Diario de Sesiones de la Asamblea de Madrid

Número 94 | 29 de noviembre de 2023 | XIII Legislatura

COMISIÓN DE DIGITALIZACIÓN

PRESIDENCIA

Ilmo. Sr. D. Gustavo Alaín Eustache Soteldo

Sesión celebrada el miércoles 29 de noviembre de 2023

ORDEN DEL DÍA

1.- C-1078(XIII)/2023 RGEP.14754. Comparecencia de la Sra. D.ª Carla Redondo Galbarriatu, Secretaria General del Instituto Nacional de Ciberseguridad (INCIBE), a petición del Grupo Parlamentario Socialista, con el siguiente objeto: contexto regulador del Proyecto de Ley PL-1(XIII)/2023 RGEP.11518, por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid. (Por vía del artículo 144.1 del Reglamento de la Asamblea).

2.- Deliberación y votación del Dictamen al PL-1(XII)/2023 RGEP.11518, de creación de la Agencia de Ciberseguridad.

3.- Ruegos y preguntas.

SUMARIO

(Se abre la sesión a las 11 horas y 3 minutos).

El Sr. **PRESIDENTE**: Muy bien, señorías, buenos días. Damos comienzo a la sesión de la Comisión de Digitalización del día de hoy. Como cuestión preliminar, solicito a los grupos que comuniquen las sustituciones de diputados para esta sesión. La señora González está... *(Pausa.)* Ninguna.

La Sra. **TORIJA LÓPEZ**: Sí, Alberto Oliver va a sustituir a Emilio Delgado.

El Sr. **PRESIDENTE**: Muy bien. ¿Y Partido Popular? *(Pausa.)* Nada, ¿no? Muy bien. Cumplido este trámite, abordamos el orden del día, abriendo el primer punto.

C-1078(XIII)/2023 RGEP.14754. Comparecencia de la Sra. D.ª Carla Redondo Galbarriatu, Secretaria General del Instituto Nacional de Ciberseguridad (INCIBE), a petición del Grupo Parlamentario Socialista, con el siguiente objeto: contexto regulador del Proyecto de Ley PL-1(XIII)/2023 RGEP.11518, por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid. (Por vía del artículo 144.1 del Reglamento de la Asamblea).

Por parte del Incibe se comunicó que, en lugar de la señora Galbarriatu, secretaria general, comparecería el director general del Incibe, don Félix Barrio, a quien damos la bienvenida, agradecemos su presencia y rogamos que ocupe su puesto en la mesa. Mientras ello sucede, les informo que la tramitación tendrá lugar de conformidad con el artículo 144, en concordancia con el 211, ambos del Reglamento de la Asamblea. Para que el compareciente conozca la tramitación, muy brevemente le indico que le corresponderá a usted un turno inicial de quince minutos, posteriormente intervendrán los portavoces de los grupos parlamentarios por tiempo máximo de diez minutos cada uno para solicitar aclaraciones sobre su exposición y le corresponderá a usted una segunda intervención para responder esas aclaraciones por un tiempo máximo de diez minutos. Así que, sin mayor dilación, damos paso a la intervención del señor Barrio, director general del Incibe; cuando quiera.

El Sr. **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD** (Barrio Juárez): Muchas gracias. Buenos días, señores diputados, un placer acompañarles hoy aquí. Muchas gracias por la invitación al Instituto Nacional de Ciberseguridad para compartir con ustedes nuestra perspectiva sobre algo muy importante, que es el proceso de creación de una agencia de ciberseguridad autonómica en la línea de algunas que ya se han creado en los últimos años y que, desde nuestro punto de vista, constituyen un instrumento que, sin duda, puede contribuir decisivamente a mejorar el nivel de gobernanza y de servicio público de ciberseguridad en el ámbito de la Administración para nuestras ciudadanas y ciudadanos. Por lo tanto, felicitarles y a su disposición.

Si me permiten, les voy a compartir una información que me gusta decir que es el rostro de qué estamos hablando cuando estamos hablando de ciberseguridad. Esto es una conexión ahora mismo

en directo a lo que es el mapa de eventos de ciberseguridad relacionados en su mayoría con ciberataques que se están recibiendo en tiempo real en la red de internet en España. Aproximadamente estamos gestionando ahora mismo del orden de 25.920 incidentes en el territorio nacional. Verán que hay otros países en los que aparecen círculos de colores, son las direcciones IP, esas direcciones que están en cualquier dispositivo que se conecta a internet en el mundo y que pertenecen a entidades y empresas españolas que tienen esos activos en el extranjero: puede ser Iberdrola, puede ser el grupo Zara..., cualquier operador crítico que nos comunica esas direcciones y que procedemos a la monitorización mediante básicamente una serie de acuerdos y convenios internacionales con entidades como, por ejemplo, puede ser Microsoft, de Estados Unidos, que nos va transfiriendo información sobre esos activos que pertenecen a la compañía y que en este caso son titularidad de alguna de las entidades o de los ciudadanos españoles. Como ven, esta es una información que se va a ir actualizando cada diez minutos. El propósito que tenemos con este mapa es que se pueda ver de una manera gráfica de qué estamos hablando cuando estamos hablando de ciberataques.

Si me permiten hacerles rápidamente un zoom, estamos agregando los datos de las IP por distritos. No tiene más propósito que la visión estadística. Podríamos llegar a saber en qué calle y en qué dirección está la IP localizada; por motivos, lógicamente, de legislación de privacidad eso solo lo haríamos bajo mandato judicial en el curso de una investigación criminal y no podemos acceder a esa información por defecto. Pero, bueno, pueden ver que, en lo que es la Comunidad de Madrid, ahora mismo podemos estar hablando de probablemente unos 12.500-13.000 eventos que se están produciendo a esta hora, el mayor número de ellos conforme vamos acercándonos a la centralidad de la capital. Si pulsamos, por ejemplo, aquí, verán las tipologías, qué tipo de incidentes de ciberseguridad se están produciendo y que están afectando a las IP de computadoras y dispositivos móviles madrileños.

En primer lugar, hay 6.732 IP que están siendo sometidas a algún tipo de chequeo no autorizado; está prohibido por la legislación europea y, por supuesto, española. Esto es gente que está intentando comprobar si ese dispositivo conectado a internet tiene algún tipo de puerta a través de la de la cual puede perpetrar un ataque, acceder al sistema y obtener información de ese posible objetivo, con lo cual, en sí mismo ya estamos hablando de un delito, que puede estar originado -luego, lo veremos, si nos da tiempo- en un tercer país. Normalmente la mayoría de los países, para su sorpresa, van a ser ordenadores que están basados en la Unión Europea o en Estados Unidos frente a lo que pudiera parecer; también veremos a China o a Rusia, pero interponen diferentes tipos de computadoras en países de origen que están bajo el ámbito de la Unión Europea o Estados Unidos, que les permite filtrar nuestros propios sistemas de control de acceso desde esos terceros países.

El segundo grupo son las bot, que esto es un tipo de virus informático. Hoy en día los virus tienen diferentes tipos de clasificación, no les aburriré, pero todos ellos se suelen agrupar bajo el concepto de software malicioso. Si hacemos un vistazo rápido a qué tenemos esta mañana en Madrid, pues veremos que en el centro de la ciudad hay 434 ciudadanos que se acaban de infectar esta mañana de un tipo de virus que se llama FluBot; esto es un tipo de virus que detectamos hace casi dos años, que ya lanzamos el aviso. Infecta básicamente a usuarios de dispositivos móviles con sistema operativo Android; llega un mensaje señuelo, normalmente un sms, que les dice que han intentado entregar un

paquete que han comprado en una tienda on line, tipo Amazon, les dirige a una página web en el caso de que pinchen sobre ese mensaje. Si es un dispositivo iPhone, va a salir una información y, si es un dispositivo Android, va a ser otra. Si es un dispositivo Android, le va a invitar a aceptar un plug-in, es decir, una especie de pequeña aplicación informática que les va a permitir localizar dónde está el repartidor, y en ese momento se va a infectar el teléfono si no tiene instalado un antivirus, cosa que sucede en casi el 40 por ciento de los usuarios de teléfonos móviles Android españoles: que no tienen antivirus instalado. Lo primero que hace ese virus es replicar el mismo falso mensaje sms a toda la lista de contactos. Multipliquen cuántos contactos podemos tener en el móvil cualquiera de nosotros, pues multiplíquenlo por 434; podemos estar hablando de medio millón de sms que acaban de salir desde el centro de Madrid a 500.000 personas que están conectadas a estos 434 usuarios conectados.

Lo segundo que va a hacer es empezar a grabar todo lo que aparezca en pantalla de ese teléfono móvil; quiere decir que va a salir no solamente la información de contraseñas de tipo tiendas de comercio electrónico, de portales de banca..., sino también toda la información confidencial los correos electrónicos de nuestra empresa corporativa si tenemos el correo electrónico en el móvil y de nuestro WhatsApp de los mensajes que estamos lanzando, y toda esa información se está reemitiendo a un tercer computador que va a hacer uso de ella. Sabemos que van buscando fundamentalmente este tipo de datos para fraude bancario, tarjetas de crédito, contraseñas de tiendas on line..., pero imagínense también si estamos hablando de un empleado público que esté viendo el correo corporativo, imagínense si estamos viendo diseños de tipo industrial de una empresa..., cualquier tipo de información. Con lo cual, aquí ya empiezan a ver que la división de la línea entre lo privado y lo público empieza a desaparecer, que es el propósito de esta comparecencia. Aquí vamos a ver que seguramente, de esos 500.000 objetivos, va a haber muchos entre los que podemos estar cualquiera de nosotros a los que nos está llegando ya ese intento para empezar de ciberataque.

Andrómeda, Loapi, Ramnit, Conda..., son otro tipo de virus. Andrómeda, en este caso, afecta a sistemas computadoras de tipo Microsoft; es también un virus que ya se identificó hace cinco o seis años, que cualquier ordenador que tenga el antivirus instalado y actualizado el software pues debería de estar neutralizándolo, pero nos dice que acaba de producirse 103 infecciones. Aquí estaremos viendo seguramente computadoras domésticas o de empresas que no están debidamente gestionadas, actualizadas, y también puede darse el caso de que estén dentro de organismos públicos, evidentemente. Loapi es un virus que viene de regalo con algunas aplicaciones que se instalan los usuarios en los teléfonos móviles; esto viene ya pues en aplicaciones de tipo descargas gratis de música, etcétera, y, una vez que lo instalas en el dispositivo, en la tableta o en el móvil, viene el virus, y también son virus que empiezan a retransmitir información y que permiten abrir puertas para acceder a los atacantes con otro tipo de propósitos, como pueden ser en este caso el secuestro de equipos de ransonware. No me extiendo más sobre este ámbito, pero para que se queden un poco con la imagen de qué estamos hablando.

En este caso concreto, la ciberseguridad en lo que es el ámbito público, para que se hagan una idea, el pasado mes de febrero, respecto a los datos sobre ataques a las Administraciones públicas españolas de 2022, el Instituto de Cuestiones Internacionales y Política Exterior extrajo una estadística

que nos indicaba que se habían producido en el último año 55.000 ataques, a un ritmo de 150 ataques al día; de todos ellos, 71 ataques diarios, ataques críticos: 9 en la Administración central, 24 de las Administraciones autonómicas y 38 en ayuntamientos. O sea que multipliquen, si ahora mismo estamos hablando de 29.000 eventos, que algunos de ellos ya son incidentes y otros pueden constituirlo, se van a materializar, posiblemente, entre 25 y 50 ataques críticos en el ámbito de Administraciones autonómicas que van a formar parte de esas IP que están ahí. Esto sirve, yo creo, para que tomemos conciencia sobre el reto que tenemos con la creación de agencias en el ámbito autonómico, que nos van a permitir, y así lo llevan haciendo desde la creación de las primeras en el ámbito de comunidades como Cataluña, Valencia o el País Vasco, multiplicar los sistemas de vigilancia y monitorización. Estamos hablando de la competencia directa de las Administraciones autonómicas en decenas y decenas de miles de equipos de activos conectados en IP a través de unas amplísimas redes como las que gestiona la Comunidad de Madrid, en el ámbito de centros educativos, centros sanitarios, sistemas de transporte, etcétera, etcétera, etcétera. Como se imaginarán, la capacidad que tenemos en el ámbito de Administración central nunca va a ser suficiente para el volumen de equipos sobre los que tenemos que desplegar sistemas de vigilancia de cómo están afectando esos miles de eventos diarios, que además están creciendo a un ritmo superior al 10 por ciento anual; probablemente este año el crecimiento sea superior al 20 por ciento. Es decir, que no solamente esto es una realidad que hay que gestionar, tenemos que prepararnos para lo peor.

El sistema de gobernanza de la ciberseguridad en España, desde mi punto de vista, es un caso de éxito y así lo hemos trasladado en numerosas ocasiones en las misiones internacionales para ayudar a diferentes países a establecer sus estrategias nacionales de ciberseguridad. Es verdad que es un sistema que no es tan popular como el de las agencias únicas centralizadas, en el cual en algunos países se ha optado por concentrar todo este esquema de agencias que ahora les voy a explicar sucintamente en una agencia única central, pero es que nuestro modelo es un modelo adecuado a nuestro sistema constitucional, legislativo y organizativo, en el cual hay una gran capacidad de gestionar el servicio público en un concepto para la tecnología que ustedes entienden perfectamente, que es el de proximidad. Porque al final solamente se puede gestionar aquello que se maneja directamente y, cuanto más lejos estamos de los sistemas de monitorización, es más difícil la inmediatez y, sobre todo, la mejora continua en el despliegue de tecnologías de prevención, de protección y de respuesta frente a unos ataques que van a acabar haciendo daño en un momento u otro a cualquier activo conectado hoy en día a internet.

A nivel político, en España es el Consejo Nacional de Seguridad, como ya conocerán, que a su vez tiene delegada en el Consejo Nacional de Ciberseguridad la coordinación a nivel de estrategias nacionales y de sistemas de gestión, administración y respuesta, en el que participan representantes de diferentes entidades ministeriales y cuyo secretariado corresponde al Departamento de Seguridad Nacional en Presidencia del Gobierno. Básicamente, lo que es a nivel operacional somos tres los ministerios -Ministerios de Defensa, de Interior y de Transformación Digital- que sí disponemos de organizaciones o agencias con competencias en materia de vigilancia, de despliegue y de servicio frente a este tipo de incidentes.

En primer lugar, en el Ministerio de Defensa, el Centro Criptológico Nacional, perteneciente al CNI, y el mando conjunto del ciberespacio: en el primer caso, con las competencias en lo que es protección frente a incidentes que afecten a las Administraciones públicas y que particularmente despliegan en incidentes que están clasificados como de nivel grave o crítico, y, en segundo lugar, el mando conjunto del ciberespacio, que entra en temas de ciberguerra y ciberdefensa con motivos obvios.

En el Ministerio del Interior, el CNPIC y la Oficina de Coordinación Cibernética, en particular, que, dependiendo de la Secretaría de Estado de Seguridad, tienen la competencia de coordinación con Policía y Guardia Civil en materia de investigación sobre ciberdelitos. Háganse cargo de que, en el último año, según la estadística del Ministerio del Interior, 1 de cada 4 crímenes o delitos que se cometen en España están en el ámbito de lo digital, exactamente un 17 por ciento de los delitos que se gestionan por Interior. Esto ha implicado que haya que crear ese organismo de coordinación, la Oficina de Coordinación Cibernética, que distribuye la respuesta de Policía y Guardia Civil.

El CNPIC, Centro Nacional de Protección de Infraestructuras Críticas, tiene las competencias en la designación de lo que se denominan operadores esenciales; es un catálogo confidencial, pero aquellas instituciones que no se nos escapa, pues pueden incluir desde las centrales nucleares a los aeropuertos, pasando por las depuradoras de agua. Desde la aprobación en el 2008 de la Ley de Infraestructuras Críticas prevemos que puede llegar a haber en España entre 8.000 y 10.000 infraestructuras críticas y operadores esenciales, pero el ritmo de designación ha sido mucho menor; en estos años no hemos alcanzado esa cifra ni de lejos y estamos todavía en trance básicamente por un problema también de gobernanza: en cuanto a la designación, implica esa necesidad de que estos organismos clasificados, el 90 por ciento privados, tengan un sistema de certificación de su ciberseguridad, una auditoría anual que demuestre su nivel de preparación para resistir este tipo de ciberataques. Cuando son designados, pasan a nuestro ámbito competencial.

Y el Instituto Nacional de Ciberseguridad es una sociedad estatal mercantil que pertenece a la Secretaría de Estado de Digitalización e Inteligencia Artificial y, por ley, tenemos la competencia de respuesta frente a incidentes de estos sectores estratégicos designados por Interior, del conjunto de ataques que afectan al sector privado, a la ciudadanía y las empresas españolas, y, en particular, el Real Decreto 311, del Esquema Nacional de Seguridad, nos establece centro de respuesta de los proveedores de las Administraciones públicas. Por lo tanto, complementamos, en este sentido, las labores de vigilancia y de respuesta que el Centro Criptológico Nacional presta a las Administraciones y en coordinación con la Secretaría General de Administración Digital, que es la que tiene las competencias de la estrategia y del desarrollo de las capacidades de ciberseguridad del sector público.

Por lo tanto, vemos que hay básicamente tres agencias de respuesta a incidentes: dos en Defensa, Incibe y organismos reguladores, que serían la Secretaría de Estado de Seguridad y la Secretaría General de Administración Digital. Con todo eso, a nivel técnico hay un sistema de coordinación impecable, una plataforma nacional, un conjunto de herramientas y un marco, que específicamente es el Esquema Nacional de Seguridad, que establece los requisitos de las Administraciones en materia de cómo se configuran las nuevas tecnologías desde el punto de vista de

la ciberseguridad y, sobre todo, y lo más importante, establecen un mecanismo de auditoría que nos permite medir el nivel de capacidades. Ese Esquema Nacional de Seguridad también es obligatorio para los proveedores.

En resumidas cuentas, un ayuntamiento será tan seguro como lo sean la empresa que le vende sus ordenadores, la empresa que gestiona sus bases de datos o la empresa que lleva su página web y que le da el soporte. Por lo tanto, hay una dependencia muy estrecha entre la gestión de los activos públicos y la gestión de nuestro sector de la industria de ciberseguridad. En ese sentido, comprenderán que Incibe haya recibido para el período que comprende 2023-2026, nada menos que 634 millones de euros del mecanismo de recuperación y resiliencia, que se unen a más de 100 millones de presupuesto que recibimos a través de los presupuestos generales del Estado, para acometer, entre otras cosas, el desarrollo de ese tejido productivo de servicios digitales, que es el que constituye la piedra de toque para poder mantener el nivel de seguridad que las Administraciones requieren. Y, con todo y ello, tenemos graves carencias en términos de número de empresas proveedoras certificadas en ciberseguridad. Hay provincias que todavía no disponen más de 3, 4, 5 o 6 pymes que tengan un nivel de adecuación a lo que requiere la legislación en materia de estándares de ciberseguridad y, por ello, la Agenda Digital para España ha establecido que la mayor parte del esfuerzo inversor en desarrollo de capacidades y de apoyo al emprendimiento se destine a aquellos territorios donde carecemos todavía de ese elemento que definimos como soberanía tecnológica nacional de ciberseguridad. No es el caso de la Comunidad de Madrid, pero evidentemente aquí también estoy seguro de que el problema de la "periferialidad", de lo que significan aquellos pequeños ayuntamientos, en particular de menos de 20.000 habitantes, que todavía tienen carencias, nos consta por la insuficiencia de medios personales y técnicos para poder disponer de esas estrategias que les permitan tener un nivel de seguridad óptimo y gestionar sus proveedores de manera conveniente.

En este sentido, el rol que tienen agencias como la que están en trámite de debatir contribuyen decisivamente a facilitar el despliegue de toda una estrategia conducente a tener capacidades de monitorización y de respuesta rápida a todo ese volumen de incidencias y, además, en una coordinación imprescindible, porque estamos hablando de responsables de ciberseguridad que van desde una escuela de Primaria a un centro de atención sanitaria, pasando por todas las Administraciones locales en el territorio. Y esto contribuye, en mi opinión, tanto para el Centro Criptológico Nacional en su labor de vigilancia como también para nosotros en la misma labor de vigilancia desde el punto de vista de los proveedores y de los usuarios finales. Creemos que directamente es tan importante que en el año 2010 desplegamos un programa de llamado CERT en un mes; CERT es el acrónimo de equipos de respuesta a incidentes que hay a nivel internacional, que pueden ser de tipo público o privado. Nuestro objetivo era que cualquier comunidad autónoma que quisiera desplegar un centro regional de ciberseguridad pudiera disponer de la implantación de nuestras herramientas nacionales y configurar la vigilancia de sus activos, reforzando nuestra capacidad, como decimos, de llegada temprana y de obtener una información directa del nivel de preparación respecto a los posibles ciberataques en ese conjunto de activos que dependen del ámbito autonómico.

Por lo tanto, en estos 14 años hemos podido comprobar que aquellas comunidades que disponen de esa capacidad propia para tener una coordinación plena de sus sistemas tecnológicos para tener sus propias estrategias e invertir son aquellas en las que más rápidamente podemos desplegar acciones de prevención y de respuesta. Ello también se ha reforzado con la iniciativa, dentro de la Agencia Digital para España, del programa Retech Ciberseguridad, un programa destinado a cofinanciar con un 75 por ciento programas de las comunidades autónomas que permitan reforzar su desarrollo de capacidades. Y, además, la Comunidad de Madrid se ha presentado a esa convocatoria, obteniendo, junto a las comunidades de Andalucía, País Vasco y Castilla y León, la coordinación de un programa de nodos que nos permitirá invertir en los próximos cuatro años hasta 60 millones de euros en el desarrollo de acciones conducentes al desarrollo de capacidades en estas comunidades en materia de tejido productivo, de servicio público, de formación, de concienciación y de un tema muy importante: fomento del empleo, dada la perentoria necesidad de disponer de más profesionales en el mercado laboral de la ciberseguridad.

El Sr. **PRESIDENTE**: Señor Barrio, solo recordarle el tiempo que tenía y que tenía otro turno, ¿okey?

El Sr. **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD** (Barrio Juárez): Sí, para ir terminando.

El Sr. **PRESIDENTE**: Vaya terminando.

El Sr. **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD** (Barrio Juárez): Gracias, presidente. Para ir terminando, hemos tenido la oportunidad de analizar la documentación que han realizado sobre la tramitación del proyecto de ley; evidentemente, consideramos muy positivo el borrador del proyecto. En cuanto a las únicas consideraciones a tener en cuenta, evidentemente, clarificar muy bien que no haya una superposición con las competencias de las agencias de titularidad estatal y clarificar muy bien, en este caso, que no solamente se van a monitorizar activos, sino que se van a hacer en el ámbito competencial que corresponde a la comunidad autónoma, habida cuenta de que también hay organismos de titularidad estatal y, por supuesto, del sector privado en la Comunidad de Madrid, y no porque esté mal planteado, pero no dejamos de sugerir que en este caso sí que se haga una especial clarificación sobre esa limitación.

Asimismo, prevenimos como lo hemos hecho con el resto de agencias, la conveniencia de evitar la coordinación en materia internacional, las referencias a la coordinación transfronteriza y con organismos de la Unión Europea, que es una competencia de las agencias estatales, del Centro Criptológico Nacional a nivel de los CERT de las agencias públicas, y del CERT de Incibe para los CERT privados en Europa, y, en ese caso, creemos que evidentemente esto pues se puede recoger perfectamente en el artículo 2.1 sobre, en este caso, el alcance de las competencias que están tramitando y que se haga referencia expresa a que siempre es limitado al ámbito de la Administración de la Comunidad de Madrid. Igualmente, la delimitación, en este caso, que pueda aparecer en las diferentes enmiendas que también hemos tenido ocasión de recibir.

Por nuestra parte, nada más. Trasladarles de nuevo nuestras felicitaciones. Creemos que es una iniciativa que hace honor a una comunidad autónoma que es un referente lógico de no solamente el resto de las comunidades españolas, sino que también va a ser un referente para la Administración pública internacional: la valentía de legislar y de contribuir a tener una coordinación a nivel de monitorización de los sistemas de prevención, de respuesta y de despliegue de sistemas de ciberseguridad. Muchas gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señor Barrio. Seguidamente abrimos el turno de los representantes de los grupos parlamentarios, por tiempo máximo de diez minutos cada uno, al exclusivo objeto de pedir aclaraciones. Por el Grupo Parlamentario Vox de Madrid, señora González Moreno tiene la palabra.

La Sra. **GONZÁLEZ MORENO**: Muchas gracias. Buenos días a todos. Muchas gracias al señor Barrio por su comparecencia. Nada, simplemente quería decir que me ha parecido muy interesante y nada más. Muchas gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señora González Moreno. Por el Grupo Parlamentario Socialista, señor Cepeda García.

El Sr. **CEPEDA GARCÍA DE LEÓN**: Gracias, presidente. Bueno, en primer lugar, dar las gracias al Incibe, al Instituto Nacional de Ciberseguridad, y además que haya hecho un esfuerzo especial en enviarnos a su máximo responsable, al director general, también demuestra el interés de la Administración General del Estado, en este caso del Instituto Nacional de Ciberseguridad, porque con su presencia hoy aquí, y además después de su exposición, lógicamente deja en evidencia la importancia de la puesta en marcha de esta iniciativa, en la que, como bien sabe, desde luego el Grupo Socialista ha querido implicarse prácticamente desde el primer momento para para intentar desarrollar algo que nos parece una estructura dentro del conjunto de la Administración absolutamente necesaria, ¿no? Y que ayer mismo, en las jornadas que se pusieron en marcha dentro del CCN, que lleva ya implementando además en colaboración con servicios de inteligencia de todo el mundo, pues es verdad que se hacía una pequeña estimación de cómo estaban las comunidades autónomas y es necesario que Madrid, gracias a esta agencia, pues tenga un nuevo impulso, ¿no? Además, como muy bien usted explicaba, en un contexto extraordinariamente importante, donde efectivamente Madrid no deja de ser uno de los grandes centros donde también está la matriz de las principales empresas tecnológicas, de investigación...; es decir, que Madrid necesita, sin lugar a dudas, una protección especial.

Cuando veíamos el gráfico en tiempo real que usted nos mostraba, efectivamente, se visualizaban algunas zonas en Cataluña, otras zonas más cercanas a Sevilla, en el entorno del sur de Andalucía, y efectivamente la zona central de España, es decir, aquí, en Madrid, y no es no es baladí, es decir, tiene su sentido, porque posiblemente también, como decía, los mayores espacios de concentración de desarrollo tecnológico están aquí, en nuestra región. Por eso, desde el primer momento nos ha parecido al Grupo Socialista muy importante intentar darle impulso y además intentar también colaborar en la gestión de la puesta en marcha de una agencia donde, desde luego, tenga una

serie de posibilidades ciertas por parte de la Administración autonómica en ese nivel también de colaboración y de cooperación necesaria, de compartir información con las estructuras que ya están en marcha por parte del de la Administración General del Estado, del Gobierno de España.

Es importante y me gustaría preguntarle, en concreto, sobre algunas cuestiones en las que efectivamente, además, nosotros hemos intentado también aportar una serie de enmiendas y nos gustaría saber su opinión. La nueva directiva europea, la NIS2, ya viene un poco incidiendo en la importancia de dotar a las Administraciones de capacidad sancionadora en el caso de que efectivamente no exista voluntad por parte de muchos proveedores, porque usted hacía una mención que es rigurosamente cierta: buena parte de las Administraciones acaban derivando buena parte de los servicios digitales a distintos proveedores. Y es verdad que la Unión Europea nos va ya incidiendo, en ese sentido, en la importancia de que todos estos proveedores también tengan que estar obviamente sometidos a un control, a una monitorización, porque tienen que garantizar los servicios, entre otras cuestiones, que las propias Administraciones contratan con ellos. A nosotros nos gustaría saber su opinión, no sé si ya en el propio texto del proyecto de ley, pero sobre todo también pensando en el futuro, porque, evidentemente, ponemos en marcha una ley dentro de pocas semanas, pero la realidad que usted nos está mostrando en tiempo real pues nos va a requerir también de nuevos esfuerzos, sobre todo por parte de la de la Administración autonómica. Y nosotros, en ese compromiso de pensar siempre en el bien común, en la gestión de las cosas pensando también en la seguridad y en la protección de nuestros ciudadanos, en este caso en Madrid, pues lógicamente sí que nos gustaría conocer también en ese sentido el futuro de que la propia agencia pudiera tener capacidad sancionadora con respecto a todos estos proveedores que están gestionando buena parte también de los servicios digitales en nuestra región. Estamos hablando, obviamente, de la Administración autonómica, de su ámbito competencial, faltaría más.

Y otra cuestión que me gustaría también preguntarle, que también hemos tenido parte del debate en el trabajo que estamos desarrollando para la puesta en de esta ley, es hasta qué nivel... Es verdad que la autonomía tiene competencias... La Ley de las Bases del Régimen Local lo explicita claramente y es verdad que Madrid, la Comunidad de Madrid, en su capacidad que tiene como Diputación Provincial, tiene unas competencias en ayuntamientos menores de 20.000, pero gustaría saber su opinión -insisto: no sé si para el texto legal o para el futuro, para futuros reglamentos que se pongan en marcha inmediatamente tras ello- sobre si sería importante visualizar, no solamente hablar del ámbito competencial... Estamos hablando de servicios de monitorización, de control de las IP..., de no solamente ayuntamientos pequeños, que por supuesto yo creo que esto es esencial, de hecho, buena parte de los agujeros de seguridad están clarísimamente ubicados en las corporaciones locales pequeñas -menos de 20.000 habitantes-, sino -yo le decía, le quería preguntar- si sería interesante que la propia agencia diera cobertura a un amplio nivel de ayuntamientos, a todos los ayuntamientos, a los 179 ayuntamientos de la de la Comunidad de Madrid, con independencia de las cuestiones presupuestarias, que ya sabemos que cuando se habla siempre de dar servicios en ese sentido hablamos de muchas cosas, pero en concreto estas dos, estos dos elementos, nos parecen muy importantes, digamos, como futuros objetos de trabajo que tenga que desarrollar la puesta en marcha de esta futura agencia. Porque, insisto, según los últimos datos que tenemos, las corporaciones locales son objetivo prioritario

de los crackers y, luego, en otro sentido, es verdad que también se detecta que cuando más suelen atacar suelen ser los viernes a las cinco de la tarde, curiosamente cuando las Administraciones y los máximos responsables...; digo en esta idea de la monitorización 24 por 7, que no existe.

Por lo tanto, es verdad que yo creo que es importante -y con esto ya acabo- que, en ese sentido, la agencia también tiene que trabajar por una mayor capacitación también, ¿por qué no decirlo?, de nuestros empleados públicos para gestionar y tener una mayor autonomía. Y también yo creo que, en ese sentido, ir generando día a día esa cultura en torno a la ciberseguridad que en muchas ocasiones... Usted ha puesto algunos ejemplos de los propios usuarios de Android en sus teléfonos, es una evidencia. Pero es verdad que muchos ciudadanos no tienen esa cultura de la ciberseguridad, piensan que estamos absolutamente siempre protegidos y que sus datos son de ellos. Es interesante yo creo la puesta en marcha de la agencia; también es un mensaje a Madrid y a los madrileños de que los ciudadanos también, y yo espero que en ese sentido la agencia haga su trabajo, de intentar cada día más trabajar en esa cultura de la de la ciberseguridad.

Y por nuestra parte nada más, agradecerle de nuevo su presencia, que nos parece muy importante que el Gobierno de España también quiera colaborar a nivel autonómico con todas las regiones, también con la Comunidad de Madrid, para intentar difundir e implementar esa cultura en torno a la ciberseguridad, tan importante para nuestros ciudadanos. Muchas gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señoría. Señora Torija López, por el Grupo Parlamentario Más Madrid, es su turno.

La Sra. **TORIJA LÓPEZ**: Gracias, presidente. Quiero agradecer especialmente al compareciente no solamente que haya venido a hacer esta intervención, sino también su gran capacidad pedagógica para explicarnos algo que a priori parece siempre complejo de una manera tan sencilla, que creo que también es parte del trabajo que hay que hacer en la línea de lo que decía el señor Cepeda de trasladar a la sociedad que esto es una cosa que está aquí en nuestro día a día y que es importante que lo que lo tengamos en cuenta.

También quiero agradecer la flexibilidad que hemos tenido en el sentido de que no era la comparecencia que estaba registrada y bien porque hemos podido atender a otra persona que venía.

Voy a ir a algunas preguntas concretas. El asunto del régimen sancionador que ha comentado su señoría del Partido Socialista a nosotros también nos preocupa bastante; de hecho, era una de las enmiendas que planteábamos. A mí me gustaría saber si cuando esta normativa europea se trasponga a la normativa en España esto tendría repercusión directamente en la agencia. Esta sería una de mis preguntas.

Yo he defendido también en el grupo de trabajo la importancia de conocer los datos, y conocer los datos supone también conocer las amenazas; usted nos ha presentado este gráfico en tiempo real. Yo durante mucho tiempo he preguntado cuáles eran los datos de las ciberamenazas en la Comunidad de Madrid. En el grupo de trabajo, cuando hablaba de la importancia de conocer estos datos de manera

pública, pues había un pequeño debate, que es extensivo también a otras áreas del conocimiento, sobre si debemos señalar los delitos que se están cometiendo y lo que hacemos es promover que haya más delitos o, al contrario, si lo que estamos haciendo es concienciando. A mí me gustaría saber cuál es su opinión a este respecto, si debemos tener informes transparentes que hablan..., por supuesto teniendo la preserva de las infraestructuras críticas, que eso claramente no puede estar a la luz, ¿no?

Otra de las cuestiones que nos ha preocupado también y que hemos reflejado en las enmiendas es un poco la actualización tecnológica; es decir, entiendo que el universo en el que nos movemos en 2023 seguramente no se va a parecer nada al que vamos a vivir dentro de dos años, y estoy poniendo un margen de tiempo que podría ser seis meses o cinco años, porque al final estas leyes que hacemos pues duran en el tiempo, y esto de la actualización me preocupa bastante.

Sobre los sistemas de certificación, que usted ha hablado de que efectivamente la Comunidad de Madrid tiene más sistemas de certificación en empresas, digamos, privadas, me gustaría saber cómo se podría fomentar desde la Agencia que aumenten esos sistemas de certificación, cómo se podrían sumar, con ayudas, con formación o con alguna cosa así.

Querría saber también, a propósito de la cooperación del Estado con las comunidades autónomas, cuál es la diferencia que supone una comunidad autónoma que tiene agencia con respecto a una comunidad autónoma que no tiene agencia, para ver un poco, bueno, la necesidad, porque estamos en esto. Aunque me ha parecido traslucir que efectivamente ha puesto en valor la importancia de las comunidades autónomas que han desarrollado una agencia, querría saber un poco ese nivel de cooperación cómo funciona y si hay diferencias, que entiendo que alguna tiene que haber cuando hay agencia a cuando no la hay.

Otra pregunta que me gustaría hacer -que no sé si conoce el dato- es cuánta gente trabaja en el Incibe; lo digo porque una de las cosas que nos falta calibrar es cuántas personas van a trabajar en la agencia madrileña, que supongo que será algo que desarrollaremos con el tiempo. También el tema de los presupuestos; le agradezco mucho que nos haya dicho los presupuestos con los que cuenta el Incibe, que, por supuesto, no pueden ser los que tiene la agencia de la Comunidad de Madrid, pero habrá que trabajar también en esta línea.

Por último -discúlpeme, porque no he tomado bien el dato y me parecía muy importante-, usted ha hablado de un programa al que se habían suscrito ya Castilla y León y Andalucía... *(Rumores.)* Si pudiese detallarlo un poco más, porque he tomado alguna nota, me ha parecido muy interesante, pero me he perdido un poco en el detalle. Y nada más. Muchísimas gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señoría. Por el Grupo Parlamentario Popular, señor Arroyo tiene la palabra.

El Sr. **ARROYO PEREA**: Sí, buenos días. Gracias, presidente. Señor Barrio, muchísimas gracias por venir a la Asamblea de Madrid y aceptar la invitación para comparecer en esta comisión, y agradecerle también sus aplicaciones dadas al comienzo de su intervención.

Quisiera ponerle un poco en antecedentes de cómo ha sido el camino hasta llegar aquí. Como ya sabrá, en la legislatura anterior este proyecto de ley ya se presentó en la Cámara para su debate a la totalidad con devolución al Gobierno; en ese momento, y quizá por motivos políticos/electorales, fue rechazado por todos los grupos de la oposición, incluido Vox, aunque sí es cierto que la premura que había hace diez meses en aprobarlo es la misma que hay hoy en día. Y ya en esta legislatura, con una mayoría absoluta, ha vuelto a esta Cámara con la misma voluntad de acuerdo que había entonces, incluso con los mismos objetivos, que no eran otros que proteger a los ciudadanos, a las pymes e instituciones de futuros ataques, así como complementar su seguridad y educar en el buen uso de las tecnologías. Y fíjense en la importancia de la aprobación de este proyecto de ley: es la primera ley que vamos a aprobar en esta legislatura para una consejería que es pionera en España. Y, además, poner el acento en esta cuestión sitúa un poco el debate encima de la mesa de hacia dónde se dirige la sociedad actual y la obligación que tienen las Administraciones públicas de velar por los ciudadanos, sus empresas, Administraciones e infraestructuras críticas. Y, además, el terreno puramente económico: tiene un coste relativamente pequeño si lo comparamos con los beneficios que tendrá para la Comunidad de Madrid, porque, señorías, ¿qué precio tiene la seguridad de nuestros datos?, ¿qué precio tiene que nuestros hijos sepan a qué riesgo se pueden enfrentar cada vez que entran en la red? o ¿qué precio tiene que exista un organismo que nos ayude a resolver cualquier incidencia que nos surja en una infraestructura o en cualquier ente público? Pues yo creo que ese debería ser el debate y no otro. Además, como como he dicho, hablamos de un presupuesto de 1,5 millones de euros, frente a los más de 510 millones de euros destinados a los presupuestos de 2024 y que previsiblemente se aprobarán a finales de mes de diciembre.

Creo que esta ley tiene claros objetivos: uno de ellos -hablaba el señor Cepeda de ello- es la creación de esta cultura de ciberseguridad, porque qué sentido tiene tirarse al mar sin saber nadar ¿no? También crear confianza y seguridad en la Comunidad de Madrid; el motor económico de España no puede ni debe quedarse atrás en esta materia y menos en estos momentos cruciales en los que actuamos como muro -y este sí- frente a algunas decisiones políticas equivocadas. Y también ayuda para fomentar la implantación del desarrollo de la ciberseguridad en el ámbito empresarial. Además, en la parte educativa, difundiendo actividades y formación adaptada a diferentes sectores de la población para reducir esa famosa brecha digital que existe hoy en día en todas las comunidades autónomas. Y, además, todo indica que es una piedra que nos vamos a encontrar todos y que nuestra obligación es apartarla, digamos, y no saltarla. Y esto creo que no sería posible sin el ente objeto de creación en esta ley. La Agencia de Ciberseguridad de la Comunidad de Madrid será la encargada de engranar todas esas piezas, coordinándose con otras instituciones como el Incibe o el CNI, sin entrar en conflicto de competencias.

Y ahora hablemos un poco de las realidades que refuerzan la necesidad de aprobar este proyecto de ley. Según los datos del informe de criminalidad del año 2022 perteneciente al Ministerio del Interior, se produjeron casi 380.000 hechos delictivos en materia de ciberseguridad en toda España, la gran mayoría además de ellos en la Comunidad de Madrid y en Cataluña, 60.000 ciberdelitos por cada una de ellas, y además adelanta esta cifra: en los seis primeros meses de 2023 ya se han cometido más del 50 por ciento de los delitos cometidos en el año anterior, casi 220.000. Por recordar algunos

de los ataques -seguro que el señor Barrio además podrá dar buena cuenta de ello-, en julio de 2022 ataque de origen ruso al CSIC, que recuperó la normalidad tras quince días; noviembre de 2022, ataque al Consejo del Poder Judicial -me refiero a un ataque informático y no a lo que quiere hacer el señor Bolaños-; marzo de 2023, el Hospital Clínic de Cataluña sufre un ataque informático con cifrado de datos y bloqueo de acceso; octubre de 2023, tres hospitales públicos también de Cataluña con los mismos problemas, y, por no extenderme mucho más, Air Europa, Vodafone, Ayuntamiento de Sevilla o incluso la propia Telemadrid. Nadie está exento de esos ataques. Evidentemente, la creación de la Agencia de Ciberseguridad de la Comunidad de Madrid no implica la desaparición de estos delitos, pero sí que ayuda a afrontarlos si estos consiguen su objetivo y además ayuda a la ciudadanía y a las empresas a detectar y a desconfiar cuando reciben algún tipo de requerimiento o de información para cualquier tipo de tarea diaria en internet.

Miren, en el País Vasco, en los primeros seis meses del año, han aumentado en un 31 por ciento los ciberdelitos si los comparamos con el primer semestre de 2022, y un dato muy preocupante: el 89 por ciento de ellos son ciberestafas, 11.508, un 30 por ciento más que en el mismo semestre del año anterior. O incluso los ciberdelitos de carácter sexual, que parece que no se pone demasiado acento: 71 por ciento más. En Cataluña, aumento del 30 por ciento de los ciberataques en 2022 respecto al año anterior, con un aumento preocupante del 150 por ciento en el sector público; aumento de un 38 por ciento de los ataques de phishing mediante campañas de correo electrónico. Incluso las inofensivas smart TV que todos tenemos en casa, desde 2011 un aumento del 11 por ciento de un troyano. Ataques a la Universidad Abierta de Cataluña con cifrado de datos; Vall d'Hebron, filtrado de datos del Liceu, suplantación de la Administración pública catalana, ayuntamientos... Viendo esas tendencias, si lo llevamos al terreno de la Comunidad de Madrid, imaginen qué es lo que puede estar sucediendo si se reciben más de 60.000 ciberataques al año. ¿Cómo podemos explicar a los madrileños qué es lo que es LockBit, o Vice Society, o Black Basta, si no es con una agencia cercana a ellos en sus municipios? ¿Cómo podemos enseñarles a diferenciar entre protocolos de navegación seguros? ¿Cómo podemos ayudarles a identificar campañas de phishing y reducir la efectividad de estas? Señorías, no hay mayor vulnerabilidad en cualquier tipo de sistema que la acción por error de un ser humano, y es aquí donde la Agencia de Ciberseguridad de la Comunidad de Madrid pondrá el foco, capacitando y formando.

Y, ahora sí, señor Barrio, me gustaría realizarle unas preguntas. Coincido con la compañera en alguna de ellas, y es una de ellas es cómo ayuda el Incibe a las Administraciones locales, ¿les dota de algún tipo de material técnico o humano para ayudarles a protegerse de los ciberataques? ¿Cómo es la coordinación con las agencias de ciberseguridad catalana, vasca y valenciana? ¿Cómo es la coordinación entre distintas Administraciones en materia de ciberseguridad? ¿Cree que es positivo que todas las comunidades autónomas tengan su propia agencia de ciberseguridad? ¿Hay alguna causa de posible incompatibilidad entre el Incibe y la creación de la agencia de ciberseguridad en una comunidad autónoma? ¿Qué estructura cree que es la necesaria para una para una agencia de este tipo? ¿Cómo funciona el Incibe ante cualquier denuncia de cualquier ataque informático? ¿Nos puede explicar un poco con más detalle cuál es el trabajo que realiza el Incibe para capacitar a ciudadanos y empresas? Y por nuestra parte nada más, espero que tenga a bien responder alguna de estas cuestiones. Muchas gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señoría. Para contestación tiene la palabra el señor Barrio por un tiempo máximo de diez minutos. Si le parece, señor Barrio, le aviso cuando llegue al minuto diez y, de ahí en adelante, lo que usted estime; adelante.

El Sr. **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD** (Barrio Juárez): Muchas gracias, señor presidente. Muchas gracias, señores portavoces, no solamente por las preguntas, sino por el esmerado cuidado en el orden de los temas, porque también a nosotros nos supone un ejercicio de análisis y de reflexión continua sobre cómo explicar cada día mejor el trabajo que se está haciendo a nivel de servicio público.

Respecto a las primeras preguntas, el señor Cepeda hacía mención a la capacidad sancionadora; la capacidad sancionadora para nosotros es un instrumento absolutamente natural en lo que es la gestión de la ciberseguridad. Esta es una capacidad que hay que tener prevista; de alguna manera han ido dando pistas de hasta cuál puede ser el alcance: han hablado de la regulación de proveedores, han hablado del tema de capacitación de personas, de las responsabilidades en las que se incurren por parte de los usuarios... Si se fijan en uno de los ejemplos que puse, el del espionaje a los teléfonos móviles, ¿qué sucede si por imprudencia o por desconocimiento un empleado público está accediendo a información de tipo sensible en su teléfono particular y lo pone a disposición en este caso de terceros países o de mafias o del cibercrimen precisamente porque no ha cumplido con las buenas prácticas en materia de gestión de datos personales o de gobierno público de la Administración? Por lo tanto, en todo lo que sean materias reguladoras que la agencia, imagino, coordinará a nivel de los diferentes departamentos implicados en materia de tecnologías de la información tiene que caber en qué medida se van a aplicar mecanismos correctores y también de regulación a efectos de prever que los proveedores o que los empleados públicos directos, o, en este caso, asistencias técnicas, hagan la debida observancia de lo que deben conocer y deben de aplicar. Por lo tanto, en ese sentido, creo que es una capacidad natural que este tipo de organismos que tienen esa capacidad de gestión de coordinación que van a tener que disponer, adaptado evidentemente a las necesidades, en este caso, de la gestión.

Respecto a los municipios, estamos hablando de economías de escala. En este caso, circunscribir a menos de 20.000 o más de 20.000..., no se trata tanto, sino que, si se despliegan sistemas de estrategias que conduzcan a un buen sistema de detección temprana, de monitorización, de soporte en el ámbito de la Administración, evidentemente que haya accesibilidad para cualquier tipo de Administración pública radicada en la Comunidad de Madrid, en el ámbito local, yo creo que es algo que evidentemente va a ser también natural, incluso cuando se comparten servicios por diferentes ámbitos de Administración; estoy pensando en centros de Atención Primaria, sanitaria, por ejemplo, y su relación con las Administraciones locales o con los sectores privados, en los que también cada vez más -y ahora haré referencia a ello- van a tener que lidiar, como puede ser, por ejemplo, el de la distribución farmacéutica, el sistema de transportes, de logística, etcétera, donde las competencias están en el ámbito autonómico. Es muy difícil hacer una limitación de que esto pueda afectar a solo municipios hasta 20.000 o que evidentemente esto sea... Otra cosa es cómo se establezca el mecanismo de

coordinación, que ahí desconozco y que evidentemente tienen que ser conscientes de que se va a producir esa casuística.

Respecto al ámbito de la trasposición de la directiva NIS2, estamos en el proceso de elaboración del nuevo real decreto de seguridad de las redes y sistemas de información para adaptarlo a la directiva de la Unión Europea 2022/2555, relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión Europea. Muy resumidamente, la nueva directiva comunitaria consolida lo que es una cesión de soberanía de los Estados al ámbito de la Comisión Europea y de la Unión en materia de regulación en materia de mercado interior; esto establece que todos los sistemas de certificación de requisitos de ciberseguridad se coordinan mediante estándares y legislación ad hoc que se debate y se aprueba en el seno de la Unión Europea. Esto es algo que supuso en el 2019 una de las mayores transformaciones en lo que es traspaso de soberanía nacional en materia de política industrial. Con la nueva directiva se amplía el alcance de toda esta materia de regulación de mercado interior: vamos a pasar de 18 sectores a 32; esto quiere decir que vamos a tener que regular sectores que hasta ahora no tenían la clasificación de operador esencial, como el mencionado de transporte, por ejemplo, o paquetería, que entra dentro de los nuevos sectores regulados, y que evidentemente también en la transferencia de competencias las autonomías van a tener que incrementar sus niveles de supervisión y de regulación a nivel de estas operaciones y mucho más en lo que afecte a la provisión de servicios públicos de la comunidad. Nuestra previsión es que, de aproximadamente 500 operadores esenciales que abordamos ahora el servicio en coordinación con el Ministerio del Interior, pues posiblemente podremos llegar en dos o tres años a entre 3.000 y 5.000 operadores, es decir, entidades, el 90 por ciento de ellas privadas, que están sujetas a la nueva legislación en materia de obligación de adaptar todos estos sistemas que yo resumía con el ciclo de estrategia de ciberseguridad, auditoría anual y un seguimiento muy escrupuloso de que aplican estándares; estándares que hasta ahora se centraban en la certificación de sistemas.

El Esquema Nacional de Seguridad, para que ustedes lo entiendan, es un sistema que certifica el sistema, cómo se gestionan todos esos activos: computadoras, dispositivos móviles, servidores... Eso se tiene que configurar con unas especificaciones técnicas; eso es certificación de sistemas. La nueva directiva va a abrir también a la obligatoriedad de certificar sistemas de gestión de la ciberseguridad; el más conocido es la ISO 27001 y que introduce básicamente sistemas de mejora continua, es decir, que haya toda una gestión de planificación y de evaluación continua de que se está cubriendo todo el ciclo de vida de la ciberseguridad. Esto es un cambio de paradigma, que también aquí va a suponer a las Administraciones cómo transferir eso a ámbitos como, por ejemplo, el de la contratación pública, donde habrá que establecer para qué proveedores tienen que cumplir con qué estándares, y no será lo mismo un proveedor que entre en el sector hospitalario de la Comunidad de Madrid que el que se adecue, por ejemplo, a temas de inspección técnica de vehículos en el caso de los vehículos, que ya van a ser todos conectados a internet y que también entrará dentro de sus ámbitos competenciales. Por lo tanto, el reto que vamos a tener es que, en los próximos tres o cuatro años, seguramente, ojalá, pues seguiremos hablando en este foro sobre la importancia de continuar avanzando en materia de adaptación de la regulación autonómica y de adecuación a esta directiva y la correspondiente adecuación a la legislación nacional.

En materia de coordinación, atendiendo a las preguntas de la señora portavoz del grupo Sumar, decirle que evidentemente concienciación, coordinación con delitos..., esto es un ámbito esencial. Para que se hagan una idea, de las campañas de publicidad institucional del Gobierno de España de los últimos tres años la segunda más importante en dotación económica ha sido la campaña de ciberseguridad que hemos gestionado desde el Instituto Nacional de Ciberseguridad. Se está haciendo un máximo esfuerzo por llevar hasta el último ciudadano, hasta el último colectivo vulnerable, los menores, las personas mayores, dependientes..., también las muy pequeñas empresas, los autónomos, los profesionales..., la importancia de tener un nivel de responsabilidad y de conocimiento suficiente para estar prevenidos ante los crecientes riesgos del uso de la tecnología y de los accesos a los servicios digitales. ¡Por supuesto! Y esto solo se consigue también, de nuevo, incrementando la cooperación con esos servicios de proximidad que constituyen en este caso las Administraciones autonómicas y locales y, en particular, es el propósito del desarrollo de capacidades que persigue el programa Retech.

El programa Retech es un programa de lanzamiento por el Ministerio de Economía y Transformación Digital que ha permitido suscripción de acuerdos con quince comunidades autónomas y que hasta 2026, a través de Incibe, invertimos 152 millones de euros: 75 por ciento de aportación del mecanismo de recuperación y resiliencia, 25 por ciento por las comunidades autónomas. Las comunidades autónomas se han organizado en tres grupos; el que mencionaba era el nodo 1, en el que está la Comunidad de Madrid, donde nosotros aportaremos hasta 15 millones de euros por comunidad en este caso y 5 millones en el caso de la Comunidad de Madrid, para poder desplegar acciones que contribuyan a desarrollar esas capacidades, que van desde el ámbito de la concienciación, la generación de empleo, el elevar el nivel de capacidad de nuestro tejido productivo en la Comunidad de Madrid y, por supuesto, la coordinación con todos los estamentos a nivel territorial que permitan tener cada vez sistemas de mayor resiliencia.

La experiencia, en este caso, con las comunidades de colaboración siempre ha conducido a resultados extraordinarios porque nos permite mejorar nuestro nivel de recepción de información de cuál es el nivel y cuál es la situación. Todos estos eventos que veían en pantalla..., es materialmente imposible gestionar de manera centralizada toda la casuística y, lo que es más importante, solo el propietario de los dispositivos tecnológicos puede hacer una óptima gestión del nivel de configuración de la seguridad y parametrizar cuáles deben ser los elementos que nos hagan establecer anomalías o mejorar la prevención. Y no tiene nada que ver un sistema de un hospital con el de una escuela pública, con el de esta propia Asamblea, y eso nadie mejor que los responsables de tecnologías.

La ventaja de tener una agencia es que precisamente optimiza la coordinación; esto no quiere decir que tenga que tener un número determinado de personas para gestionar, pero sí que permite coordinar con los propietarios de todos esos sistemas de tecnologías, que sí están distribuidos en las decenas de miles de activos que gestionan, en este caso, la Administración autonómica. Y a lo mejor la agencia tendrá que coordinarse con los directores de TI de cada una de las consejerías, de cada una de las agencias, a nivel de coordinación con el caso de proveedores... Por supuesto, todos los departamentos están concernidos de una manera u otra, porque estamos hablando de la ciberseguridad

que va desde el tema de la privacidad, de la protección de datos personales, hasta los delitos, que pueden constituir a lo mejor el 2 o el 3 por ciento del total de los incidentes de ciberseguridad. No confundamos, los ciberdelitos, evidentemente, son la cara visible, pero en la mayoría de los casos estamos hablando de incidentes que no se van a poder someter a una persecución criminal porque a lo mejor el ciberataque está ubicado en un tercer país con el que no tenemos ningún tipo de acuerdo ni posibilidad de cooperación. Por lo tanto, tenemos que asumir que la "policialización" -valga la palabra- de la ciberseguridad solo va a tener un alcance en ese ámbito restringido del ámbito del ciberdelito y ahí es donde la directiva comunitaria precisamente incide: que la ciberseguridad depende fundamentalmente de nuestra capacidad como reguladores para que los agentes privados, en cuya responsabilidad recae el nivel de resiliencia, se adecuen a una debida observancia de buenas prácticas y de normas de ciberseguridad. Ese es el gran reto y esa es la gran aportación que puede tener una agencia. ¿Todas las comunidades tienen que tener agencia?

El Sr. **PRESIDENTE**: Señor Barrio, a partir de ahora, lo que considere.

El Sr. **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD** (Barrio Juárez): Gracias. Quizás no todas, las agencias... Nuestra experiencia con otras comunidades autónomas. Nosotros tenemos..., uno de nuestros servicios es el 017, que funciona a 24/7 todo el año, atención telefónica y mediante sistema de mensajería de 8 de la mañana a 11 de la noche, y cualquier ciudadano, cualquier empresa, pyme, autónomo..., puede acceder a nosotros. Estamos gestionando del orden de 3.000 usuarios semanales, con una plantilla dedicada de unas 50 personas; esperamos llegar a 80 personas en dos años a nivel que está subiendo el volumen de ciudadanos víctimas de casos de fraude bancarios, de ataques y de estos problemas que veíamos antes en el mapa de eventos. Las agencias nos han trasladado que este servicio cubre sobradamente y no están desplegando servicios alternativos. En este caso hay un nivel de coordinación que facilita la mayor eficiencia en la gestión de los recursos públicos. Esto está permitiendo, que con agencia catalana, por ejemplo, con quien mantenemos una colaboración activa, ya nosotros no vamos a redundar en este sistema de atención al ciudadano, vamos a incidir en servicios de coordinación y de prevención en lo que es activo. Yo creo que esto es una ventaja porque nos permite optimizar ese nivel de atención a las necesidades particulares.

En el conjunto de Incibe hay unas 310 personas trabajando, de las cuales 155 son personal propio y el resto, como en el caso de las personas que atienden al 017, son personas a través de asistencias técnicas. Insisto, no hay una traslación, no hay una regla de tres para dimensionar los recursos, sobre todo es la capacidad de coordinación con los que ya existen en materia de responsabilidad de nuevas tecnologías. Y ahí es donde una agencia optimiza porque puede asignar prioridades y puede facilitar la delegación de funciones y limitarse a labores de supervisión y coordinación, con la ventaja de que ya dispone de toda la serie de herramientas que le van a facilitar, en este caso, el Centro Criptológico Nacional y el propio Incibe, para poder gestionar de manera lo más rápida posible la gestión de los incidentes en todos sus ciclos de vida.

El conflicto de competencias, siempre y cuando no excedamos el ámbito de coordinación nacional e internacional, que, por motivos también de eficiencia, no solamente de legislación, tienen que recaer en autoridades nacionales... Yo creo que hay un escenario más de coordinación y de buena voluntad en un sector, el de la ciberseguridad, en el que a los responsables, que normalmente que venimos del ámbito técnico, lo que nos prima es que seamos capaces de prevenir, de prepararnos y de responder adecuadamente. Yo creo que, afortunadamente, en el caso de la ciberseguridad, es una materia de Estado, es una materia en la que todos coincidirán conmigo en que no tiene por qué haber un espacio de conflicto, porque todos coincidimos en la enorme importancia y esto ha preservado la normalidad en las relaciones a nivel autonómico.

En cuanto al resto de preguntas, hablaban, sobre todo, desde el punto de vista de las capacidades. Nosotros podemos crecer indefinidamente y nunca va a ser suficiente. Posiblemente todos los servicios públicos que podamos articular se nos van a quedar escasos por el nivel de dependencia de lo digital. El 22 por ciento del producto interior bruto español depende de la conectividad digital. Y ustedes tuvieron ocasión de vivirlo durante el confinamiento: fue gracias a que teníamos un magnífico sistema de telecomunicaciones y de servicios digitales que España pudo pasar de la noche a la mañana en materia de continuidad operativa y sin caída de los sistemas, sin problemas de disponibilidad y manteniendo la normalidad para nuestras ciudadanas y ciudadanos. Por lo tanto, yo creo que a nadie se le escapa que cada vez más tenemos que acometer la obligatoriedad de gestionar todas estas capacidades.

Y, sobre todo, permítanme incidir, estamos hablando de esa falta de fronteras que separen lo público de lo privado, y ahí es donde entra lo que son organismos de representación, como en este caso la Asamblea. Yo creo que es muy importante la capacidad de diálogo permanente de proximidad que hay con agentes que tienen diferentes niveles de preparación para este cambio tecnológico. En el caso de los ayuntamientos muy pequeños, evidentemente, hay graves carencias. No se trata solo de que haya un organismo que atienda el incidente, sino de que trabajemos en todo ese ciclo de capacidades, que empieza por esa pyme que es la que vende el ordenador en el pueblecito a esa Administración local, y que nos aseguremos de que llegue la banda ancha y que nos aseguremos de que todos los sistemas están perfectamente preparados para que no tengan que sufrir ningún tipo de daño los ciudadanos de esa remota Administración local. Por lo tanto, hay que mantener ese nivel de pie firme en la base local y de proximidad con los agentes públicos y privados, y nadie mejor que, en este caso, una Administración autonómica. Muchas gracias.

El Sr. **PRESIDENTE**: Muchísimas gracias, señor Barrio. Lo primero, agradecerle, tanto de parte de esta presidencia como de esta Mesa y de la comisión, su presencia aquí hoy y decirle que esperamos tenerle pronto nuevamente; información importante que nos ha facilitado el día de hoy y, bueno, seguir trabajando, así que muchísimas gracias.

El Sr. **DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD** (Barrio Juárez): Muchísimas gracias y mucha suerte.

El Sr. **PRESIDENTE**: Vamos a hacer un pequeño receso de cinco minutos y llamo a portavoces a Mesa.

(Se suspende la sesión a las 12 horas y 7 minutos).

(Se reanuda la sesión a las 12 horas y 20 minutos).

El Sr. **PRESIDENTE**: Muy bien, entonces ya iniciamos, retomamos, sí.

Deliberación y votación del Dictamen al PL-1(XII)/2023 RGEP.11518, de creación de la Agencia de Ciberseguridad.

Muy bien; entonces, admitimos la enmienda técnica y las transaccionales, ¿no? *(Pausa.)* Muy bien. Les traslado que la Mesa, con el parecer unánime de los portavoces, acordó la no inclusión de designación de ponencia en el seno de la comisión con la voluntad de agilizar en la mayor medida la tramitación de este proyecto de ley debido a su relevancia; por consiguiente, corresponderá a la comisión la aprobación del dictamen sin texto previo del informe de ponencia. Asimismo procede informar a los miembros de la comisión de que la Mesa, oídos los portavoces de los grupos parlamentarios, acordó ordenar el presente debate con un turno único de intervención de cinco minutos, de menor a mayor, para que los portavoces de los grupos defiendan sus enmiendas o fijen sus posiciones; concluido el debate y a resultas del mismo tendrán lugar las votaciones.

Al respecto de ello, informo también de que se han formalizado ante esta Mesa enmiendas transaccionales a las enmiendas 2, 4, 6, 16, 20, 31, 36 y 37 del Grupo Parlamentario Socialista, por el Grupo Parlamentario Socialista y el Grupo Parlamentario Popular, a las enmiendas 1, 5, 6, 18 y 25 por el Grupo Parlamentario Más Madrid y el Grupo Parlamentario Socialista, a las enmiendas transaccionales 1 del Grupo Socialista... (Pausa.) ¿Más Madrid y Grupo Popular? (Rumores.) (Pausa.) Venga, nuevamente. A las enmiendas 2, 4, 6,16, 20, 31, 36 y 37 del Grupo Parlamentario Socialista; a las enmiendas 1, 5, 6, 18 y 25 del Grupo Parlamentario Más Madrid; a las enmiendas transaccionales 1 del Grupo Socialista y 2 del Grupo Más Madrid; a la exposición de motivos, primero..., perdón, 1, tras primero, 12 del Grupo Socialista y 7 del Grupo Parlamentario Más Madrid, ambas a la exposición de motivos, 1, párrafo decimotercero; y 21 del Grupo Socialista y 10 del Grupo Más Madrid al artículo 3.2 letra k). Todas ellas han sido admitidas a trámite por esta Mesa, de conformidad con lo establecido por el artículo 147.2 del Reglamento de la Asamblea.

Asimismo, a tenor de las observaciones expuestas en informe jurídico emitido por los servicios jurídicos de la Asamblea, el Grupo Parlamentario Popular ha presentado una enmienda técnica al artículo 8 del texto del proyecto de ley. Esta enmienda también ha sido admitida a trámite por la Mesa de la comisión en virtud del precitado artículo reglamentario.

Expuesto lo anterior, sin mayor dilación, damos comienzo al debate. En primer lugar, tiene la palabra, en representación del Grupo Parlamentario Vox, la señora González Moreno por un tiempo máximo de cinco minutos.

La Sra. **GONZÁLEZ MORENO**: Muchas gracias. Bueno, como todos saben, Vox presentó una enmienda a la totalidad de este proyecto de ley y no ha presentado enmiendas parciales. Seguimos considerando que no hay una diferencia entre las comunidades que van a contar con la Agencia de Ciberseguridad y las que no. Y, por lo tanto, en este en este grupo de enmiendas nos vamos a abstener. Muchas gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señoría. Por parte del Grupo Parlamentario Socialista tiene la palabra el señor Cepeda García de León.

El Sr. **CEPEDA GARCÍA DE LEÓN**: Muchas gracias, presidente. Bien, por parte de nuestro grupo, del Grupo Socialista, queremos, sobre todo, poner encima de la mesa que nos queremos congratular por el trabajo de equipo de todos los grupos parlamentarios; me parece que ha sido muy importante. Yo quiero reconocer abiertamente la actitud también constructiva del Grupo Parlamentario Popular, que, con una mayoría absoluta en esta Cámara, ha sido capaz de tener en consideración también las enmiendas del resto de los grupos parlamentarios, en concreto del Grupo Parlamentario Socialista, que ha hecho casi cuarenta enmiendas. Técnicamente, además, hemos intentado acercar este proyecto, que es un proyecto, como acabamos de observar con el compareciente anterior, muy importante, que nos parece que es estructural de cara a la digitalización cada vez más de los servicios públicos, pero también del día a día de la gestión de los ciudadanos madrileños. La apuesta de mi grupo es intentar garantizar cada vez más la seguridad de los madrileños, también en el mundo digital. Y en ese sentido van las prácticamente cuarenta enmiendas que mi grupo ha puesto encima de la mesa, muchas de ellas que han sido consideradas, como decía, por el grupo mayoritario de la Cámara y otras también transaccionadas con el Grupo Más Madrid, que también ha hecho un esfuerzo y que también queremos felicitar, lógicamente, el trabajo que ha venido desarrollando para acercar entre todos posiciones y hacer de este proyecto un proyecto global y colectivo para todos los madrileños.

Es verdad que ha habido algunas -y voy a incidir un poco aquí- que no han sido aprobadas, que no han sido consideradas por parte del Partido Popular; bien, perfecto. Es verdad que nosotros hemos intentado también con nuestras enmiendas acercar un modelo más amplio respecto, por ejemplo, a la dirección de la agencia, y, en este sentido, les voy a anunciar que mi grupo va a seguir manteniendo vivas este tipo de enmiendas, este grupo de enmiendas donde se habla de un modelo y nosotros queremos insistir en ese modelo que, bajo nuestro prisma, debería mantener la agencia.

Vamos a mantener también vivas algunas enmiendas que tienen que ver, por ejemplo, con la capacidad sancionadora de futuro. Bueno, simplemente que quede ahí también constancia, como un modelo de trabajo que, como hemos escuchado también hace tan solo unos minutos, debe seguir desarrollándose como un objetivo por parte de la agencia. De la misma manera que la consideración también a ir incidiendo en el futuro tecnológico, que ya es una realidad hoy; estoy hablando de la de la

realidad de la computación cuántica. Nos parece que es importante que la agencia tenga en consideración -incluso diría yo que el conjunto de la consejería, pero, bueno, hablamos de la agencia de ciberseguridad- cómo la computación cuántica nos va a colocar ante nuevos retos inmediatos y, por qué no decirlo, la inteligencia artificial. Yo sé que el consejero está también empeñado en la puesta en marcha de un futuro instituto, pero la inteligencia artificial es un elemento clave también en la gestión de las nuevas ciberamenazas y, sobre todo, los grupos de ciberdelincuentes, que la están utilizando, obviamente, a la contra. Y yo creo que la Agencia de Ciberseguridad también tiene que tener en consideración cómo la inteligencia artificial puede ser ese gran motor de ciberamenazas del que nos tenemos que proteger, ¿no?

Y, por último, el tema de los ayuntamientos. Vamos a mantener también vivas las enmiendas relativas a los ayuntamientos, como decía, como un toque de atención, donde efectivamente las competencias están perfectamente puestas en la ley, y yo también entiendo la posición en este sentido del Grupo Popular de no aceptarlas, pero, digamos que, como modelo, pues sí que es verdad que nosotros vamos a intentar, al menos en el debate, de cara al pleno, el poder elevar esta situación y esta circunstancia que nos parece que es un compromiso cierto; es decir, por parte del Grupo Socialista estamos comprometidos con la Administración local, que nos parece que es el gran foco, el gran agujero de la ciberseguridad del conjunto de las Administraciones públicas y, en este sentido, vamos a seguir levantando -entre comillas- esa bandera. Porque, como hemos estado explicando, al final los proveedores de servicios digitales están hoy generando, digamos, esa cobertura desde el punto de vista del trabajo institucional, también a los grandes municipios, a los grandes, a los pequeños y a los medianos, y en ese sentido estamos seguros que la Agencia de Ciberseguridad va a tener mucha tarea y mucho trabajo.

Pero, en términos generales, como al final el objetivo colectivo es que esto sea una realidad y que haya una nueva estructura dentro de la Administración autonómica para colaborar con la Administración local por abajo y con la Administración General del Estado por arriba, insisto, humildemente hemos intentado hacer ese trabajo para aportar lo mejor y que al final este proyecto sea una realidad para todos los madrileños, que yo creo que es el objetivo. Me parece -y con esto ya acabo- que, si somos capaces de sacarlo hacia adelante, pues estaremos haciendo también un ejercicio de que la política y los políticos, también en Madrid, servimos para algo. Muchas gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señoría. Por el Grupo Parlamentario Más Madrid tiene la palabra, señora Torija.

La Sra. **TORIJA LÓPEZ**: Gracias, presidente. Yo quería empezar haciendo ese agradecimiento extensivo a lo que han supuesto las dinámicas de trabajo en esta comisión, que ha hecho posible que hoy estemos aquí y donde vamos a trabajar, donde vamos a votar una ley, yo creo, en un porcentaje muy importante diferente. Creo que requiere un agradecimiento especial la letrada de la comisión, que, como sabemos a las cuatro de la mañana todavía estaba recabando información.

Creo que uno de los papeles que tenemos en la Asamblea de Madrid como diputados es la parte legislativa y creo que -y quiero reseñarlo aquí, porque estamos en un momento en el que han entrado varias leyes en la Asamblea de Madrid- es un procedimiento que hay que cuidar especialmente.

Esta ley no ha contado con una ponencia de ley, que nos habría hecho el trabajo más sencillo, hemos tenido que organizarnos en un grupo de trabajo que en realidad no ha existido. Bueno, efectivamente, como todos hemos empujado, tenemos un buen resultado, pero creo que hay que poner los cauces para que esto no suceda y que todos los procedimientos legislativos, que al final es el trabajo que realmente incide en la vida de los madrileños, se hagan de la manera adecuada; los que podemos hacer, ya hay otros que reglamentariamente, como hemos podido ver hoy y ya sabíamos con anterioridad, son más difíciles de modificar. Es decir, a mí me sigue pareciendo ilógico que escuchemos al compareciente cuando tenemos la ley prácticamente cerrada y no cuando estamos en el proceso de enmiendas; eso es verdad que sería algo más difícil de modificar, pero no la generación de ponencias. Quiero hacerlo notar porque, bueno, estamos a las puertas aquí, a final de año, y este procedimiento... Entonces, las urgencias yo creo que lo que hacen es hacer peores leyes y estamos aquí para hacer mejores leyes.

En ese sentido, nosotros presentamos una enmienda a la totalidad hace pocas semanas en el pleno de la Asamblea. Yo sacaba un desplegable con un porcentaje de parecido del texto legislativo entre lo que se había presentado en el mes de febrero y el texto de la ley; entonces, decía que el porcentaje era un 98,9 por ciento de igualdad. Aunque ahora mismo todavía no tenemos el texto definitivo cerrado, pero un poco los cálculos que he podido hacer con todo el trabajo que se ha hecho me permiten decir que la ley ha cambiado en un 40 por ciento y que si una ley ha cambiado en un 40 por ciento es porque se ha hecho un trabajo en ese sentido que hay que poner en valor.

Efectivamente, como ha dicho el señor Cepeda, hay muchas cosas en las que hemos transaccionado directamente con el Partido Popular y algunas con el Partido Socialista. Hay enmiendas que han sido rechazadas, pero que el espíritu de la propia enmienda estaba en parte de la de las consideraciones jurídicas o de las consideraciones técnicas y, aunque la enmienda como tal ha sido rechazada, el espíritu sí que se incorpora a la ley. Así que yo creo que el trabajo que hemos hecho desde mi grupo parlamentario con 25 enmiendas es bastante notable; aun así, hay algunas de ellas en la línea de lo que ha dicho hoy el compareciente: lo que tiene que ver con el régimen sancionador o algunas cuestiones de transparencia y publicidad, y nosotros, por supuesto, la cuestión de la paridad, que para nosotros es muy importante, también la mantendremos, mantendremos esas enmiendas vivas para para el pleno.

No puedo dejar de hacer una alusión al partido Vox, porque me resulta sorprendente que en lo que es el trabajo parlamentario no haya opinado en ningún momento sobre nada, independientemente de que pueda votar que no a una ley. Hemos vivido procedimientos legislativos en la legislatura anterior y uno puede estar en contra de una ley y, aun así, a sabiendas de que esa ley se va a aprobar, trabajar en la mejora de la ley, que, como digo, es la mejora para las madrileñas y los madrileños. Así que, bueno, quería hacerlo notar. Y nada más. Gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señoría. Para concluir el debate, en representación del Grupo Parlamentario Popular, señor Navarro, tiene la palabra.

El Sr. **NAVARRO MORALES**: Gracias, presidente. Bueno, yo quería casi hablar hoy más en la parte personal que en la parte como como portavoz. Muchos de nosotros -no sé si incluso todos- somos nuevos en esta Asamblea, así que nos enfrentamos a la primera ley de la legislatura y para nosotros era realmente un reto esa responsabilidad de la que estábamos hablando de estar a la altura y de tener la oportunidad de mejorar la vida y, en ese caso, la protección de nuestros ciudadanos. Entonces, en primer lugar, vaya por delante el gracias. Ayer lo hablábamos el portavoz adjunto y yo, realmente hemos disfrutado todo el procedimiento legislativo y todo el procedimiento de la ley, y gracias a todos los portavoces y a todos los miembros de la comisión por lo fácil que lo habéis hecho. El tono creo que debe ser un ejemplo en un futuro para próximas leyes, porque el tono siempre ha primado por encima de todo, la responsabilidad que teníamos de cara a los madrileños. Gracias también a la letrada -me sumo-, el trabajo ha sido increíble y los que sabemos las horas que le has dedicado y a qué hora pues, bueno, creo que es de agradecer lo fácil que nos lo has puesto.

Como decía, era nuestra primera ley para muchos de nosotros que somos nuevos en la Asamblea, en una consejería que también es nueva y que es innovadora en el resto de España, que es la Consejería de Digitalización, y también para ellos una ley..., muchos de los políticos que hay allí, que tienen esa responsabilidad de llevar la consejería adelante, también nuevos en esas lides. Así que, bueno, creo que esa ilusión por hacer algo que realmente sirva y que realmente se pueda aterrizar en el ciudadano, en las empresas, en los ayuntamientos, y que les podamos ayudar, creo que se ha notado elevando el tono y elevando la responsabilidad que teníamos por encima de las siglas políticas.

Lo que hablabais hace un momento, hace diez meses fue imposible, por los motivos que fuera, sacar adelante esta ley; a día de hoy, por lo que hemos hablado, contará con un amplio apoyo y es una pena que, al igual que nosotros hemos disfrutado mucho en esta parte de modificar la ley y mejorarla con las aportaciones de todos los partidos políticos y de la letrada, otro grupo, Vox, no haya podido disfrutarlo tanto y haya sido el no por delante. Creo que, si realmente se hubieran remangado, aunque fueran a votar que no por los motivos que fuera, hubieran trabajado, hubieran apoyado esa ley y hubieran hecho propuestas, pues seguramente la portavoz, que también es nueva como nosotros, pues lo habría disfrutado mucho más de lo que lo ha hecho.

Ese texto al final va a ser la herramienta ideal para ayudar a los ayuntamientos, de momento, a los más pequeños, a los de menos de 20.000 habitantes, que realmente son los que menos medios materiales y, sobre todo, humanos tienen a disposición. Y, como bien ha dicho el presidente del Incibe -que desde aquí nuestro agradecimiento porque la exposición ha sido muy pedagógica y muy positiva-, ayudar también a las empresas y a los madrileños.

Sin duda, el trabajo de las enmiendas, de las 64 enmiendas que se han debatido en los diferentes órganos, y el nivel de detalle al que creo que hemos llegado con esas enmiendas sin duda

han enriquecido mucho el texto; lo ha enriquecido y lo han actualizado, porque, como hemos hablado, era un texto de hace unos meses que estaba pendiente de aprobar.

Y, bueno, para terminar, mi portavoz adjunto lo ha dicho hace un momento: ¿qué precio tiene la seguridad de nuestros hijos?, ¿qué precio tiene la seguridad de las empresas?, ¿qué precio tiene la seguridad de las Administraciones? Lo digo yo, que sufrimos, siendo concejal de Informática del Ayuntamiento de Arroyomolinos, un ataque informático en plena pandemia debido al teletrabajo, justo a la semana. Entonces, ¿qué precio tuvo para el Ayuntamiento de Arroyomolinos la pérdida de información que sufrimos, además, en ese momento tan concreto? Seguramente, solamente en un ciberataque, en ese que voy a poner como ejemplo, el que sufrí en mis carnes, será superior a 1,5 millones de euros, que es en lo que está estimado el presupuesto de la agencia. Como bien sabéis, hemos rechazado las propuestas del PSOE de ampliar más la estructura porque queríamos empezar con una estructura más humilde, más más pequeña, con un presupuesto de solo 1,5 millones de euros, que creo que el primer día de funcionamiento de esta agencia se va a haber visto amortizado por la cantidad de ataques que podamos parar o esa ayuda que podamos ofrecer a empresas, ciudadanos y ayuntamientos.

Así que, sin más, acabo como como empecé, con un gracias en mayúscula por esas aportaciones y un gracias también a nivel personal, porque creo que los portavoces y nuestros equipos en el trato personal lo hemos puesto muy fácil y también es de agradecer, y a la letrada y a la Mesa pues igual, un agradecimiento en mayúsculas. Gracias.

El Sr. **PRESIDENTE**: Muchas gracias, señoría. Señorías, concluido el debate, vamos a proceder a las votaciones. Les comunico que la votación ordinaria se va a realizar por bloques de tipos de enmiendas y, en su caso, por grupo parlamentario, sin perjuicio de que algún grupo solicite votación separada de alguna o algunas enmiendas, como se convino en la última Mesa y Portavoces por unanimidad, y se procederá, conforme a lo dispuesto en el artículo 124.1 del Reglamento, alzando la mano, en primer lugar, quienes aprueben, seguidamente los que desaprueben y finalmente quienes se abstengan.

Esta presidencia ha entendido que por parte del portavoz del Grupo Parlamentario Socialista se retiraban sus enmiendas números 22 y 32, ¿es así? *(Pausa.)* Por parte de la portavoz adjunta del Grupo Parlamentario Más Madrid se retiraban sus enmiendas números 3 y 15, ¿es así? *(Pausa.)* Muy bien.

Bien, considerando todo lo anterior, esta presidencia llama a votación. En primer lugar, votamos las enmiendas transaccionales presentadas a las enmiendas 2, 4, 6, 16, 20, 31, 36 y 37 del Grupo Parlamentario Socialista. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* Muy bien. Sí, muy bien. El resultado la votación ha sido: 16 votos a favor, cero en contra y 1 abstención. En consecuencia, queda aprobada.

En segundo lugar, votamos las enmiendas transaccionales presentadas a las enmiendas números 1, 5, 6, 18 y 25 del Grupo Parlamentario Más Madrid. ¿Votos a favor? *(Pausa.)* Igual, muy

bien. ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* Pues el resultado de la votación ha sido: 16 votos a favor, cero en contra y 1 abstención. En consecuencia, queda aprobada.

En tercer lugar, votamos la transaccional a las enmiendas 1 del Grupo Socialista y 2 del Grupo Más Madrid, la transaccional 12 del Grupo Socialista y 7 del Grupo Más Madrid y la transaccional a las enmiendas 21 del Grupo Socialista y 10 del Grupo Más Madrid. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 16 votos a favor, cero en contra y 1 abstención. En consecuencia, queda aprobada.

Seguidamente votamos las enmiendas al proyecto de ley formalizadas por el Grupo Parlamentario Socialista no retiradas y no afectadas por las transaccionales; esto es, enmiendas 3, 5, 7, 8, 9, 10, 11, 13, 14, 15, 17, 18, 19, 23, 24, 25, 26, 27, 28, 29, 30, 33, 34, 35, 38 y 39.

El Sr. **NAVARRO MORALES**: Señor presidente, aquí solicitamos la votación separada, por favor.

El Sr. **PRESIDENTE**: Muy bien, solicitan votación separada. A ver, pues entonces vamos a votar primero... *(Rumores.)* ¡Claro, claro!

El Sr. **NAVARRO MORALES**: Tenemos intención de votar a favor -discúlpeme- 3, 5, 7, 8, 9, 10, 11, 18, 27 y 34.

El Sr. **PRESIDENTE**: Está bien. Muy bien, solo por aclarar, se solicita votación separada de las enmiendas 3, 5, 7, 8, 9, 10, 11, 18, 27 y 34. Muy bien. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* Muy bien. El resultado de la votación ha sido: 16 votos a favor, cero en contra y 1 abstención. En consecuencia, queda aprobada. *(Pausa).*

Votamos, a continuación, las restantes enmiendas del Grupo Socialista no retiradas y no afectadas por las transaccionales; esto es, las enmiendas 13, 14, 15, 17, 19, 23, 24, 25, 26, 28, 29, 30, 33, 35, 38 y 39. ¿Votos a favor? *(Pausa.) (Rumores.)* Estas son las del Grupo Socialista. Perdón, perdón, es que llevamos aquí un leve retraso. *(Pausa.)* Ahora falta ¿en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* Muy bien. 6 votos a favor, 10 votos en contra y 1 abstención. Con lo cual, se rechaza.

Procedemos a la votación de las enmiendas formalizadas por el Grupo Parlamentario Más Madrid al proyecto de ley no retiradas y no afectadas por las transaccionales: enmiendas 4, 8, 9, 11, 12, 13, 14, 16, 17, 19, 20, 21, 22, 23 y 24.

El Sr. **NAVARRO MORALES**: Señor presidente, aquí solicitamos la votación separada de la 4 y la 12.

El Sr. **PRESIDENTE**: La 4 y la 12, vale; entonces, como solicitan, votamos primero estas últimas: la 4 y la 12. Muy bien. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 16 votos a favor, cero votos en contra y 1 abstención. En consecuencia, queda aprobada.

Votamos seguidamente el resto de las enmiendas al proyecto de ley del Grupo Más Madrid no retiradas ni afectadas por las transaccionales: 8, 9, 11, 13, 14, 16, 17, 19, 20, 21, 22, 23 y 24. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 6 votos a favor, 10 votos en contra y 1 abstención. En consecuencia, queda rechazada.

Votamos, a continuación, la enmienda técnica presentada por el Grupo Popular al texto del artículo 8.1 del proyecto de ley a la vista de las observaciones efectuadas por la letrada en su informe jurídico. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 16 votos a favor, cero en contra y 1 abstención. En consecuencia, queda aprobada.

Seguidamente procedemos a la votación de las enmiendas o correcciones técnicas planteadas por la letrada en su informe jurídico. El artículo 1, apartados 1, 2 y 3, y el artículo 3, apartado 1, y el artículo 3, apartado 2, letra d), e inclusión de nueva letra final en dicho apartado 2. Procedemos a la votación. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 16 votos a favor, cero en contra y 1 abstención. En consecuencia, queda aprobado.

Seguidamente procedemos a la votación de las enmiendas formales, ortográficas o gramaticales planteadas por la letrada en su informe jurídico, concretamente a la exposición de motivos, epígrafe primero, párrafos séptimo, décimo, penúltimo y último; exposición de motivos, epígrafe dos, párrafo cuarto; exposición de motivos, epígrafe tres, párrafos primero, tercero, cuarto y quinto; artículo 1.1, artículo 1.2 y artículo 1.3, en este caso, con la llamada a las correcciones en el texto, y 1.4; artículo 2.3 primero y segundo; artículo 3.2 y 3.2, letra f) y letra i); artículo 5.2, letras h), i) y j); artículo 6.1, letras b), d), d) y j); artículo 6.5; artículo 7.2 y 7.2, letras j), l), m), o), p) y q). Finalmente, la homogeneización en todo el texto de la ortografía en las menciones al consejero delegado de la agencia y las referencias al Derecho público o privado. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 16 votos a favor, cero votos en contra y 1 abstención. En consecuencia, queda aprobado.

Seguidamente votamos el articulado del texto del proyecto de ley en su conjunto con las enmiendas, las enmiendas transaccionales, la enmienda técnica y enmiendas y correcciones técnicas y formales que acabamos de aprobar en la comisión. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 16 votos a favor, 1 voto en contra y cero abstenciones. En consecuencia, queda aprobado.

Señorías, finalmente procedemos a la votación de la exposición de motivos en su conjunto con las enmiendas, las enmiendas transaccionales, las enmiendas y correcciones técnicas y formales que acabamos de aprobar. ¿Votos a favor? *(Pausa.)* ¿Votos en contra? *(Pausa.)* ¿Abstenciones? *(Pausa.)* El resultado de la votación ha sido: 16 votos a favor, 1 en contra y cero abstenciones. En consecuencia, queda aprobado y, con ello, queda aprobado el dictamen de la comisión del Proyecto de Ley 1/2023, de creación de la Agencia de Ciberseguridad de la Comunidad de Madrid, que será elevado a la Mesa de la Asamblea para la tramitación subsiguiente que proceda, conforme a lo dispuesto por el artículo 146 del Reglamento de la Asamblea.

Esta presidencia recuerda a los grupos parlamentarios que, conforme a lo dispuesto por el artículo 147 del Reglamento, disponen del plazo de los dos días siguientes a la aprobación del presente dictamen para comunicar por escrito a la Mesa de la Cámara las enmiendas y votos particulares que, habiendo sido debatidos y votados en la comisión, no se hayan aprobado en el dictamen y pretendan ser defendidos en el pleno; por tanto, hasta el viernes y hora de cierre del registro general de la Asamblea.

Finalizada la tramitación de la iniciativa legislativa, pasamos al tercer punto del orden del día.

——— RUEGOS Y PREGUNTAS. ———

¿Alguien tiene ruegos o preguntas a esta Mesa?

El Sr. **CEPEDA GARCÍA DE LEÓN**: Señor presidente, para que conste en acta ya que en mi intervención inicial no lo he podido hacer, quiero agradecer también a los servicios técnicos tanto de la consejería como de todos los grupos parlamentarios y especialmente representado la figura de la letrada de esta comisión, doña Almudena Marazuela, que, sin lugar a dudas, sin su trabajo tan exhaustivo y con tanto detalle, todo este elenco de votaciones que acabamos de tener no hubiera sido posible; por lo tanto, agradecerles su trabajo, claro que sí.

El Sr. **PRESIDENTE**: Muy bien, y yo igual: agradecer a todos el trabajo y especialmente a Almudena, que ha sido clave y fundamental, así que enhorabuena. Se levanta la sesión. Muchas gracias.

(Se levanta la sesión a las 12 horas y 53 minutos).

DIRECCIÓN DE GESTIÓN PARLAMENTARIA

SERVICIO DE PUBLICACIONES

Plaza de la Asamblea de Madrid, 1 - 28018-Madrid

Web: www.asambleamadrid.es

e-mail: publicaciones@asambleamadrid.es

Depósito legal: M. 19.464-1983 - ISSN 1131-7051

Asamblea de Madrid