempo. Esto, como ya se ha dicho, es una revolución digital; estamos evolucionando de un sistema que era eminentemente físico a un sistema en el que estamos cada vez más en un mundo virtual. Trasladar organizaciones e incluso plantillas a ese mundo cuesta tiempo; en muchos casos es un tema organizativo. Ese déficit existe pero, por ejemplo, en nuestro ministerio está previsto abordar esta situación, entre otras muchas, no solo en el CNPIC sino también en las Fuerzas y Cuerpos de Seguridad a través de un plan director de ciberseguridad que va a enlazar, lógicamente, con la Estrategia de ciberseguridad nacional. Eso es algo que se nos está encargando empezar a trabajar sobre ello. Obviamente, la visita a El Pardo cuando quieran, estamos totalmente abiertos a enseñarles aquello, que además es un lugar bucólico y cuenta con unas instalaciones que tecnológicamente están francamente bien.

En cuanto al marco regulatorio —y enlazo con la parte de la reforma—, apuntaba precisamente la parte sancionadora, pero hay mucho más. Desde 2011, nosotros quizás hemos sido de los primeros que

cve: DSCG-12-CM-97

empezamos a abordar el tema de la ciberseguridad de forma muy puntual pero no creíamos que fuera a tener tanta importancia como siete años después hemos descubierto; entonces, necesitamos alinear esa norma con la Directiva NIS. Me preguntaba sobre nuestro papel. Yo mismo he estado en el grupo de trabajo de la redacción del anteproyecto de la Directiva NIS, que lógicamente lidera el Minetad, el Ministerio de Energía a través de la Secretaria de Estado de Seguridad, Información y Agenda Digital. Hemos participado directamente en ella fundamentalmente porque en la Directiva NIS los sujetos regulados son, por un lado, la figura del operador esencial y, por otro, la del proveedor digital. El operador esencial lo define la Directiva NIS como aquel que proporciona servicios esenciales y que de alguna forma depende de la red de sistemas de información para la provisión de esos servicios. Esto encaja cien por cien con la Ley de Infraestructuras Críticas porque es integral. Es decir, cuando nosotros empezamos a trabajar en esto fuimos mucho más allá de la Directiva 114/2008 y no solo cogimos los sectores de energía y transporte, sino que fuimos a por todos los sectores y con un concepto integral, con lo cual esa parte sí la tenemos avanzada. Es cierto que la Directiva NIS está mucho más elaborada, está mucho más avanzada y vamos a tener que revisar la Ley PIC para integrarla según esa directiva —la parte que nos ocupa— y para tener un marco normativo que sea homogéneo y que esté alineado, que no vaya buscando cosas diferentes. En este sentido, el papel del grupo de trabajo para la redacción ya ha finalizado, está en proceso de redacción en las diferentes secretarías técnicas y entiendo que el siguiente paso sería el Consejo de Estado. Y después ya presentarla a las Cortes. Respecto a los plazos, lamento no tener datos.

En cuanto a las infraestructuras críticas, ¿cómo las actualizamos? El catálogo lo que contiene son las infraestructuras críticas. Al catálogo acceden tanto nuestras unidades como los propios operadores; entonces, la actualización es automática porque cuando hay algún cambio de la propia infraestructura o de treinta y cinco campos que tenemos para definir, es el propio operador el que nos lo dice; por ejemplo: hemos cambiado el director de seguridad, ahora se llama no sé quién; o hemos puesto un teléfono diferente, o esta infraestructura ya no da servicio, etcétera. Es decir, en el propio sistema se puede actualizar y después tenemos una interlocución permanente con los operadores. La designación de operadores se hace a través de los planes estratégicos sectoriales y es validada por la propia Comisión PIC, que, como digo, no solo somos nosotros, nosotros somos el brazo ejecutor, pero ahí hay ocho ministerios, está el Centro Nacional de Inteligencia, el Consejo de Seguridad Nuclear, están las comunidades autónomas, la FEM, y todos estos actores validan estas designaciones.

En lo referente a elecciones, como saben es el Ministerio del Interior, a través de la Subsecretaría de Interior, el órgano competente para la organización y celebración de elecciones generales. Por lo tanto, cuando hay elecciones es la Subsecretaría de Interior la que toma cartas en el asunto, la que efectúa la contratación de las empresas en cuestión y la que hace el seguimiento. En los últimos años hemos estado participando con la Subsecretaría de Interior para apoyarles tanto técnicamente como en situaciones de *fake news* o con información que podemos, digamos, extraer para que la Subsecretaría de Interior pueda realizar su trabajo de forma adecuada, correcta.

Me preguntaba la representante del Grupo Popular si se ha articulado algún dispositivo extraordinario de seguridad. Efectivamente, en las últimas elecciones hemos estado colaborando precisamente por el tema de las amenazas híbridas, las *fake news*, que han cogido este vuelo, y es algo en lo que estamos trabajando. Estamos organizando boletines de forma semanal sobre ciberterrorismo, ciberyihadismo y también en el ámbito de las *fake news*, tenemos personal dedicado ello, pero nos limitamos a recopilar esa información para que se analice —los analistas están en otro sitio— se haga inteligencia por parte de los órganos competentes que están en las Fuerzas y Cuerpos de Seguridad.

Respecto a la implantación de la Directiva NIS, diré que está avanzada; el propósito es fundamentalmente no llegar a un tipo de doble imposición. Los operadores críticos que tenemos identificados la inmensa mayoría van a ser también operadores de servicios esenciales, tal y como exige la Directiva NIS. Vamos a intentar también hacer una aproximación holística; es decir, no solo a aquellos sectores que la Directiva NIS nos encomienda, sino integrarlos con los doce sectores que tenemos en España, así no dejamos ningún sector fuera. Nos parece algo poco seguro dejar algún sector fuera porque en muchos casos puede tener dependencia sobre otro. Yo confío que en próximas fechas —en los próximos meses o semanas— pueda llegar el texto. Es un texto moderno, donde están integradas las necesidades que tenemos; creo que es de los más avanzados a nivel europeo, por lo que he podido ver, incluyendo el concepto de seguridad integral, cosa que en otros países no se está haciendo, se está haciendo solo ciberseguridad. En este sentido, creo que va a ser un buen texto para empezar a trabajar. Respecto a una comparativa con otros centros, sobre lo que también me han preguntado, creemos

cve: DSCG-12-CM-97

modestamente que no estamos en mal lugar porque el concepto de seguridad integral lo tienen cuatro países: Estados Unidos, Gran Bretaña, Francia y nosotros. Hay otros países muy avanzados que endorsan la protección de las infraestructuras críticas solo al ámbito de la ciberseguridad. En el caso nuestro creo que esto está bien equilibrado. De hecho, es de cierto orgullo para nosotros que sea un modelo que se está siguiendo en Iberoamérica. Nos viene muy bien también a nivel empresa porque muchos operadores críticos españoles también están allí trabajando, con lo cual están aplicando nuestra metodología en estos países en muchos casos.

En cuanto a ciberincidentes, el año pasado llegamos a 885 sobre los sectores que ya vimos anteriormente, sobre todo sistema financiero, energía, transporte y agua. Esto no quiere decir que todos sean incidentes contra infraestructuras críticas, sino contra los operadores críticos, contra sus redes y contra sus sistemas. Afortunadamente, aquellos que pudieran ser problemáticos para la provisión de los servicios esenciales han sido muy escasos y además han sido todos abortados. Pero, como saben, un incidente que ocurra dentro de la red de un operador se puede trasladar desde el mundo IT —tecnología de la información—, que es el más tradicional, al mundo del Internet de las cosas, al OT, que es el que regula las máquinas. Hoy el problema que tenemos aquí, que es lo que estamos trabajando con los operadores, es precisamente que haya un corte o algún tipo de *fairwall* entre el mundo IT y el mundo OT. ¿Por qué? Hace pocos años las máquinas se regulaban de forma analógica; después pasaron a ser reguladas a través de una intranet —Internet todavía no funcionaba suficientemente bien y era todavía cara—, pero cuando Internet funciona con rapidez, con eficiencia y es barata lo que se ha hecho en muchos casos es conectar las redes corporativas —las IT— con las redes de los elementos que regulan la operativa de una empresa, de una organización, sea la que sea. Esto nos proporciona una pasarela que alguien puede atacar; atacando una rede corporativa, se puede meter en la parte industrial de una empresa. Si esta empresa está dando servicios esenciales podemos tener un problema del tipo que relatábamos anteriormente, que nos paren máquinas, lo que significa que nos quedamos sin energía, sin servicios sanitarios o sin agua.

En cuanto a la pregunta sobre cuál era el sector más peligroso, creo que todos tienen su particularidad. Hay algunos, que me voy a reservar, que están más maduros que otros; es decir, son más seguros que otros. Pero les puedo decir, para tranquilizarles, que el nivel de seguridad es alto, con opciones de mejora como siempre. El más peligroso, si no estuviera bien securizado, cosa que no es así, sería el eléctrico y el de las TIC, por razones obvias. Sin energía eléctrica no funciona absolutamente nada. Hay un documental que se llama *American Blackout,* de 2010, de National Geographic, que escenifica un ataque cibernético contra la red eléctrica de Estados Unidos y se ve cómo con esto de las interdependencias día a día van cayendo sistemas y se quedan prácticamente en la edad de piedra. Esto es muy difícil que suceda hoy en día, primero porque las redes están redundadas, después porque es difícil dar con esa tecla y por último porque están bien securizadas, pero potencialmente esa sería la parte más peligrosa, evidentemente. Y las tecnologías, las TIC. Hoy día todo va por tecnología de información y de la comunicación; si nos quedamos sin eso nos quedamos también, por ejemplo, sin el servicio bancario de telepagos. Es decir, está todo imbricado.

En cuanto a la cooperación con empresas, es alta; es mejorable, como todo, pero como ya indiqué es alta y creo que hay una buena predisposición. Fundamentalmente nos falta avanzar en algunas de ellas a nivel gerencial, a nivel directivo, que vean que la seguridad es algo realmente importante para la propia empresa, incluso económicamente hablando. Antes me ha parecido que en su intervención decía que eran intangibles. Bueno, son intangibles hasta que pasan las cosas. El WannaCry les costó 300 millones de euros a tres empresas multinacionales, que prácticamente han tenido que cambiar toda la estructura de seguridad y posiblemente de sus empleados. No prever esto les costó 300 millones de euros. En este sentido, hace falta que la parte directiva vea, se conciencie de que la seguridad es una inversión, no es un gasto, es algo muy manido pero es así.

En cuanto a las actividades de inspección y ejercicios, tengo que decir que nosotros nos basamos mucho en las Fuerzas y Cuerpos de Seguridad del Estado —que son las que están sobre el terreno— para inspeccionar las infraestructuras. En la parte cibernética esa inspección se lleva a cabo en la mayoría de los casos a través del CERT de Seguridad e Industria cuando se trata de operadores críticos del sector privado, y estamos trabajando permanentemente en la realización de ejercicios. Aquí tengo una presentación que hicimos en Sofía hace unos días, y diré que en el tema de ejercicios estamos trabajando tanto en la parte física como en la cibernética. Por ejemplo —está en inglés porque fue una presentación ante la Comisión—, recientemente trabajamos con Red Eléctrica para responder a un cero eléctrico donde nosotros y Red Eléctrica teníamos la labor de coordinación con España, con Portugal y con Francia. Es

cve: DSCG-12-CM-97

un sistema que está interconectado, lógicamente, y el ejercicio escenificó precisamente la caída del sistema eléctrico en España y cómo se reponía tanto en Francia como en Portugal. Nosotros trabajamos de la mano de Red Eléctrica y de las Fuerzas y Cuerpos de Seguridad del Estado para restituir el servicio y para proteger las infraestructuras críticas. Hay un protocolo, una comunicación, donde están las eléctricas españolas y los cuerpos policiales de nuestro país y se está llevando a cabo de forma adecuada. Este tipo de ejercicios los hacemos cada dos años porque si pasa algún día de verdad más vale haber tenido práctica; no es igual la práctica a que quede todo sobre papel.

Ciberseguridad. A los ciberejercicios del año pasado le llamamos CyberEx y participaron 28 empresas españolas de tecnología, de la energía y del transporte. Empezamos con 5 en el año 2013, 9 en 2014, 15 en 2015, 18 en 2016; es decir, vamos creciendo. Y esto es algo que además es interesante porque de alguna forma hay métricas; en este caso se trabajó sobre un ataque persistente. Y también estamos trabajando en ejercicios internacionales, precisamente con la OEA y con los países latinoamericanos. Estamos trabajando bastante en este aspecto, en este caso de la mano del Incibe.

No sé si me he dejado alguna pregunta, presidente.

El señor **PRESIDENTE:** Muchísimas gracias.

Para el segundo turno tienen tres minutos. Señor Salvador.

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

Quiero volver a felicitarle porque nos ha contestado a las preguntas superdetalladamente y añadiendo información. Cuando yo me refería a intangible no me refería a los 300 millones que les cuestan a las empresas que se han visto atacadas, sino a la pérdida de confianza. Si a esas empresas les cuesta 300, pues a lo mejor nos cuesta 3000 o 4000 en la desconfianza en el resto de empresas que no han sido atacadas y que no les ha costado nada, pero que van a sufrir unos efectos. Me refería a ese tema cuando hablaba del intangible.

Si me voy de mi casa, y estoy solo, sé que tengo que mirar si las ventanas están cerradas, si la calefacción está desconectada, si el gas está apagado, y después salgo, cierro la puerta y cojo la llave, como usted ha dicho. Pero eso se nos ha inculcado a todos con muchísimo tiempo y de una manera normal. Digo esto porque a veces parece que la gente es torpe y no se entera de que tiene que aplicar no sé qué protocolo, pero si ahora mismo a todos los que estamos aquí nos hicieran un examen sobre los tres o cuatro pasos que hay que dar vinculados a esto, la gran mayoría de nosotros pondría cosas totalmente diferentes. Por tanto, lo primero que hay que decir es que no hay un protocolo; nadie nos ha contado nada para que sepamos qué protocolo tenemos que aplicar. Lo único que se dice a la gente es que tenga prevención, reservas, cuidado con lo que está utilizando. Por eso, creo que primero hay que avanzar en elaborar esos protocolos para que sean legibles y entendibles para los ciudadanos, como pasó con el Internet para tontos cuando empezó a utilizarse entre personas que no eran población nativa.

El tema de la persecución ya lo comenté una vez, pero lo vuelvo a repetir, no por mí ni por mis compañeros de Comisión sino por el significado que tiene. Porque hablamos de infraestructuras críticas, algo que ya vemos cómo evoluciona, y si hablamos de delitos muy concretos también sabemos cómo se hace la persecución, pero yo me quiero referir al acoso a particulares. Hace tiempo dije que empezaron a circular correos por esta casa contando *fake news* sobre mí: circulaba que me había denunciado una asociación por violencia de género, etcétera. Yo me fui a la policía y les enseñé los correos que estaban mandando y les dije que no existía ninguna asociación, que no había ninguna identificación pero que, aun así, los correos los estaba mandando alguien. Podía tener la sensación de quién podía ser, una persona que ya habría creado problemas de acoso anteriormente y por los que le habrían condenado ya; pero, no había prueba. Vas a la policía, donde te dicen que van a solicitar a los operadores que les den esas direcciones, pero luego entran en contacto con la justicia y la justicia dice: es que, como no hay denuncia, no se puede seguir. Y le dicen a la policía que paren. ¿Cómo va a haber denuncia si lo que me hace falta es saber quién está mandando esto para poder denunciarlo? Si no sé quién lo manda, ¿cómo lo voy a denunciar? Y si no lo sé y no lo puedo denunciar, entonces se para. En este sentido, los ciudadanos tienen mucha desprotección. Yo lo puedo contar aquí y yo no tengo en ese sentido ningún tipo de problema, pero hay gente que sí lo puede tener, que puede encontrarse en situaciones muy delicadas, muy complicadas y sentirse inermes sin saber cómo se pueden defender. Hoy hemos visto que a Donald Trump le han dicho que no puede bloquear a quien le está atacando, a un *trol*. En esto es en lo único que estoy de acuerdo con él, en que lo pudiera hacer, pero una juez dice que no se puede bloquear porque se rompe no sé qué derecho; me imagino que será porque es presidente de Estados Unidos. Hay muchas cosas que arreglar y espero que todos contribuyamos a ello.

cve: DSCG-12-CM-97

El señor **PRESIDENTE:** Muchísimas gracias, señor Salvador.
¿Señor Comorera? **(Denegación).** ¿Señor Hernando? **(Denegación).**
Señora Vázquez.

La señora **VÁZQUEZ BLANCO:** Quiero darle las gracias por todas las respuestas, hacer una consideración y una pregunta. En cuanto a la consideración, quiero decir que lo que estaba contando el señor Salvador es cierto porque más diputadas y yo —sobre todo fueron mujeres— recibimos los e-mails sobre este compañero. **(El señor Salvador García: Pero esos son de nueva generación).** Pues no sé; yo los recibí hace poco y le mostré mi apoyo enseñándole lo que estábamos recibiendo porque no consideraba que un diputado podía tener este tipo de trato, sea del partido que sea; es decir, si los recibiera de otro compañero, también se los haría llegar. Por último, y más que pregunta es una consideración personal, todos los comparecientes hablan del déficit de personal. Yo soy una entusiasta de la ciberreserva; empecé a hablar de la ciberreserva en esta Comisión, de la necesidad de dar oportunidad a gente con talento de ponerse a disposición del Estado en un momento dado y con un criterio concreto; no todos los días sino ante una situación crítica muy importante, y estoy pensando ahora en el caso del Reino Unido, donde cuando los militares profesionalmente cesan los están mandando a una reserva, los están formando y algunos se están integrando en una ciberreserva. Solo era eso.

El señor **PRESIDENTE:** Muchísimas gracias.
Señor Sánchez, ¿alguna consideración sobre las dos consideraciones que acabamos de escuchar?

El señor **DIRECTOR DEL CENTRO NACIONAL DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS, CNPIC** (Sánchez Gómez): Estoy totalmente de acuerdo con esas apreciaciones; además, es cuestión de tiempo. Como ha dicho bien el señor Salvador, estamos en el inicio de una era y no nos está dando tiempo a reaccionar; es una cuestión cultural. Un tema de seguridad muy clásico es el de la seguridad vial; han pasado muchos años para llegar adonde estamos hoy día, que ya todo el mundo se pone el cinturón de seguridad, se tiene otra conciencia sobre beber al volante, etcétera. Al principio los coches circulaban por diferentes sitios, por donde querían, pero luego se empezó a regularizar y ya tenemos conciencia de seguridad, en este caso vial. Esa conciencia no la tenemos en el ámbito de la ciberseguridad, pero yo creo que en ningún país porque no nos ha dado tiempo a implantarla, a construirla. Lógicamente este protocolo de seguridad, que está dentro de una línea de acción concreta, se está empezando a implantar. El Ministerio del Interior —no lo he dicho— está trabajando en la constitución de una mesa de Internet seguro con los grandes operadores de Internet para colaborar en la parte que nos puede competer, pero este es un tema que los nativos digitales, los que ya han nacido con Internet, seguro que lo tendrán mucho más interiorizado que los que no lo somos. En los próximos años esto irá mejorando. El único pero es que todo avanza tan rápido y el impacto puede ser potencialmente tan alto que ese desfase lo queremos cubrir acelerando cosas como la ciberreserva. Tenemos que cubrir los déficits cuanto antes pero porque el mundo avanza muy rápido, no porque no haya propósito ni mentalización en este caso de las instituciones de Gobierno o de las instituciones políticas como esta. Se tienen que implantar medidas, pero vamos siempre mucho más lentos de lo que avanzan los tiempos en este ámbito. Ahí está la disyuntiva; en cualquier caso, vamos en el buen camino.

El señor **PRESIDENTE:** Muchas gracias, señor Sánchez. Ya decía don Hilarión que las ciencias adelantan que es una barbaridad.
Sus señorías tienen que estar de vuelta dentro de un cuarto de hora. **(Pausa).**

— DEL SEÑOR REGO FERNÁNDEZ (SOCIO DE IHACKLABS), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 219/001246 y número de expediente del Senado 715/000514).

El señor **PRESIDENTE:** Señorías, vamos a empezar la última de las comparecencias.
Nos acompaña don Miguel Rego Fernández, a quien doy la bienvenida a esta Comisión y expreso mi agradecimiento en nombre de todos los diputados y diputadas, senadores y senadoras —políticamente correcto todo— por estar aquí. Le doy la palabra.

El señor **REGO FERNÁNDEZ** (Socio de iHackLabs): Muchas gracias, señor presidente. Buenas tardes, señorías.

cve: DSCG-12-CM-97

Permítanme que empiece diciendo que es para mí un motivo de orgullo comparecer hoy ante ustedes e indicarles muy brevemente que soy un servidor público, no solamente vocacional sino *de facto.* Soy teniente coronel de la Armada Española y he prestado servicios en la Armada; es mi formación base y oficial de la Armada lo seguiré siendo toda la vida. Por circunstancias, tuve la oportunidad de complementar mi experiencia profesional pasando al sector privado, en el que he tenido la ocasión de trabajar en ciberseguridad en cliente final, para la compañía de telecomunicaciones ONO y para dos grandes consultoras, Deloitte y Ernst&Young. Asimismo, he tenido el privilegio de dirigir el Instituto Nacional de Ciberseguridad entre los años 2013 y 2016, cuando el Gobierno decidió impulsar las acciones en el campo de la ciberseguridad. Soy colaborador habitual de la Organización de Estados americanos en el desarrollo de políticas de ciberseguridad en las Américas. Y, como no tengo aversión al riesgo, recientemente he fundado una *startup* para completar el círculo, y espero que esa iniciativa salga bien, ¿quién sabe?

Comenzaré trasladándoles nuestra visión de los riesgos del ciberespacio, con la idea fundamental de que ustedes entiendan que el ecosistema de riesgos es absolutamente dinámico, cambiante y complejo. Por lo tanto, iniciativas estáticas que no sean capaces de adaptarse a esta mutabilidad que tiene la amenaza no son de valor en este momento. Esta complejidad se acrecienta con el hecho de que cada vez somos más digitales y aumenta por lo tanto la superficie de ataque, y la tendencia es que la economía, la industria e incluso nuestra manera de comunicarnos y de relacionarnos sea cada vez más digital. Esta situación, en mi modesta opinión, ha venido para quedarse. Si me permiten, quedémonos con dos fotos: la primera, que necesitamos un entrenamiento o capacitación continua para que nuestros profesionales sean capaces de adaptarse a esta situación cambiante; la segunda, que la manera de gestionar los riesgos tiene que ser también mutable y adaptable a la situación del ecosistema de amenazas.

Yo les voy a hablar hoy de dos aspectos en los que me temo que parcialmente puedo coincidir con mi colega y amigo Pedro Pablo Pérez, de Telefónica. Quiero resaltar la importancia que tiene para cualquier país desarrollar políticas públicas y capacidades que tengan como objetivo la generación del talento profesional en ciberseguridad y el desarrollo de un ecosistema de empresas de ciberseguridad, pero antes permítanme que centre la discusión en las capacidades y los modelos públicos de ciberseguridad. **(Continúa su intervención apoyándose en un** *powerpoint).*

Como pueden ver ustedes en la presentación, el primer paso —que es el que ha adoptado España— consiste en desarrollar una estrategia nacional de ciberseguridad o, como lo llaman en algunos países de Latinoamérica, una política de seguridad cibernética. En la mayoría de los casos podríamos decir que es un libro blanco en el que se definen objetivos y también se apuntan algunas líneas de acción que luego, en todo caso, se tienen que desarrollar con capacidades concretas y específicas, tal y como les propongo en el mapa que tienen a la derecha de esta *slide*.

En este punto debo decirles que España ha sido un país que ha venido trabajando su estrategia de ciberseguridad nacional, que se aprobó en 2013 como ustedes conocen bien y que ahora mismo se encuentra en proceso de revisión, pero permítanme que comparta en esta experiencia pública que les he presentado la importancia de que cualquier estrategia vaya acompañada de una memoria económica; si no, vamos a quedarnos en el plano de las buenas intenciones, vamos a quedarnos en el plano de un libro blanco. Permítanme que ponga como ejemplo experiencias del mundo anglosajón, como la estrategia de ciberseguridad de Reino Unido, con el que nos une un panorama geoestratégico de amenazas común y del que quizá nos separen algunos ceros en cuanto a inversión en ciberseguridad. En todo caso, es un ejercicio muy importante. Cualquier estrategia tiene que venir acompañada de una estimación y de una planificación económica.

Como pueden ver ustedes, el desarrollo de cualquier modelo de capacidades en ciberseguridad consta de los aspectos que he incluido y tratado de resumir en esta *slide*. Hay que desarrollar mecanismos de ciberdefensa para proteger los intereses nacionales en el ciberespacio. Hay que desarrollar capacidades de una manera holística en la lucha contra el cibercrimen, no solamente cubriendo las necesidades que puedan tener nuestras Fuerzas y Cuerpos de Seguridad del Estado, sino complementándolo con una especialización concreta en la fiscalía y en la judicatura. Es importante también desarrollar planes y capacidades para la protección de toda la cadena de valor, desde el ciudadano, desde el sector privado. Son muy importantes también las infraestructuras críticas, y permítanme que les recuerde, señorías, que el 80 % de esas infraestructuras críticas están en manos del sector privado. Quisiera resaltar la importancia, al desarrollar un modelo de este tipo, de la colaboración público-privada y de desarrollar mecanismos de coordinación con el sector privado. Por último, es

cve: DSCG-12-CM-97

importante la protección de las infraestructuras de telecomunicaciones y los sistemas de información del Gobierno y de las instituciones públicas.

Me he permitido destacarles el objeto de esta comparecencia, que son los aspectos relacionados con el talento y el emprendimiento, donde pretendo llamar su atención sobre algunos aspectos por los cuales es importante tener en cuenta estos elementos. Permítanme también —he sido un poco osado— que les haga algunas recomendaciones para poder impulsarlo.

A riesgo de repetirme con la exposición que ha hecho mi colega, Pedro Pablo Pérez, les diría, empezando por el mercado de la ciberseguridad, que es un mercado profesional, absolutamente en alza, pero que tiene un programa importante en cuanto a que las oportunidades profesionales no se cubren ni se van a cubrir en los próximos años. Los motivos de esta mayor demanda de profesionales básicamente son: por un lado, que somos más digitales, y a más digitalización, más ciberseguridad y, por tanto, más demanda de profesionales; por otro lado, que partimos de un nivel de madurez bajo y de un nivel de concienciación bajo que progresivamente va mejorando. Si nos atenemos a las cifras globales, probablemente ustedes ya saben que en este momento hay un desfase entre oferta y demanda y que estamos hablando, por centrarnos en lo que nos es más cercano, de que en Europa en 2022 habrá un 'agujero de ozono' —si me permiten la expresión— entre oferta y demanda de 350 000 profesionales. Eso quiere decir que se va a necesitar cubrir 350 000 posiciones y no se va a poder hacer, salvo que hagamos determinadas cosas. Si no me equivoco, teniendo en cuenta que somos en torno a 511 millones de habitantes en la Unión Europea y que España ocupa el 9 %, en 2022 tendremos aproximadamente 30 000 posiciones sin cubrir. Creo que es algo suficientemente importante como para que empecemos a trabajar en ello.

¿Por qué tenemos que impulsar desde las instituciones públicas el desarrollo profesional en materia de ciberseguridad? Permítanme que comparta cinco reflexiones, aunque probablemente hay muchas más. La primera y más obvia es que faltan especialistas en ciberseguridad en valor absoluto. La segunda —y es importante resaltarlo— es que son puestos críticos —y repito bien, críticos— para nuestras Fuerzas Armadas, para las Fuerzas y Cuerpos de Seguridad del Estado y para los operadores de infraestructura crítica. Por lo tanto, la seguridad nacional en el ámbito del ciberespacio se puede ver debilitada precisamente por esa falta de talento. La tercera es que este es un mercado profesional en crecimiento continuo de salarios y con alta rotación. Eso, para los que nos dedicamos en nuestro día a día a la ciberseguridad, a día de hoy es un problema. Nos faltan profesionales, tenemos que pagarles mucho más —creo que Pedro Pablo Pérez ha hablado de salarios—, pero no es una burbuja, es decir, no es algo que en un momento determinado vaya a estallar, sino que lo que hay que hacer es incidir sobre el mercado para que se normalice y no siga creciendo de esa forma diríamos no controlada. La cuarta es que, en un país que tiene un problema estructural en cuanto al paro juvenil, la tasa de desempleo en este sector es cero. Por lo tanto, hay una enorme oportunidad para un país de servicios, como somos nosotros. Dirán ustedes que esto es un tópico, pero es cierto —y yo personal y humildemente lo he podido compartir— que hay talento para la ciberseguridad en los jóvenes españoles. Lo puedo acreditar porque he podido vivirlo de primera mano cuando estuve a cargo del Instituto Nacional de Ciberseguridad. La quinta, y también muy importante, es que no se trata solamente de cubrir las necesidades que tenga España, es que la demanda es global. Por lo tanto, tenemos la posibilidad de generar oportunidades para nuestros jóvenes, no solamente para que cubran nuestras necesidades, sino para que puedan proyectarse de forma internacional mejorando el posicionamiento de España, generando marca y una capacidad complementaria de influencia.

Entro ahora en algunas medidas para desarrollar e impulsar el mercado de profesionales. En primer lugar, es muy importante determinar específicamente cuáles son las necesidades profesionales del sector privado y del sector público. Ahora mismo es un aspecto que no tiene mucha madurez, en el sentido de que no llevamos muchos años hablando de ciberseguridad y planteándonos este problema. Por lo tanto, es necesario poner negro sobre blanco, estructurar muy bien cuáles son los perfiles profesionales, cuales son los *hard* y los *soft skills* necesarios, pero también debo decirles que ya hay materia avanzada y que organismos como el Instituto de estandarización del Gobierno federal de los Estados Unidos, el NIST, ya han hecho algún trabajo. No quiero decir que lo que hayan hecho en Estados Unidos sea de aplicación inmediata en España, pero es una buena referencia. El Reino Unido también ha hecho algún trabajo en ese sentido. Por tanto, sería más bien una labor prospectiva de analizar lo que se ha hecho y tratar de adaptarlo a la realidad nacional.

También es importante definir un catálogo de roles profesionales ligado al aspecto anterior, inventariando perfectamente las capacidades y las competencias. Es importante también alinear el

cve: DSCG-12-CM-97

esfuerzo que están haciendo las universidades con la demanda. En el ámbito de la ciberseguridad se ve un *gap* entre la oferta universitaria, la formación reglada, y lo que luego necesitamos las empresas. En los másteres privados y en los másteres profesionales se forman especialistas en ciberseguridad, pero no es eso lo que necesitan las empresas en la mayoría de los casos. Permítanme que les comente que, como en cualquier carrera profesional, tenemos que empezar trabajando desde la base de la pirámide. Hay todo un desarrollo profesional en el campo de la ciberseguridad hasta llegar a puestos de dirección, pero hay que empezar con una hiperespecialización en la base, con perfiles muy concretos, que son precisamente los que no se encuentran.

Desde mi modesta experiencia, también comparto con ustedes que la generación de talento en ciberseguridad, como en cualquier otro ámbito, es un ciclo de vida que empieza en el colegio. Mi experiencia en el Incibe es que empezábamos a detectar potenciales talentos desde los doce años, y lo hacíamos a través de una iniciativa que se llamaba Cyber Olimpics, que eran unos concursos entre colegios en los que, simplemente dando como premio material de electrónica, los colegios se animaban y los chicos competían y se veía que había un talento grandísimo. Es importante promover ese tipo de iniciativas. Además, de manera paralela a la generación de una cultura de ciberseguridad nacional, como establece nuestra estrategia, es importante que haya eventos, algunos de ellos organizados por organismos públicos, precisamente para promover concursos, competiciones, talleres para jóvenes alrededor de la ciberseguridad y las oportunidades profesionales que trae.

En lo relativo al emprendimiento y al mercado de productos de ciberseguridad, tengo que decirles que esta es una carrera en la que los buenos perdemos. La innovación en el campo de los malos es continua. Es lo que yo les he comentado sobre la mutabilidad de la amenaza. Se desarrollan nuevas técnicas de ataque. Ahora se habla más de la amenaza híbrida, utilizando temas de posverdad y redes sociales. El ingenio de los malos es increíble. La única manera de cubrir de alguna forma esa ventaja competitiva, si me permiten, que tienen los malos es con la innovación, con la generación de productos y servicios, con la investigación técnico-científica en materia de ciberseguridad. Hay un mercado muy interesante también alrededor de ello. Comparto con ustedes algunos datos que demuestran que hay un crecimiento interanual del mercado de entre el 14 % y el 20 %. No traigo datos de operaciones de *mergers and acquisitions,* de inversiones, pero les comento algunas fuentes muy interesantes, como pueden ser estos analistas de Silicon Valley, que se llaman Momentum Partners y que realizan un informe anual que caracteriza el mercado de la ciberseguridad alrededor de Silicon Valley, que es un mercado al final muy representativo; no es el todo, pero es muy importante.

Permítanme, señorías, que les señale que se queden con el crecimiento que hay en Latinoamérica. Uno de los aspectos que quiero resaltar es la oportunidad real que tienen las empresas españolas de tecnología de copar un mercado que es naturalmente nuestro y al que ahora, por alguna circunstancia, no estamos llegando. Se lo digo por mi experiencia personal en estos últimos meses de *startup* y porque realmente, cuando interactúas con el mercado latinoamericano, ellos te lo piden. Hay una barrera idiomática con Estados Unidos y hay una cierta desconfianza, pero hay una mayor aproximación natural, como ellos dicen, hacia la madre patria; esto es un tópico, pero es verdad, y cuando uno va por allí ve que es cierto. Por tanto, para nosotros es un mercado natural y, como saben ustedes, con unos indicadores de crecimiento económico muy interesantes; son mercados que están creciendo.

Algunas razones para impulsar el mercado del desarrollo del emprendimiento. Les comentaba la complejidad y la mutabilidad de las ciberamenazas, la obviedad de la penetración digital creciente, la realidad de la economía y de la industria que son digitales; necesitamos reducir la dependencia exterior de productos clave de nuestra seguridad —no quiero decir eliminarla pero, en la medida de lo posible, tratar de reducir esa dependencia exterior que en este momento la centraría en Israel y en Estados Unidos fundamentalmente—; es un mercado en crecimiento continuo; hay oportunidades —volvemos al mismo punto que en el caso del talento— para el desarrollo y el crecimiento profesional de los jóvenes; y, como les decía, señorías, hay mercados de alta permeabilidad a la tecnología española, superreceptivos a la tecnología española.

Termino. Me permito hacer una serie de recomendaciones para impulsar el desarrollo del emprendimiento. En primer lugar —y muy importante—, identificar la demanda sofisticada. La demanda sofisticada es aquella que va un poquito más por delante del resto del mercado y la componen, fundamentalmente, nuestras Fuerzas y Cuerpos de Seguridad del Estado, la defensa, el sector financiero y, probablemente, la energía. Van un poquito por encima en cuanto a necesidades, su nivel de digitalización también es muy alto y la identificación de esas necesidades, normalmente no cubiertas, puede ser un

cve: DSCG-12-CM-97

impulsor claro para la investigación y para la transferencia finalmente a la industria. Sobre la base de esa determinación de necesidades, mi recomendación es crear un plan de investigación para evitar solapamientos entre las actividades que realizan los centros de investigación y las universidades españolas, y —permítanme que les diga— tratando de poner algo de practicidad en la investigación. Tenemos auténticos expertos en criptografía cuántica en España, pero eso se traduce al final en unos *paper* magníficos. Hay que orientar la investigación, en mi opinión, a que tenga resultados concretos que atiendan necesidades concretas y que eso tenga una transferencia a la industria, porque tenemos que acordarnos de la «i» final, que es muy importante. Luego está fomentar la cultura de emprendimiento de los jóvenes. Con todos mis respetos —y soy funcionario— los jóvenes no pueden tener como aspiración ser funcionarios o nada más. Sí, sí, tienen vocación, pero no como una solución profesional; se lo digo con todos mis respetos y desde el hecho de que yo con dieciocho años estudié para entrar en la Escuela Naval Militar, aunque por otros motivos. La cultura del emprendimiento es algo que hay que fomentar, que no tienen los jóvenes españoles y que es una salida importante, como ven ustedes, y mueve la economía española.

Hay que promover programas específicos para la implantación de programas de incubación y aceleración de las *startups*. Ustedes conocen perfectamente el famoso valle de la muerte que estoy pasando ahora y que espero que finalice el 31 de diciembre de este año, en el que siempre hay una incertidumbre. En ese momento es cuando más se requiere financiación pública y contar con ciertas capacidades que permitan la sostenibilidad en un momento complicado, en el que uno está generando mercado, está desarrollando oportunidades. Es muy importante. Si la ciberseguridad es una cuestión de importancia nacional, apoyemos la generación de la industria nacional con ciertos instrumentos públicos.

Finalmente, igual que decía en el caso del talento, es importante generar espacios de encuentro entre emprendedores y mecanismos privados de inversión. Es un momento interesante en el que hay mucho interés en colocar dinero de inversores privados en aspectos relacionados con la ciberseguridad, en productos y servicios. También hay que fomentar la creatividad de los jóvenes promoviendo concursos de ideas donde puedan realmente presentar prototipos de proyectos que luego puedan dar o no —depende de muchas circunstancias— soluciones a problemas planteados.

Señorías, con esto finalizo mi comparecencia. Como les comentaba al principio, mi objetivo es que sus señorías se queden con la idea de cuán importantes son la generación de talento y el emprendimiento, y yo lo apuntaría desde dos perspectivas: no solamente como una herramienta para un mejor control de los riesgos del ciberespacio, sino también —y muy importante— como una magnífica oportunidad para los jóvenes y para España como país en su posicionamiento geoestratégico.

Muchas gracias, señor presidente. **(Aplausos).**

El señor **PRESIDENTE:** Muchísimas gracias, señor Rego. La verdad es que me parece extraordinariamente útil su exposición y hay una serie de conclusiones que probablemente nos sean de una enorme utilidad a la hora de hacer nuestras propias conclusiones parlamentarias, por lo cual le estoy doblemente agradecido.

Empezamos este turno con el señor Salvador.

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

Me ha gustado bastante su intervención y quiero felicitarle y darle las gracias por venir a comparecer. Me ha gustado mucho porque los comparecientes vienen y explican, como es lógico, la necesidad de crear una cultura de todo esto, de intentar divulgarlo y de que todo el mundo comprenda qué sucede, qué hay que hacer y por dónde podríamos ir, pero pocos entran en la especialización en temas concretos, y usted ha cogido un carril y, aparte de ponernos un marco general, se ha metido en algo que estamos detallando en todas las comparecencias que es muy importante, que es la captación de talento y el aprovechamiento de esas oportunidades.

Tomando notas al leer su propia intervención, creo que también es gráfico para demostrar cómo está realmente esto. Hay una cuestión clara: necesitamos profesionales y necesitamos todo; necesitamos decirle al país que esto es muy importante, que hay que darle la financiación adecuada, que la seguridad digital es tan importante como el resto de la seguridad y que es un igual —lo que se ha planteado anteriormente—_. A partir de ahí, tenemos que hacer muchas cosas que no nos ha hado tiempo a hacer hasta ahora y que además corren prisa porque los riesgos están ahí y, como usted ha dicho también, la innovación de los malos es permanente, porque ese es su negocio. Usted ha detallado la importancia del mercado, la importancia de los sueldos —como se ha dicho antes también—, el paro cero, etcétera, y ha hablado de determinar la necesidad de profesionales, requisitos de conocimiento y especialización. Es un

cve: DSCG-12-CM-97

reconocimiento de que no está determinado. Estamos en el discurso de que necesitamos más profesionales, pero luego habla de definir un catálogo de roles profesionales y competencias que se adapten mejor. Completamente de acuerdo, pero se supone que ya podíamos tener eso y saber qué es lo que estamos buscando. Cuando dice desarrollar nuevos programas y adaptarlos a las necesidades del mercado laboral, tres cuartos de lo mismo. Que sepamos que hace falta captar talento y que es una oportunidad y que es un sector que va tener una alta capacitación, etcétera, todo eso ya lo sabemos, pero es verdad que corresponde a la Administración y a quien tenga que estar encargado de ello empezar a avanzar rápidamente. Esperemos que esta ponencia sirva también para ello.

Otro elemento fundamental, el tema de la cultura. Usted hablaba de promover en colegios, organizar eventos, asociaciones, reuniones... Es el reconocimiento tácito de la realidad, que es que no existe esa cultura, pero tenemos que empezar por ella y empezar ya. Es absolutamente determinante. Hablaba también del tema de la financiación en un momento determinado y venía a decir que se necesitaba una financiación específica. El compareciente anterior también ha reconocido que la estrategia de seguridad nacional no tiene esa financiación específica. Sin embargo, se hace en base al presupuesto del los departamentos acometiendo las tareas que les encarga la estrategia. Lo normal sería al revés. Nos ha contado el caso del Reino Unido, donde existe un presupuesto para esa estrategia y luego ya se desarrolla donde se tenga que desarrollar y se lleva el dinero en los años que haga falta. Nos hace falta todo.

Quería decirle que tomamos buena nota. Yo creo que el presidente estará contento porque hemos cogido un montón de aportaciones muy importantes para la ponencia. Yo le querría animar, ya que ha cogido este carril, a que usted mismo ayude a determinar esas cosas que decía. El primero que lo defina bien al final estará poniendo parte de la solución, en vez de estar todos reflexionando todo el día sobre lo que hace falta, pero es necesario que alguien se siente y lo ponga sobre la mesa. ¿Considera que la formación continua de los profesionales que están actualmente en el sector de la ciberseguridad es la adecuada? Lo digo porque si estamos hablando de que no se ha definido, aunque se sepa *grosso modo*, cuál debe ser exactamente esa formación, qué grado de especialización, qué tipo de funciones y qué roles tienen que desempeñar los profesionales que estamos captando, que vienen de telecomunicaciones, de ingeniería informática o de donde vengan, ¿hay un plan para que hagan bien su trabajo y una formación continua para saber cómo evolucionan según las amenazas? ¿O eso también implica una pérdida de talento importante en la gestión del mismo? ¿Qué opina de la inversión en innovación, en I+D+i en su conjunto? ¿Es un inversión adecuada? ¿Es una inversión que se adapta a la evolución tecnológica? La tecnología avanza con rapidez pero, ¿cree que está habiendo una renovación y una adaptación a esos retos o no existe? A partir de ahí, repito, solo quiero felicitarle porque ha bajado a un grado de especialización que yo creo que nos va a ayudar mucho en esta Comisión.

Muchas gracias.

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

Tiene la palabra la senadora Angustia Gómez.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.

Muchas gracias por su exposición, señor Rego. Le agradezco que también nos la haya dejado para que podamos repasarla después. Muchas de las cosas sobre las que yo quería profundizar ya han salido, sobre todo el tema de la educación y de la formación reglada, que yo además varias veces he defendido en esta Comisión. Creo que ya se conoce muy bien nuestra postura al respecto, por tanto, no voy a profundizar ahí. Como usted sí tiene un programa específico de talento y capacitación, nos gustaría que nos contara un poco más cómo se desarrollan esos programas y sobre todo, con esa visión global que tiene de la integración de la formación privada y de cómo debería adaptarse la formación reglada, cuál es el enfoque que le dan —entiendo— bajo esta perspectiva para que, llegado el momento de que las políticas integrales públicas decidan abordarlo, se puedan integrar entre sí. Me gustaría que profundizase en eso mucho más.

También gustaría saber cómo relacionan este proyecto específico de ciberseguridad nacional con esos espacios públicos. Como trabaja en un campo más o menos desconocido para el trabajo que hasta este momento estamos desarrollando en la ponencia de ciberseguridad, que es específicamente la ciberseguridad industrial, que yo creo que tiene componentes totalmente diferentes al marco global desde el que estamos habituados a ver la perspectiva, y sobre todo por tener un componente privado mucho más

cve: DSCG-12-CM-97

alto que otros espacios -yo creo que tiene necesidades especiales-, nos gustaría saber cómo desde la empresa los trabajan y qué colaboración cree usted que desde el campo de actuaciones y desde el campo formativo se deben abordar conjuntamente para mejorar el espacio.

Termino queriendo conocer su opinión, después de haber trabajado en el sector público y ahora hacerlo desde el sector privado. Creo que es interesante esa perspectiva global, que se debe ver de forma diferente desde los dos al respecto de la formación de la ciudadanía. Siempre es el espacio en el que más se desconoce la ciberseguridad o en concreto todo el campo de la seguridad. Por tanto, quisiéramos conocer cómo cree que hemos avanzado, en qué punto se está de conocimiento desde su experiencia en el Incibe y desde su conocimiento ahora en iHackLabs o en Ono o en las empresas privadas en las que ha colaborado y ha participado, para saber cómo continuar a partir de aquí porque también es uno de los puntos específicos que queremos mejorar.

Muchas gracias.

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

Senador Raffo.

El señor **RAFFO CAMARILLO:** Gracias, presidente.

Me sumo al agradecimiento que el propio presidente ha trasladado al compareciente en la Comisión que tenemos que desarrollar aquí, que yo creo que reúne unas condiciones especiales, porque respecto a toda la tanda de comparecientes que llevamos tenemos a alguien que conoce tanto el sector público como el sector privado. Eso se nota en la propia exposición, cómo tiene identificadas las prioridades y las debilidades que existen con idea de convertirlas en puntos de mejora para actuar de cara al futuro. Yo quería aprovechar esas condiciones y esas características del compareciente de hoy porque -él mismo lo planteado en una de las diapositivas- nos enfrentamos a un problema complejo en un contexto complejo y cambiante. Esto define en realidad bastante bien el problema al que nos tenemos que enfrentar. Precisamente por eso, como estamos en una institución pública y teniendo en cuenta esas características del problema al que nos enfrentamos, en un contexto complejo y ante un problema complejo y cambiante, existe la necesidad del diseño de una política pública que es la que corresponde a las administraciones públicas, al Gobierno y a las instituciones que tienen que legislar, como es el caso de los que estamos aquí presentes en una Comisión mixta. Por resumir mucho, con idea de facilitar la respuesta, diré que como cualquier política pública tiene que tener un apartado de cómo recaba información para aproximarse a la realidad de un problema, cuál es la debilidad en el sentido de dónde están agrupados los datos y las fuentes de datos que nos hacen falta para tomar decisiones y si hay una debilidad en este sentido que nos plantee cuál sería el punto de mejora.

En segundo lugar, como cualquier organización, igual que el sector privado, la Administración pública, los poderes del Estado, de las administraciones autonómicas, etcétera, necesitan tener un instrumento de planificación, que en este caso sería una planificación estratégica que de hecho la tenemos a nivel nacional con la estrategia que existe en este ámbito y en el ámbito de la seguridad nacional en general. Querríamos saber si identifica alguna debilidad en los procesos de planificación que se han ido llevando hasta ahora con idea de convertirlos en puntos de mejora, teniendo conciencia de que esta planificación no es una planificación a cuatro, seis o diez años, en la que se diagnostica y a los seis años o por lo menos a los dos o tres años se hace una evaluación, sino que es permanente el seguimiento y la monitorización en este tipo de planificación. Nos gustaría que nos pudiera facilitar, a partir del conocimiento fruto de su experiencia, al hilo de los distintos ámbitos donde ha estado, los puntos débiles que podríamos mejorar de cara al futuro.

Hay otro apartado, que es el de la regulación, que es propio también de las instituciones públicas. En cuanto a las normas y a las leyes si haría falta dotarnos, aparte del reglamento que a partir de mañana ya está en funcionamiento, de algún otro punto de mejora que usted identifique. Después hay un apartado que, independientemente de qué es lo que exige un modelo de planificación estratégica, cualquier modelo de planificación actual y moderno exige, que es el asunto relacionado con las alianzas entre los distintos actores o agentes que intervienen en enfrentar un problema o una situación determinada. La pregunta es si en esta alianza en colaboración con la cooperación, pero que prefiero denominar alianza porque va muchísimo más allá, en lo que corresponde a los departamentos de la Administración pública y a las distintas administraciones públicas hay algún punto de mejora que nos podría trasladar.

Finalmente, quiero plantear las tres formas de abordaje para enfrentamos a un problema que causa daño: una, la prevención, y no hacer otra cosa; dos, la protección y la intervención para recuperar o

cve: DSCG-12-CM-97

rehabilitar ese sistema, que sería una parte y, tres, hacer las dos cosas, proteger el sistema cibernético y el ciberespacio de nuestro país. También me gustaría saber si en estos métodos de abordaje esa parte de promoción o de prevención la estamos cumpliendo de forma debida o hay algún punto crítico.

Muchas gracias.

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

Diputada Vázquez.

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

Quiero darle las gracias a don Miguel Rego, que nos ha hecho una exposición, creo que hasta el momento de las más precisas y concretas, desde el punto de vista de su experiencia, ya que ha pasado por el ámbito público y ahora está en el privado. Cuando solicitamos la comparecencia creíamos que era la persona más adecuada —y me alegro que hoy a todos los grupos les guste— porque sabíamos que lo que aportase iba a ser muy importante e interesante de cara a las conclusiones últimas que se emitan por parte de la Comisión de Seguridad Nacional.

Sí quería hacer, antes de nada, una precisión porque hay mucha gente que nos está viendo por televisión; quería tomar el testigo, porque me van escribiendo en las redes, y me dicen: Ana sí que hay talento, pero no sabemos canalizarlo. Mi primera consideración es que hay gente dispuesta y con talento y me gustaría saber qué valoración o qué opinión le merece que el Estado pudiera canalizar, en según qué situaciones, una ciberreserva. En estos momentos estoy pensando en esta gente que está pendiente de nuestras comparecencias, que quieren hacer algo más por el Estado, que quieren ayudar algo más, aportar al Estado español lo que ellos sí conocen, saben y pueden hacer de manera voluntaria.

Dicho esto, me gustaría hacerle una serie de preguntas. Usted estuvo en el Incibe; mejor que nadie puede decirnos, al igual que aquí ha hecho una crítica constructiva al decir que la estrategia nacional de ciberseguridad debe de llevar memoria económica —como también dijo el anterior compareciente—, qué aspectos del Incibe considera que deberíamos tomar en consideración para poder reformar o si está todo perfecto y no debemos hacer ninguna modificación. Otra de las cosas que me gustaría saber, desde su punto de vista profesional en ambos lados, público y privado, cómo es la cooperación. En varias ponencias se ha puesto sobre la mesa la crítica a las empresas privadas por la falta de rigurosidad en comunicar los ciberincidentes o el retraso en comunicarlos, muchas veces por cuestiones de reputación y otras por cuestiones económicas o de otra índole, no tanto a lo mejor por los profesionales que se dedican a la ciberseguridad en esas empresas sino por los directivos de esas empresas. ¿Qué mecanismos se podrían aplicar para que esas comunicaciones fueran más fructíferas?

Hablaba usted, y ya lo han dicho también más comparecientes, de la formación. Yo estoy de acuerdo en que hay que reformar, pero unos nos dicen, másters; otros, carreras; otros, el modelo francés, desde educación primaria. ¿Qué modelo podemos hacer? Usted dijo: másters privados, no. De acuerdo. ¿Qué modelo? Cuando hagamos las conclusiones tenemos que escribir algo más, y esto empata con la pregunta que ha hecho mi compañera del Grupo Podemos.

En cuanto a la concienciación, efectivamente, si ahora nos pregunta a nosotros posiblemente seamos los peores porque estamos conectados a la red wifi del Congreso, que varias veces ya ha tenido problemas; los primeros imprudentes somos nosotros. ¿Cómo podemos nosotros, o el Estado, concienciar a la sociedad? El anterior compareciente ponía sobre la mesa las campañas de seguridad vial. Ahora todos nos ponemos el cinturón, dejamos de beber, etcétera. ¿Qué podemos hacer para hablar de la ciberseguridad? Porque hasta que no te pasa no eres consciente del problema y de la gravedad que tiene. Hace quince o veinte años el problema era recibir un *email* que traía un virus, pero ahora estamos hablando de que hay más de 8400 millones de dispositivos conectados a Internet. Y no solo eso, las propias empresas, con los daños económicos que ello supone.

Nada más. Darle las gracias. No tengo más preguntas porque me las han copado entre ellos. **(Risas).** Como decía el señor Cosidó, esto de ser el último en intervenir te da la suerte de que somos el grupo mayoritario en las Cortes Generales, aunque también te deja un poco en evidencia respecto a las preguntas. Pero me alegro de coincidir con ellos, es de las pocas veces en las que coincidimos, aunque en la Comisión de Seguridad Nacional es muy habitual.

Muchas gracias.

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

cve: DSCG-12-CM-97

Vamos a lograr el milagro de llegar a un consenso, no solo en las conclusiones sino en las preguntas, lo cual facilita mucho las cosas.

El señor **REGO FERNÁNDEZ** (Socio de iHackLabs)**:** Gracias, señor presidente. Quería hacerle una pregunta en relación con la intervención, si se puede ver fuera de esta sala.

La señora **VÁZQUEZ BLANCO:** Se está viendo.

El señor **REGO FERNÁNDEZ** (Socio de iHackLabs)**:** ¿Es pública?

El señor **PRESIDENTE:** Al parecer, la senadora dice que somos estrellas televisivas en este momento.

El señor **SALVADOR ARMENDÁRIZ:** Se retransmite en directo.

La señora **VÁZQUEZ BLANCO:** No, señor presidente, está en directo y sí, es verdad, que tengo colaboradores —alguno conocido también por usted— y las estaban viendo.

El señor **PRESIDENTE:** Siento que no le hayamos advertido, pero no ha cometido usted ninguna…

El señor **REGO FERNÁNDEZ** (Socio de iHackLabS)**:** Ahora, a la hora de responder a estas preguntas tengo en cuenta esas circunstancias. En todo caso, quedo a disposición de sus señorías.

El señor **PRESIDENTE:** Siento no haberle advertido que esto era así. Esta institución tiene luz y taquígrafos y ahora ya las nuevas tecnologías.

El señor **REGO FERNÁNDEZ** (Socio de iHackLabs)**:** En todo caso, quedo a la disposición de sus señorías. Trataré de ser preciso en la respuesta a las preguntas. Pero, les pido a sus señorías que me precisen si al final la respuesta…

El señor **PRESIDENTE:** Hay un segundo turno.

El señor **REGO FERNÁNDEZ** (Socio de iHackLabs)**:** Perfecto.

Muchos de ustedes han coincidido en la importancia de la formación continuada, la capacitación, en cómo abordarlo, cómo hacerlo. Creo que como cualquier otro aspecto pasa por una definición clara de los objetivos. Es decir, en muchas circunstancias tratamos de dar una respuesta, si me permiten, poco estructurada al no tener claros cuáles son los objetivos finales y yo he intentado apuntar en mi intervención la importancia de definir claramente cuáles son esos objetivos para que luego la formación, ya sea reglada o no reglada, ya sea basada en programas universitarios o motivada por iniciativas privadas —léanse certificaciones nacionales e internacionales— puedan dar respuesta. Pero creo que aquí lo fundamental es tener perfectamente definidos cuáles son esos perfiles profesionales y cuales son los *hard* y los *softskill* necesarios para poderlos alcanzar. Y al final, teniendo claro ese modelo, si podemos —y con ello hablo de las universidades, de los centros de educación— orientar nuestra formación a dar respuesta a esas necesidades. Por lo tanto, creo que ese es el elemento fundamental que he tratado de destacar.

En cuanto a la inversión, España invierte públicamente en el desarrollo, en el I+D en tecnología. Yo sí que creo, y se hizo algún intento en mi etapa en el Instituto Nacional de Ciberseguridad, pilotado y coordinado desde la Secretaría de Estado y con el apoyo de Red.es, para crear un fondo específico; creo que es fundamental crear un fondo específico de apoyo a la inversión en ciberseguridad. Porque, y esa es la realidad, al final la ciberseguridad es un elemento todavía porcentualmente muy pequeño en lo que es el océano de la inversión en tecnología. Por lo tanto, si está metido dentro de ese todo se diluye considerablemente a la hora de poder desarrollarse, adquirir fondos y potenciar iniciativas. Porque es una parte todavía pequeña muy importante de lo que sería el esfuerzo en I+D+i en el ámbito general de las tecnologías de la información. Luego mi recomendación sería trabajar para conseguir el diseño de una serie de instrumentos públicos de apoyo al emprendimiento, pero específicamente centrados en la ciberseguridad.

Hay una pregunta centrada en los programas de capacitación, quizá en el segundo turno podamos profundizar más, pero mi aproximación sigue siendo la misma, si me permiten, que es empezar el edificio por los cimientos y por definir perfectamente los perfiles y las capacidades necesarias.

Los programas de formación existentes. Hay una cuestión interesante que se está imponiendo poco a poco y permítanme que ponga el símil de las Fuerzas Armadas, y es que los militares nos formamos pero

cve: DSCG-12-CM-97

luego estamos permanentemente capacitándonos. Es un símil muy interesante porque para ingresar en el Ejército o en las Fuerzas Armadas se necesita una formación previa; durante el tiempo en la academia militar te formas, posteriormente también te especializas pero durante todo tu ciclo de vida te estás permanentemente capacitando y entrenando, y quiero ponerles ese símil porque precisamente es debido a esa mutabilidad, al carácter cambiante que tiene la amenaza y lo que hay que proteger por lo que yo trataría de replicar estos escenarios de capacitación y entrenamiento continuo. Entonces, ¿cómo habría que adaptar los programas de formación? Fíjense, ahora mismo son películas, una foto que trata de responder de una manera estática a una realidad pero esa realidad se está moviendo continuamente; por lo tanto, la formación que estamos diseñando en un momento y ejecutando en el minuto siguiente —porque esto va muy deprisa- no tiene exactamente el mismo grado de eficacia, y en mi opinión habría que acudir a fórmulas imaginativas. Y, si me permiten hacer la referencia al Incibe, en 2016 sacamos un estudio en tendencias de ciberseguridad que trataba de alguna manera de iluminar o inspirar a los emprendedores sobre en qué tecnologías había que invertir y trabajar, y una de ellas estaba centrada —lo recuerdo perfectamente— en los entornos de ciberentrenamiento, *cyber range* y este tipo de soluciones, lo que se llama campos de maniobra cibernéticos.

En cuanto al ámbito que preguntaba su señoría de la ciberseguridad industrial, es uno de los temas más importantes; el nivel de madurez es muy bajo. Partimos de una cultura de aislamiento, es decir, los sistemas de ciberseguridad industrial que, como saben sus señorías, son de los que dependen realmente los servicios esenciales de la nación, son tecnología muchas veces no IT en sentido estricto, son tecnologías específicas *ad hoc,* vienen de mundo de protocolos no estándar, pero se están moviendo progresivamente al mundo de Internet, al mundo IP, y por lo tanto ahora ya son accesibles, y también por un tema de evolución natural, se están apoyando cada vez más en sistemas vamos a llamar estándar. Aquí hay un problema muy serio porque en actos de ciberterrorismo o cuando su origen venga por parte de un país donde tengamos intereses o donde tengamos una crisis, el objetivo claro va a ser el bloqueo, la destrucción y el sabotaje de estas tecnologías. Ahí hay que hacer un esfuerzo claramente específico en todos los sentidos, en desarrollo de productos y servicios, en formación y capacitación, pero, fíjense, empezando sobre todo por la cultura y la concienciación en muchos casos. En mi opinión —como pueden ver sus señorías, es una de las líneas de actividad de mi compañía—, creo que —si me permiten el símil— se empieza a mover la rueda, es decir, empieza a trabajarse, en general hay mayor madurez en los modelos de gobierno en la ciberseguridad industrial, empiezan a aparecer proyectos en los que se trata de mejorar el marco de control, se empieza a mover, pero es un campo importante, muy sensible, y que requiere un esfuerzo especial.

Respecto a los aspectos de colaboración, yo diría que la ponderación del ciberespacio es uno de los mejores ejemplos —si me permite decirlo el presidente— de los mejores escenarios donde la colaboración internacional es imprescindible en todos los aspectos. Desde el punto de vista —por ejemplo a través del convenio de Budapest y otros convenios— de establecer una armonización en la identificación, en la categorización de lo que es un ciberdelito, en mejorar la colaboración entre las policías especializadas de cada país. Fíjense ustedes que cuando ocurre una acción ilícita en el ciberespacio el origen es complejo en el sentido de que podemos estar recibiendo un ataque de un país cuando el origen es un tercero y existe una clara heterogeneidad en la conceptualización jurídica del ilícito. Es muy complicado, ya que lo que es delito en España no lo es en otro país, y eso hace que sea, repito, realmente complicado. La colaboración internacional yo diría que es esencial en todos los aspectos, desde el punto de vista de la organización jurídica como comentaba, pero también desde el punto de vista operativo. Desde el punto de vista interior, podría poner otro excelente ejemplo de lo importante que es la colaboración público-privada pero, fíjense ustedes, público-público también, y aquí me quedo. Es un campo de mejora increíble; aquí me quedo.

¿Dónde está la información y los puntos de datos para mejorar? Creo que esta pregunta va muy ligada con los temas de cooperación público-privada. Yo les comentaba, señorías, que es muy importante la colaboración público-privada en el sentido de que los operadores de infraestructura crítica, los operadores de servicios esenciales son claves para la estabilidad de la economía, de la sociedad, para nuestra seguridad. Tiene que haber un flujo de información y una colaboración continuada, sostenida y de calidad entre todos los actores, pero no dejaría fuera de este entorno de colaboración, por ejemplo, a las universidades y a los centros de investigación, que, como hemos venido comentando, son elementos

cve: DSCG-12-CM-97

esenciales para el desarrollo de programas de investigación científica, para la generación de soluciones que puedan tener su trazabilidad hacia la industria. Por tanto, yo diría que es un entorno, el de la protección del ciberespacio, que *per se* debería fomentar la colaboración entre todas las instituciones.

En relación a cómo se trasladan las políticas del Estado a los ámbitos regionales, yo diría que hay muchísimo de mejora en este campo. Desde el punto de vista de la protección de las infraestructuras de telecomunicación y de tecnología del sector público, tanto en el ámbito de la Administración General como la autonómica y la local, se hecho un esfuerzo muy grande en los últimos años a través de la implantación y desarrollo del esquema nacional de seguridad. Es cierto que quizá no ha tenido el nivel de capilaridad deseable por una cuestión estrictamente presupuestaria, pero creo que es un modelo —si no lo conocen sus señorías les invito a que profundicen— que es una referencia internacional en cómo proteger las tecnologías en el ámbito de lo público. Ese es un aspecto, pero en lo que se refiere al desarrollo de acciones específicas de servicios públicos dirigidos a las empresas y los ciudadanos, creo sinceramente que el campo de mejora en la coordinación entre las distintas administraciones es claro y notorio.

Hablábamos también de puntos débiles, pero permítanme que no profundice excesivamente dado el carácter público que tiene esta intervención.

En cuanto a la regulación que falta, quisiera destacar la regulación que tenemos. Podemos decir con orgullo que somos un referente internacional en materia de protección de infraestructuras críticas, eso es así. Estamos tremendamente avanzados en relación no ya con otras regiones, sino dentro de la Unión Europea; somos un país de referencia en materia de protección de infraestructuras críticas, y creo que ese modelo se va a reforzar una vez que se realice la transposición de la directiva europea de seguridad en redes e información. Somos un auténtico referente en materia de protección de infraestructuras del sector público, como les he mencionado anteriormente.

Creo de verdad que hay un modelo bueno, un modelo sólido, pero es un modelo que quizá no se ha podido desarrollar en toda su profundidad por una cuestión que he mencionado antes, que es la falta de una memoria económica. El modelo está bien diseñado, está bien conceptualizado y nuestras Fuerzas y Cuerpos de Seguridad del Estado son referencia internacional, ocupan un puesto de relevancia en Europol en materia de investigación tecnológica. Podemos sentirnos orgullosos, pero nos falta ese punto más debido a nuestro propio modelo de país altamente dependiente de las tecnologías; nos falta un punto más de velocidad, si me lo permiten.

En respuesta a las alianzas o modelos de colaboración entre los distintos departamentos del Gobierno, creo que en este punto hay una oportunidad de mejora tremenda. Fíjense ustedes, señorías, cómo el Reino Unido ha ido a un modelo de concentración de capacidades a través de la creación de una Agencia Nacional de Ciberseguridad donde se consolidan gran parte de las capacidades. Si ustedes analizan cómo se estructuran los países de nuestro entorno en materia de protección del ciberespacio, verán cómo la arquitectura es mucho más sencilla que la nuestra; mucho más sencilla. Si me permiten la osadía, les invitaría a hacer una reflexión sobre cómo organizarnos mejor. Como saben ustedes, a la hora de gestionar los recursos, uno mas uno es tres; es decir, la capacidad de agrupar racionalmente distintos organismos va a permitir también una mayor eficiencia en cuanto a la gestión de los recursos, que sabemos que son recursos, si no escasos, sí restringidos, evidentemente. Creo que en ese punto también podríamos hacer algunas mejoras interesantes. Si ustedes lo analizan, en muchos Estados hay dos ámbitos autónomos que quedan fuera, que son el ámbito de la defensa y el ámbito de los servicios de inteligencia, pero que hay una tendencia a agrupar todos los demás en una única agencia, y eso permite sinergias desde todos los puntos de vista.

Con respecto a la prevención y protección, yo quisiera que sus señorías se quedasen con un tema que ya es un tópico en el mundo de la ciberseguridad, y es que la cuestión no es prevenir para que no te ataquen porque la realidad es que te van a atacar. La cuestión que hay que debatir es cuándo te van a atacar; esa es la cuestión que hay que debatir. Por mucho que tratemos de tener políticas preventivas, lo importante es la detección y la respuesta, sin desmerecer a las otras, pero es que va a ser una realidad, no vamos a poder prevenir lo suficiente para no dejar de ser atacados. Teniendo en cuenta esto, creo que las acciones encaminadas a mejorar la cultura de la ciberseguridad en la sociedad española son muy importantes. Es muy importante inculcar prácticas de lo que se llama en algunos ámbitos la ciberhigiene. No sé si sus señorías han tenido oportunidad de escuchar este término; ya saben que los especialistas en ciberseguridad ponemos el prefijo cíber a muchas cosas y queda muy *cool*, pero todo tiene un sentido. Realmente, la ciberhigiene trata de seguir las mismas pautas que seguían nuestros padres cuando éramos pequeños a la hora de inculcarnos buenas prácticas de higiene personal, de tal manera que cuando

cve: DSCG-12-CM-97

fuéramos adultos las incorporaríamos de una manera automática y prácticamente sin cuestionarlo porque nuestra madre nos educó de esa forma. Esa idea lo que trata es de generar esas buenas prácticas en nuestros hijos, nativos digitales, para que durante toda su vida actúen de una manera higiénica, preventiva, que evite en la medida de lo posible en su esfera profesional y personal que sucedan incidentes de ciberseguridad o ser objeto de fraude.

En relación con el talento, quisiera tener la oportunidad de destacar, por si no lo he expresado con claridad en mi intervención, que en España hay talento. De hecho, como les he dicho, esto de que en España hay talento es un tópico, pero es que de una manera empírica lo he visto. En los tres años que he estado al frente de Incibe he tenido muchas oportunidades, a través de distintas iniciativas, a través de concursos y a través de talleres, de detectarlo en España. No sé por qué, no soy sociólogo y lo siento, pero esa es la realidad.

Les voy a poner un ejemplo que no sé si conocen; hace cuatro años se decidió crear una iniciativa a nivel europeo que se llama European Ciber Security Challenge, que es una competición de países en materia de ciberseguridad en la que se dan unas condiciones, como que los participantes tienen que tener cierta edad y no tienen que trabajar formalmente o estar contratados por una empresa de ciberseguridad. Cuando yo estaba en Incibe nos enteramos de esa competición una vez que ya se había producido la primera edición y decidimos formar a la selección española. Fuimos identificando talento a través de distintas iniciativas y lo presentamos a esa primera edición en la que quedamos cuartos de ocho, siendo, como se dice en la NBA, los *rookies* mejor valorados. Al siguiente año se ganó entre doce países, y el año pasado, que se celebró en Málaga y fue organizado por España, se volvió a ganar y ya eran catorce los países que estaban compitiendo. Quizá es una anécdota, pero de alguna manera es un hecho concreto donde se ve que hay talento.

En relación con la ciberreserva, que mencionaba su señoría, como oficial de la Armada soy —¡cómo no!— un firme defensor de la oportunidad que ofrece una ciberreserva para mejorar la integración de la sociedad civil en la defensa nacional, para generar una mayor cultura de defensa y, desde luego, es un instrumento, por qué no, para generar cultura de ciberseguridad. Mi preocupación, que he manifestado públicamente, está basada fundamentalmente en que creo que a la hora de ver cómo se ejecuta y cómo se materializa esa ciberreserva hay que ser muy cuidadoso y muy meticuloso en la definición de los escenarios de actuación, en primer lugar, y en cómo se va a captar el talento necesario para cubrir esas necesidades en un mercado que saben ustedes que es claramente deficitario, en segundo lugar. Si me permiten, aquí me gustaría ponerles como ejemplo una iniciativa habitual en el mundo anglosajón —en Estados Unidos y Reino Unido especialmente, aunque también en Australia— en el que en la búsqueda de posibles profesionales para integrar en la ciberreserva los ministerios de Defensa proporcionan programas de capacitación para el personal de las Fuerzas Armadas que se va a desvincular de las mismas y que, por lo tanto, están buscando una oportunidad profesional. Eso permite cubrir parcialmente, por un lado, las necesidades de ciberreserva y, sin duda, es una contribución general al mercado de ciberseguridad, en tanto en cuanto se están generando profesionales que luego pueden prestar sus servicios en instituciones públicas y privadas.

En cuanto a que hay que cambiar el Incibe, yo creo que quizá una de las debilidades que tiene el Incibe —lo planteo, pero no tengo la solución— es su propia personalidad jurídica. Incibe es una sociedad pública estatal y, por lo tanto, su capacidad reguladora es nula y está sujeto a los condicionantes que aplica cualquier empresa del sector público, si bien es una empresa deficitaria, si me lo permiten, porque se está utilizando para proporcionar servicios públicos. Creo que habría que realizar el ejercicio, en la medida de lo posible y con las posibilidades que nos ofrece nuestra Ley de servicios públicos, de buscar una figura jurídica que sea más acorde.

Señorías, aquí hay un problema para el que tampoco tengo la solución, y es que cuanto más vinculada a la Administración está una organización que presta servicio de ciberseguridad, mayor empaque jurídico tiene como una entidad regulatoria, pero mayor es también la pérdida de flexibilidad, que es algo fundamental en el mundo del ciberespacio. Me refiero no tanto a una ligereza en la contratación —no lo interpreten así—, sino, en muchos casos, en dotarse de recursos, poder realizar algún tipo de acción concreta cuando se requiere. Hay una tensión entre ser más Administración o menos, en los dos sentidos que les planteo. Lamentablemente, no tengo la solución.

En cuanto a la comunicación de ciberincidentes por parte de sectores estratégicos e infraestructuras críticas, hay que decir que la tendencia en la regulación es a imponer la notificación de incidentes. Si en el pasado ha habido incidentes importantes —yo no tengo esa visión— que no hayan sido oportunamente

cve: DSCG-12-CM-97

comunicados —en mi experiencia personal no ha sido así, pero no dudo de que haya podido haberlo—, creo que esa situación claramente va a desaparecer por dos cosas fundamentales que ustedes conocen bien: en primer lugar, la implantación del Reglamento Europeo de Protección de Datos y la futura ley orgánica que está muy avanzada; en segundo lugar, porque la propia Directiva NIS exige la notificación de aquellos incidentes de ciberseguridad que afecten gravemente a la provisión de servicios esenciales. Luego, sí o sí, la tendencia general es a obligar a notificar esos incidentes. Lo que pasa es que después nos tendremos que poner de acuerdo en qué es un incidente y qué no lo es, y cuándo hay que notificarlo, porque, como sus señorías pueden imaginar, en un operador de infraestructura crítica, en una entidad pública, al día hay miles de intentos de intrusión y cosas que en un momento determinado podrían ser catalogadas como incidentes. Habrá que hacer un trabajo muy fino de taxonomía de lo que es y de lo que no es.

Respecto al modelo de educación, creo que ya hemos comentado algo, aunque quizá se puede profundizar más. En cuanto a la forma de plantear el modelo de concienciación en la sociedad, cuando he tenido la oportunidad de hacer una exposición pública en alguna conferencia o congreso, siempre me gusta poner como modelo el plan que se siguió en seguridad vial, porque creo que ha sido muy exitoso. Por lo que se refiere a cómo plantear la concienciación en ciberseguridad, yo diría que de una manera formal, es decir, definiendo unos objetivos y una línea de acción. Es muy obvio lo que voy a decir, pero es que las iniciativas voluntaristas que no responden a unos objetivos concretos tienen la eficacia que tienen, pero en muchos casos nos hacen perder un recurso valioso, que es el presupuestario. Creo que se deberían sentar las instituciones que tienen responsabilidades en cuanto a la concienciación para diseñar un plan nacional de concienciación en toda su amplitud, fijar unos objetivos y unos indicadores para medir el resultado. Eso es lo que les diría.

Creo que con esto he respondido, señor presidente.

El señor **PRESIDENTE:** Muchas gracias.

Antes de dar la palabra para consumir un segundo turno, si me lo permite, quisiera hacer una observación. Ha dicho usted que la colaboración internacional es imprescindible en este terreno, cosa que es una obviedad, y que el obstáculo más importante para ello es la distinta tipificación penal de los delitos relacionados con la ciberseguridad. Como conclusión, se me ocurre que se podrían incluir en la ponencia —son los ponentes los que lo dirán y usted me confirmará si estoy acertado o no— los ciberdelitos en el catálogo de supuestos de la euroorden en la que la entrega se produce automáticamente sin necesidad de pasar por la doble incriminación, en cuyo caso sí que nos encontraríamos con el problema que usted ha mencionado. Probablemente podría ser operativo. Esto lo digo para demostrar que de vez en cuando al presidente se le ocurre algo.

Tiene la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Intervengo simplemente para felicitarle por la comparecencia y decirle que nos ha dejado muchísima información que va a ser muy útil, porque ha sido muy concreta, y que vamos a aprovecharla bien.

Muchas gracias.

El señor **PRESIDENTE:** Tiene la palabra la senadora Angustia.

La señora **ANGUSTIA GÓMEZ:** Señor presidente, solo quiero agradecer al compareciente su explicación, porque se ha extendido sobremanera en muchas cosas que nos interesan. También quiero darle las gracias por su contribución a nuestro trabajo.

El señor **PRESIDENTE:** Tiene la palabra el senador Raffo.

El señor **RAFFO CAMARILLO:** Quiero agradecerle su presencia aquí. Creo que, tanto en la primera como en la segunda parte de su intervención ya nos había identificado algunas prioridades, fruto de su experiencia. Ahora solo pido un último esfuerzo, que sé que no es fácil, pero que nos llevará poco tiempo. Precisamente porque en su intervención ha identificado los puntos de mejora, por su experiencia extensa y vasta, creo que sería una oportunidad perdida no preguntarle cuáles serían los tres aspectos de mejora más importantes, dentro de la batería de los que hemos tratado. Repito, los tres elementos más importantes que hay que mejorar.

El señor **PRESIDENTE:** Tiene la palabra la señora Vázquez.

cve: DSCG-12-CM-97

La señora **VÁZQUEZ BLANCO:** Simplemente, a efectos de que conste en el *Diario de Sesiones* y para que el señor Rego se vaya tranquilo, quiero decir que la alusión que me estaban haciendo a través de Twitter no era por el señor Rego, sino por el anterior compareciente. Esté tranquilo, porque me están diciendo que la exposición ha sido brillante, y yo lo corroboro, por supuesto.

El señor **PRESIDENTE:** Tiene la palabra el señor Rego para responder a sus comentarios.

El señor **REGO FERNÁNDEZ** (Socio de iHackLabs): Como los Mandamientos, voy a tratar de resumirlo en tres.

El señor **PRESIDENTE:** Los Mandamientos se resumen en dos.

El señor **REGO FERNÁNDEZ** (Socio de iHackLabs): Sí, pero en este caso lo resumiré en tres, señor presidente. El primero, memoria económica; el segundo, reconsiderar el modelo organizativo de las capacidades públicas en materia de ciberseguridad; el tercero —si tengo que elegirlo me pone usted en un compromiso—, como hay que empezar las casas por los cimientos, crear un plan nacional de concienciación en materia de ciberseguridad.

El señor **PRESIDENTE:** Muchas gracias, señor Rego. Doy las gracias a sus señorías, porque después de una semana cargada de acontecimientos hemos tenido una sesión muy larga. Les agradezco a todos su presencia.

Les recuerdo que puesto que, al parecer, tenemos legislatura, sería bueno que fuésemos acelerando nuestros trabajos para culminarlos en una ponencia que, a mi juicio, puede ser importante en un tema que también lo es.

Se levanta la sesión.

Eran las cinco y diez minutos de la tarde.

cve: DSCG-12-CM-97