BOLETÍN OFICIAL
DE LAS CORTES GENERALES

SECCIÓN CORTES GENERALES

XV LEGISLATURA

Serie A:
ACTIVIDADES PARLAMENTARIAS 27 de marzo de 2026 Núm. 223 Pág. 1

Otros textos

COMISIONES MIXTAS, SUBCOMISIONES Y PONENCIAS

154/000007 (CD)
573/000003 (S)
Ponencia de análisis de las amenazas en el ciberespacio, en la era de la Inteligencia Artificial y la Computación Cuántica, para la elaboración de un informe de riesgos y recomendaciones de mejora.
Informe aprobado por la Ponencia y propuestas de modificación.

En cumplimiento de lo dispuesto en el artículo 97 del Reglamento de la Cámara, se ordena la publicación en el Boletín Oficial de las Cortes, Sección Cortes Generales, del Informe aprobado por la Ponencia de análisis de las amenazas en el ciberespacio, en la era de la Inteligencia Artificial y la Computación Cuántica, para la elaboración de un informe de riesgos y recomendaciones de mejora, constituida en el seno de la Comisión Mixta de Seguridad Nacional, así como de las propuestas de modificación presentadas al mismo.

Palacio del Congreso de los Diputados, 24 de marzo de 2026.—P.D. El Letrado Mayor de las Cortes Generales, **Fernando Galindo Elola-Olaso.**

cve: BOCG-15-CG-A-223

INFORME DE LA PONENCIA DE ANÁLISIS DE LAS AMENAZAS EN EL CIBERESPACIO, EN LA ERA DE LA INTELIGENCIA ARTIFICIAL Y LA COMPUTACIÓN CUÁNTICA, PARA LA ELABORACIÓN DE UN INFORME DE RIESGOS Y RECOMENDACIONES DE MEJORA, APROBADO EN SU REUNIÓN DE 24 DE FEBRERO DE 2026

ÍNDICE

I. INTRODUCCIÓN

1. Objeto del Informe

El presente informe tiene por objeto presentar y reflejar de manera sistemática las conclusiones de la Ponencia de Análisis de las Amenazas en el Ciberespacio, en la Era de la Inteligencia Artificial y de la Computación Cuántica, así como formular recomendaciones de mejora en el ámbito de la seguridad nacional, la protección de las **entidades** críticas, el

cve: BOCG-15-CG-A-223

funcionamiento de las instituciones públicas y la salvaguarda de la ciudadanía **a partir de una nueva visión socializada y amplia de ciberseguridad.**

El informe se elabora en el marco de la Ponencia de la ya mencionada materia, constituida en el seno de la Comisión Mixta de Seguridad Nacional, y responde al mandato expreso de recabar, escuchar y sistematizar las aportaciones realizadas por un amplio y plural conjunto de comparecientes[1]. A tal efecto, la Ponencia ha contado con testimonios y comparecencias de expertos procedentes del sector público, del ámbito judicial y policial, de empresas tecnológicas y de ciberseguridad, del sector de las infraestructuras críticas, del mundo académico y de la sociedad civil, con el objetivo de disponer de una visión rigurosa, plural y actualizada del fenómeno.

Desde esta perspectiva, el informe no se limita a describir el estado de la cuestión, sino que se construye deliberadamente a partir del análisis comparado de las opiniones, diagnósticos, advertencias y propuestas formuladas por los distintos expertos comparecientes, estructurándolos por ejes temáticos y orientándolos a la mejora de las políticas públicas en materia de ciberseguridad, desde un enfoque práctico, institucional y alineado con las necesidades reales del Estado y de la ciudadanía.

2. Miembros de la Ponencia

La Ponencia fue constituida en el seno de la Comisión Mixta de Seguridad Nacional conforme a lo acordado por dicha Comisión, y estuvo presidida por su presidenta, Excelentísima Señora Doña Edurne Uriarte Bengoechea, actuando como coordinadora de los trabajos. La composición de la Ponencia reflejó la pluralidad parlamentaria, con representación de los distintos grupos **parlamentarios** presentes en **el Congreso de los Diputados y en el Senado**, contando asimismo con el asesoramiento técnico y jurídico de los letrados de la Comisión Mixta de Seguridad Nacional, responsables de la asistencia técnica y de la redacción de los acuerdos e informes.

Concretamente, formaron parte como ponentes**, además de la Sra. Presidenta de la Comisión Mixta de Seguridad Nacional,** los siguientes **dieciséis diputados y senadores**:

— Excmo. Sr. D. Mario Cortés Carballo. Diputado por Málaga-*Grupo Parlamentario Popular en el Congreso.*

— Excmo. Sr. D. Fernando Adolfo Gutiérrez Díaz de Otazu. Senador por Melilla-*Grupo Parlamentario Popular en el Senado*.

— Excmo. Sr. D. José Antonio Monago Terraza. Senador por Badajoz-*Grupo Parlamentario Popular en el Senado*.

— Excmo. Sr. D. Juan Luis Pedreño Molina. Diputado por Murcia-*Grupo Parlamentario Popular en el Congreso.*

— Excmo. Sr. D. Miguel Carmelo Dalmau Blanco. Senador por Zaragoza-*Grupo Parlamentario Socialista en el Senado.*

— Excmo. Sr. D. José Antonio Rodríguez Salas. Diputado por Granada-*Grupo Parlamentario Socialista en el Congreso.*

— Excmo. Sr. D. Víctor Javier Ruiz de Diego. Diputado por Zaragoza-*Grupo Parlamentario Socialista en el Congreso.*

— Excma. Sra. Dña. Inmaculada Sánchez Roca. Senadora por Murcia-*Grupo Parlamentario Socialista en el Senado.*

— Excmo. Sr. D. Alberto Asarta Cuevas. Diputado por Castellón-*Grupo Parlamentario VOX en el Congreso.*

— Excmo. Sr. D. Ignacio Gil Lázaro. Diputado por Valencia-*Grupo Parlamentario VOX en el Congreso.*

— Excma. Sra. Dña. Teslem Andala Ubbi. Diputada por Madrid-*Grupo Parlamentario Plurinacional SUMAR en el Congreso.*

— Excmo. Sr. D. Francisco Sierra Caballero. Diputado por Sevilla-*Grupo Parlamentario Plurinacional SUMAR en el Congreso.*

cve: BOCG-15-CG-A-223

— Excmo. Sr. D. Francesc-Marc Álvaro Vidal. Diputado por Barcelona-*Grupo Parlamentario Republicano en el Congreso.*

— Excma. Sra. Dña. Míriam Nogueras i Camero. Diputada por Barcelona-*Grupo Parlamentario Junts per Catalunya en el Congreso*.

— Excmo. Sr. D. Jon Iñarritu García. Diputado por Guipúzcoa-*Grupo Parlamentario Euskal Herria Bildu en el Congreso.*

— Excmo. Sr. D. Mikel Legarda Uriarte. Diputado por Álava-*Grupo Parlamentario Vasco (EAJ-PNV) en el Congreso.*

Asimismo, han asistido a la Ponencia los letrados de las Cortes Generales, Ilmo. Sr. D. Andrés Jiménez Díaz e Ilmo. Sr. D. Fernando Castillo López.

3. Fecha y contexto

La Ponencia fue creada por acuerdo unánime de la Comisión Mixta de Seguridad Nacional en su sesión celebrada el 19 de septiembre de 2024, tras la solicitud formulada por el Grupo Parlamentario Popular en el Congreso el 25 de junio de 2024. Dicho acuerdo fue publicado en el Boletín Oficial de las Cortes Generales el 24 de septiembre de 2024.

Los trabajos de la Ponencia se desarrollaron entre los meses de octubre de 2024 y **febrero** de 202**6**, periodo durante el cual se celebraron diversas sesiones de ordenación y comparecencias de expertos. Este intervalo temporal coincide con un contexto caracterizado por:

— Un incremento sostenido del cibercrimen y de los ataques dirigidos contra infraestructuras críticas, administraciones públicas y empresas privadas.

— La aceleración del desarrollo y despliegue de tecnologías basadas en inteligencia artificial, tanto con fines defensivos como ofensivos.

— La consolidación de la computación cuántica como riesgo estratégico emergente para los sistemas de cifrado actualmente utilizados.

— La tramitación y aplicación de nuevos marcos normativos europeos, como la Directiva NIS2 y el Reglamento Europeo de Inteligencia Artificial.

Este contexto confiere a los trabajos de la Ponencia un carácter especialmente relevante y oportuno, al situarse en un momento de transformación profunda del entorno digital y de la seguridad nacional.

4. Alcance y metodología

El informe se basa exclusivamente en el análisis de las comparecencias celebradas ante la Ponencia, así como en la documentación aportada por los comparecientes, de conformidad con lo previsto en el acuerdo de creación de la misma. Las comparecencias se realizaron a puerta cerrada, sin publicación de Diario de Sesiones, y fueron objeto de transcripción interna destinada a facilitar la elaboración del informe.

Desde el punto de vista metodológico, el trabajo realizado se articula sobre las siguientes premisas:

— Enfoque cualitativo: el informe recoge y sistematiza aportaciones procedentes de responsables institucionales, fuerzas y cuerpos de seguridad, operadores de infraestructuras críticas, empresas tecnológicas, asociaciones profesionales, fiscalía, academia y organizaciones de la sociedad civil.

— Exposición temática y transversal: frente a una exposición por comparecientes, el informe reorganiza los contenidos en grandes ejes analíticos (amenazas, impactos, brechas, recomendaciones), permitiendo identificar patrones comunes, convergencias y divergencias.

— Tratamiento fidedigno y confidencial de fuentes: el informe se elabora a partir de las aportaciones, valoraciones y consideraciones expresas formuladas por los comparecientes en el curso de las sesiones de la Ponencia. Por razones de seguridad y confidencialidad, no

cve: BOCG-15-CG-A-223

se incorporan citas literales individualizadas de los comparecientes; no obstante, se recogen de forma fiel y sistemática los contenidos sustantivos de sus intervenciones.

— Orientación a la mejora de políticas públicas: el informe prioriza la identificación de riesgos sistémicos y la formulación de recomendaciones operativas, estratégicas y normativas, con especial atención a la protección del ciudadano y a la seguridad nacional.

El alcance del informe se circunscribe, por tanto, al análisis de riesgos y recomendaciones de mejora en materia de ciberseguridad en el contexto actual, sin perjuicio de que sus conclusiones puedan servir de base para futuros desarrollos normativos, estratégicos o institucionales.

II. ANÁLISIS DE LA COYUNTURA ACTUAL: LA TRANSFORMACIÓN DEL ENTORNO DIGITAL

1. Contexto general: aceleración tecnológica, aumento del cibercrimen y riesgos para la seguridad nacional y la ciudadanía

El conjunto de comparecencias evidencia una coincidencia transversal: España se encuentra inmersa en el proceso global de acelerada transformación digital que ha modificado profundamente la naturaleza de las amenazas que enfrenta el Estado, la economía y la ciudadanía. Los expertos provenientes de instituciones públicas, empresas tecnológicas, cuerpos policiales, Fiscalía, operadores críticos y sociedad civil coinciden en que el ciberespacio se ha convertido en un dominio estratégico cuyo funcionamiento condiciona la estabilidad del país.

El elemento central que vertebra este diagnóstico es la aceleración tecnológica. Tal y como señalaron los diferentes comparecientes, la velocidad de evolución de la tecnología ha comprimido los ciclos de cambio: procesos que antes requerían años ahora se transforman en cuestión de meses. La inteligencia artificial (IA) generativa, las nuevas **tecnologías de telecomunicaciones**, la computación cuántica, la expansión de dispositivos conectados y la automatización masiva han creado un entorno dinámico donde la capacidad ofensiva crece más rápido que la defensiva, exponiendo a la sociedad a riesgos sin precedentes.

Paralelamente, el cibercrimen no solo crece en volumen, sino en sofisticación y organización. Los datos aportados por la Fiscalía, la Guardia Civil, la Policía Nacional, el Instituto Nacional de Ciberseguridad (INCIBE) y empresas especializadas muestran una tendencia sostenida al alza. En el ámbito penal, los procedimientos por ciberdelitos han aumentado más de un 14 % en un solo año, y más del 60 % respecto a 2020. El 83,4 % corresponde a estafas digitales, con modalidades cada vez más complejas, desde *phishing*[2] multicanal hasta engaños afectivos, fraudes de inversión o estafas masivas vinculadas a criptomonedas. Tanto la Guardia Civil como la Policía Nacional señalaron que el volumen real es muy superior al registrado, dado que hasta el 80 % de las víctimas no denuncia, especialmente en casos de fraude emocional o extorsión sexual.

Del mismo modo, operadores privados y empresas proveedoras de *software* y *hardware* confirmaron la magnitud del fenómeno: compañías como MasOrange o Telefónica registran diariamente **miles** de intentos de intrusión, y empresas internacionales como Cisco, Palo Alto Networks o Check Point detectan cientos de miles de millones de eventos globales al día. La infraestructura crítica española ha sido objeto de campañas de hacktivismo prorruso, ataques a cadenas de suministro, explotación de vulnerabilidades en servicios esenciales y actividad de ataques APT[3] ligados a Rusia, China, Irán y Corea del Norte. En este último caso, la infiltración laboral mediante identidades sintéticas ha sido señalada como una amenaza emergente y especialmente peligrosa, pues combina ingeniería social, acceso interno y exfiltración silenciosa.

Además, organismos públicos han identificado más de cuatro millones de dispositivos vulnerables en el territorio nacional, y expertos del sector privado subrayaron la elevada exposición de España en el contexto internacional, señalando que nuestro país se sitúa entre los diez Estados que más ciberataques reciben a nivel mundial, ocupando

cve: BOCG-15-CG-A-223

concretamente la octava posición, **si bien no existen cifras oficiales homologables que lo acrediten.**

Este fenómeno tiene implicaciones directas para la seguridad nacional. La interrupción de redes de telecomunicaciones, energía, infraestructuras o transporte puede paralizar sectores enteros. Los ejemplos que nos ofrecen diferentes conflictos a lo largo de todo el orbe —en materia de protección digital de infraestructuras críticas o campañas masivas de desinformación— demuestran que el ciberespacio es un vector real de conflicto interestatal.

Por otra parte, la dimensión ciudadana ocupa un lugar central. Las comparecencias de organizaciones sociales, Fiscalía y cuerpos policiales coinciden en que el ciudadano es el eslabón más débil del ecosistema de seguridad: carece de formación, sufre estafas masivas, es víctima de manipulación emocional y desinformación, y está expuesto a prácticas avanzadas de ingeniería social potenciadas por IA. Los menores son especialmente vulnerables, con un aumento cuantitativo y cualitativo de delitos de grooming[4], sextorsión y explotación sexual digital.

En conjunto, las aportaciones recabadas describen una coyuntura de elevada complejidad, marcada por el incremento sostenido del riesgo y por una brecha cada vez más evidente entre la capacidad ofensiva de los actores maliciosos y la capacidad defensiva de las instituciones, las empresas y la ciudadanía.

Por ello, otro eje común entre los comparecientes es el reconocimiento de que la sociedad española —al igual que el resto de las economías avanzadas— ha pasado de estar digitalizada a ser digitalmente dependiente. El concepto «sociedad fígital» sintetiza esta realidad: lo físico y lo digital forman un continuo inseparable, sin fronteras claras entre un dominio y otro.

La digitalización ha alcanzado todos los estratos: administraciones, servicios esenciales, infraestructuras críticas, pymes, ciudadanos y hogares conectados. Esta integración conlleva dos efectos simultáneos: el incremento, por un lado, de la eficiencia, conectividad, capacidad de procesamiento y generación de datos; pero al mismo tiempo se produce una exposición total a ataques en cualquier punto de la red. Esta realidad hace imprescindible la coordinación público-privada **y fortalecer y priorizar la cooperación pública-pública a escala estatal y europea.**

Además, muchos sistemas heredados (OT industriales[5], redes municipales, equipamiento médico o sistemas automatizados) no fueron diseñados bajo criterios de ciberseguridad, lo que amplifica la vulnerabilidad en la superficie de ataque.

Asimismo, esta dependencia digital se refleja en los riesgos de cadenas de suministro. Casos como *SolarWinds*, *Logink* o el incidente global derivado del fallo de *CrowdStrike* muestran que errores, vulnerabilidades o ataques a un proveedor pueden escalar hasta paralizar sectores enteros. Esta interdependencia convierte al ciberespacio en una infraestructura crítica transversal.

En consecuencia, la digitalización, aun constituyendo un factor clave de competitividad, incrementa también el riesgo sistémico al permitir que actores de muy distinta naturaleza, ya sean Estados hostiles, grupos criminales o usuarios maliciosos, puedan comprometer servicios esenciales desde cualquier punto del mundo.

2. Inteligencia artificial e hiperautomatización

Precisamente, la inteligencia artificial aparece como el fenómeno más disruptivo de esta «revolución digital». Todas las comparecencias técnicas coinciden en que la IA ha convertido el cibercrimen en una actividad automatizada, escalable y extremadamente rápida, reduciendo drásticamente las barreras de entrada. De entre los ejemplos que reflejan el sustantivo impacto de esta nueva tecnología en la seguridad del ciberespacio destacan:

— La generación de *ransomware*[6] en horas y exfiltración de datos en minutos.
— La automatización del *phishing* y su personalización mediante algoritmos generativos.
— La capacidad de la IA para detectar vulnerabilidades en redes complejas sin intervención humana.

cve: BOCG-15-CG-A-223

— El uso de IA para crear identidades sintéticas, suplantar voces en segundos o generar *deepfakes*[7] convincentes no son más que algunos ejemplos del sustantivo impacto que esta nueva tecnología está teniendo en la seguridad del ciberespacio.

Además, la IA permite ataques multifrontales simultáneos, en los que un mismo actor puede lanzar campañas combinadas de intrusión, fraude, desinformación y denegación de servicio. Algunas empresas destacaron que el 70 % de los incidentes ya afectan simultáneamente a tres o más superficies de ataque. Sin embargo, la IA no es solo un riesgo: también representa una oportunidad. Los operadores y empresas de ciberseguridad explicaron que la IA defensiva permite priorizar alertas en tiempo real, automatizar respuestas e identificar patrones de ataque imposibles de detectar manualmente. Algunos comparecientes indicaron que su aplicación puede reducir de manera notable los tiempos de gestión de incidentes, con reducciones medias de hasta 27 días en determinados procesos, en comparación con enfoques manuales o poco automatizados.

Algunos comparecientes aportaron ejemplos concretos del impacto operativo de la inteligencia artificial aplicada a la ciberseguridad. En particular, se señaló que la incorporación de sistemas avanzados de análisis automatizado en centros de operaciones de seguridad ha permitido reducir de forma significativa los tiempos de investigación de incidentes, pasando de decenas de minutos a apenas unos pocos, con mejoras de eficiencia cercanas al 80 %. Estas capacidades no sustituyen al analista humano, sino que actúan como un apoyo permanente, facilitando la priorización de alertas, la correlación de eventos y la toma de decisiones en tiempo real. No obstante, existe cierto consenso acerca de la desigualdad existente en el despliegue de capacidades de IA defensiva en España, especialmente en pymes y administraciones locales.

3. Amenaza cuántica

La computación cuántica constituye el riesgo tecnológico emergente más grave a medio plazo. Varios comparecientes alertaron de que, antes de 2030, podría alcanzarse capacidad suficiente para vulnerar los algoritmos criptográficos que hoy protegen comunicaciones, datos críticos y transacciones digitales.

Los expertos indicaron que:

— Estados y grupos criminales ya están adoptando la estrategia *store now, decrypt later*, es decir, almacenar datos cifrados actuales para descifrarlos en el futuro.

— El ciclo de renovación tecnológica en infraestructuras críticas es lento (6-10 años), lo que significa que muchas tecnologías actuales seguirán operativas cuando llegue el *Q-Day*, el día en que la computación cuántica sea comercial.

— Aunque el NIST[8] ya ha publicado los estándares de criptografía poscuántica, su implantación es incipiente en España[9].

— Equipamientos, redes y dispositivos no son compatibles de forma nativa con algoritmos poscuánticos, lo que exige una transición progresiva pero urgente.

— El sector privado ya trabaja en soluciones híbridas de transición, pruebas de QKD[10], algoritmos resistentes y simulaciones cuánticas. Sin embargo, casi todos los comparecientes coincidieron en que España y Europa están retrasadas respecto a otros países en la adopción de estrategias poscuánticas.

— Debe distinguirse de forma expresa entre la criptografía postcuántica, concebida como una solución generalizable y compatible con infraestructuras actuales, y la distribución cuántica de claves (QKD), que requiere *hardware* específico y se orienta a enlaces de comunicaciones altamente críticos. Ambos enfoques no son excluyentes, sino complementarios, y una transición eficaz previsiblemente combinará soluciones clásicas, postcuánticas y, en casos muy concretos, tecnologías cuánticas dedicadas.

— La amenaza cuántica no es solo tecnológica: implica riesgos geopolíticos, económicos y de soberanía, pues quien controle la capacidad cuántica controlará la capacidad de descifrar comunicaciones, proteger infraestructuras o incluso condicionar procesos democráticos.

cve: BOCG-15-CG-A-223

III. DIAGNÓSTICO GENERAL-AMENAZAS

1. Cibercrimen masivo: industrialización y escalabilidad del delito digital

Las comparecencias coinciden en que el cibercrimen ha dejado de ser un fenómeno marginal para convertirse en una industria global altamente organizada, con modelos de negocio propios, estructuras jerárquicas y servicios comercializados como si se tratase de un mercado legítimo.

En este contexto, algunos comparecientes aportaron datos que permiten dimensionar con precisión la magnitud del fenómeno en España. En 2023, el INCIBE-CERT[11] gestionó un total de 266.594 incidentes de ciberseguridad, lo que supuso un incremento del 24 % respecto al año anterior. **Sin embargo, resulta importante resaltar que se están mezclando dos conceptos: cibercrimen y ciberincidentes. Respecto al primero, las estadísticas oficiales son las del Ministerio del Interior y la Fiscalía General del Estado en su Memoria anual. Respecto al segundo, estos ciberincidentes engloban hechos que pueden ser considerados como cibercrimen, pero también otros incidentes que no lo son (por ejemplo: fallos software, fallos humanos, hechos no delictivos…).** La gran mayoría de estos incidentes afectaron a ciudadanía y empresas, si bien también se registraron incidencias relevantes en la red académica y, de forma específica, en operadores críticos y esenciales.

Del mismo modo, los datos expuestos por Fiscalía, Guardia Civil, INCIBE y empresas privadas también muestran un crecimiento sostenido del cibercrimen en España, con incrementos anuales superiores al 14 % en procedimientos penales y más de 170.000 incidentes gestionados por organismos públicos. El sector privado eleva esta cifra a millones de intentos diarios en operadores de telecomunicaciones, administradores de infraestructuras críticas y plataformas digitales.

El fenómeno más relevante es la industrialización del delito, impulsada por la inteligencia artificial y por plataformas clandestinas accesibles para individuos sin conocimientos especializados. Los comparecientes destacaron la proliferación del *Ransomware-as-a-Service* (RaaS)[12], la existencia de mercados de datos robados, accesos corporativos y herramientas ofensivas listas para usar y la capacidad de automatizar ataques para comprometer simultáneamente miles de dispositivos o usuarios.

Este cibercrimen masivo se caracteriza además por su baja tasa de denuncia (en torno al 20 % o incluso menos), lo que dificulta su medición real y contribuye a una enorme infrarrepresentación del problema.

2. APT, Actores Estatales y *hacktivismo*: ciberconflicto y operaciones encubiertas

La inmensa mayoría de comparecientes alertaron de que las amenazas más sofisticadas proceden de grupos de ciberinteligencia vinculados a Estados. Se mencionan de forma reiterada las llamadas APT (*Advanced Persistent Threat*, o Amenazas persistentes avanzadas); en especial las de origen ruso, chino, iraní y norcoreano, cuyas actividades incluyen espionaje político, militar y económico, robo de propiedad intelectual, exploración persistente de vulnerabilidades en infraestructuras críticas y operaciones de desinformación coordinadas con intrusiones técnicas.

Los expertos llamados a comparecer señalaron que estos actores han elevado el umbral técnico del ataque, comprometiendo cadenas de suministro, usando identidades sintéticas para infiltración laboral (destacando el caso de Corea del Norte) y efectuando ataques complejos y silenciosos dirigidos a operadores estratégicos. Asimismo, advirtieron de una tendencia creciente al uso de grupos de ciberdelincuencia con motivación económica por parte de determinados Estados, que recurren a estos actores para llevar a cabo operaciones de ciberespionaje, sabotaje o desinformación. Esta convergencia entre criminalidad organizada y acción estatal dificulta la atribución de los ataques, incrementa la complejidad del entorno de amenazas y reduce los umbrales de responsabilidad política y jurídica.

cve: BOCG-15-CG-A-223

Del mismo modo, el contexto geopolítico —conflicto en Ucrania, tensiones en Oriente Medio, rivalidades estratégicas en el ámbito tecnológico— alimenta esta actividad y sitúa a España dentro de un ecosistema global de riesgo.

Por otro lado, las comparecencias policiales y de operadores críticos confirmaron una presencia creciente de grupos *hacktivistas*, especialmente vinculados a causas geopolíticas o campañas de presión internacional. El más citado fue NoName057 (prorruso), responsable de ataques de denegación de servicio contra administraciones públicas españolas, páginas institucionales y operadores estratégicos.

Aunque estos ataques rara vez provocan daños técnicos severos, sí generan interrupciones temporales de servicio, pérdida de confianza pública y exposición mediática que los actores explotan como parte de su narrativa propagandística.

Los *hacktivistas* operan **normalmente,** mediante técnicas simples pero masivas, aprovechando herramientas automatizadas accesibles y voluntarios distribuidos globalmente. Este fenómeno se intensifica en momentos de tensión internacional, procesos electorales o aprobación de leyes sensibles. En este sentido, determinadas campañas de hacktivismo, si bien presentan un impacto técnico limitado, buscan deliberadamente un elevado impacto mediático y reputacional. Este tipo de ataques, frecuentemente materializados mediante acciones de denegación de servicio, adquieren especial relevancia en contextos de tensión geopolítica, al amplificar narrativas y generar efectos desestabilizadores desproporcionados respecto a su complejidad técnica.

3. Estafas y fraude digital: la amenaza más extendida y socialmente dañina

Las cifras aportadas por la Fiscalía, la Guardia Civil, la Policía Nacional y la Asociación Nacional contra la Estafa con Manipulación Emocional (ANCEME) revelan que el fraude digital es la categoría delictiva dominante, representando más de ocho de cada diez ciberdelitos.

Entre las modalidades más relevantes destacan:

— *Phishing*, *smishing*[13] y *vishing*[14] cada vez más personalizados mediante IA.
— Estafas de inversión, especialmente en criptomonedas, con perjuicios multimillonarios.
— Fraudes bancarios mediante suplantación, accesos remotos o interceptación de doble factor.
— Estafas amorosas o de manipulación emocional, que combinan ingeniería social con técnicas psicológicas sistemáticas.
— Suplantación de identidad reforzada por *deepfakes*, particularmente de voz.

El correo electrónico continúa siendo el principal punto de entrada, al concentrar cerca del 58 % de los ataques detectados. Se destacó asimismo el uso recurrente de malware distribuido mediante falsas actualizaciones, empleado como puerta de entrada para *botnets*[15] y herramientas de acceso remoto, lo que refuerza la importancia de la concienciación y de las medidas de protección en este ámbito. Además, la mayor parte de las víctimas no denuncia, bien por vergüenza, por desconocimiento o por la percepción de inutilidad, lo que distorsiona la capacidad del Estado para dimensionar el fenómeno y asignar recursos adecuados.

La IA ha multiplicado la escala del fraude: un solo atacante puede generar miles de mensajes personalizados, crear perfiles digitales completamente verosímiles o simular conversaciones humanas convincentes.

4. Explotación sexual infantil: emergencia silenciosa pero en crecimiento

Las comparecencias de la Fiscalía y cuerpos policiales alertaron de un crecimiento significativo y cualitativo de los delitos contra menores en entornos digitales. Entre las principales tendencias se encuentran:

— *Grooming* sistemático mediante identidades falsas.
— Generación de imágenes manipuladas o falsas mediante IA (incluidos desnudos sintéticos).

cve: BOCG-15-CG-A-223

— Retransmisión en directo de contenido sexual con menores, detectado incluso dentro de territorio nacional.

— Captación y coacción psicológica mediante técnicas equivalentes a las de grupos de trata.

Estos delitos presentan tres características particularmente graves:

1. Baja detectabilidad, porque dependen del aislamiento emocional de la víctima.
2. Velocidad de proliferación, gracias a IA y plataformas de mensajería cifrada.
3. Alta revictimización, pues una sola imagen puede circular indefinidamente.

Los expertos subrayaron la necesidad de reforzar medios técnicos y humanos, tanto en investigación como en prevención, y de actualizar el Código Penal para reflejar la realidad digital del abuso.

5. Desinformación y propaganda: erosión social y riesgo democrático

La desinformación fue identificada como una amenaza estratégica de primer orden. Los comparecientes coincidieron en que las campañas de influencia digital se han convertido en un instrumento geopolítico y criminal de enorme impacto. Además, la IA generativa permite producir contenido falso a escala industrial: imágenes, vídeos, voces sintéticas y narrativas automatizadas capaces de manipular percepciones y decisiones.

Los principales protagonistas de esta modalidad delictiva son actores estatales con objetivos geopolíticos. Concretamente, Rusia lleva a cabo campañas globales bien financiadas, según algunos comparecientes, con presupuestos que podrían alcanzar la escala de miles de millones de dólares. Sus operaciones incluyen manipulación algorítmica, amplificación de narrativas, ataques coordinados de DDoS[16] y desinformación. Otros países mencionados fueron China o Irán.

Precisamente, algunos comparecientes señalaron que la IA ha sido empleada en al menos un tercio de los procesos electorales celebrados a nivel mundial entre finales de 2023 y comienzos de 2024, principalmente mediante campañas de desinformación, suplantación y difusión de contenidos manipulados. Este fenómeno fue vinculado al uso de *deepfakes*, técnicas de ingeniería social y operaciones de influencia dirigidas contra procesos democráticos.

No obstante, también aprovechan esta técnica actores delincuenciales, como grupos vinculados a criptoestafas o campañas de fraude que utilizan desinformación masiva para captar víctimas, manipular mercados o desplazar la atención policial.

El impacto social de esta estrategia criminal no es en absoluto despreciable para la ciudadanía. ONGs de derechos digitales alertaron de que la desinformación afecta de manera desproporcionada a colectivos vulnerables, distorsiona debates en la agenda pública/mediática, socava la confianza pública en instituciones y alimenta la polarización y los discursos de odio.

6. Impacto en sectores críticos: riesgos operativos y efectos en cascada sobre los servicios básicos

Las comparecencias de la Ponencia han revelado que las ciberamenazas se han consolidado como uno de los principales factores de riesgo estructural para el funcionamiento del Estado, afectando de manera directa a los sectores esenciales que sostienen la actividad económica, la vida cotidiana y la prestación de servicios públicos. De forma transversal, los expertos dejaron claro que ningún sector crítico está fuera del alcance de la ciberdelincuencia, los actores estatales o el *hacktivismo*, y que la sofisticación tecnológica está incrementando el impacto potencial de cada ataque.

En relación con la Administración Pública, algunos comparecientes aportaron datos que permiten dimensionar con mayor precisión la magnitud del fenómeno. En 2024, el Centro Criptológico Nacional (CCN) gestionó más de 177.000 incidentes, el CERT del INCIBE más de 97.000 y el Equipo de Respuesta ante Incidentes de Ciberseguridad del

cve: BOCG-15-CG-A-223

Mando Conjunto del Ciberespacio (ESPDEF-CERT) cerca de 1.000. Entre los operadores de servicios esenciales, los sectores más afectados fueron el transporte, el ámbito tributario y financiero, la energía y las tecnologías de la información y la comunicación, siendo la mayoría de los incidentes resultado de acciones maliciosas deliberadas. INCIBE, por su parte, gestionó más de 83.000 incidentes en el sector privado, mientras que el ámbito de defensa registró 1.480 incidentes en su red.

Dentro de esta realidad, el sector de la energía fue señalado como uno de los más atacados y sensibles. Los expertos destacaron que buena parte de las infraestructuras industriales españolas utilizan sistemas OT heredados, no diseñados originalmente para soportar amenazas digitales. Esta fragilidad estructural, unida a la complejidad de las cadenas de suministro, incrementa exponencialmente la vulnerabilidad.

También se advirtió que ataques coordinados contra redes eléctricas o centros de control podrían generar efectos en cascada que afectarían simultáneamente a transporte, telecomunicaciones y servicios esenciales. La memoria de incidentes internacionales y el papel geopolítico de la energía sitúan a este sector en una zona de riesgo elevado.

El transporte aparece igualmente como uno de los sectores más afectados. Precisamente, se mencionó en la Ponencia que el transporte se encuentra entre los sectores que más incidentes concentran, tanto por su alto nivel de digitalización como por su exposición a amenazas híbridas. Las comparecencias recordaron que los sistemas de gestión aeroportuaria, ferroviaria y portuaria dependen de redes altamente automatizadas susceptibles a ataques de denegación de servicio, intrusiones o explotación de vulnerabilidades. El *hacktivismo* prorruso ha demostrado que incluso ataques no destructivos pueden afectar la disponibilidad de páginas institucionales o sistemas de comunicación, dificultando operaciones y erosionando la confianza del usuario. En un sector donde los tiempos y la continuidad del servicio son esenciales, incluso incidentes superficiales generan daños reputacionales y operativos relevantes.

Por otro lado, el sector de telecomunicaciones fue descrito por los operadores como el «sistema nervioso» del conjunto del país. Empresas como MasOrange o Telefónica reportaron que reciben diariamente **miles** de intentos de intrusión, afectando a redes móviles, fibra, infraestructura *cloud* y servicios gestionados. Cisco señaló que, a escala global, detecta más de 800.000 millones de amenazas al día, lo que da una medida del entorno en el que operan las telecomunicaciones españolas. Debido a que este sector da servicio a todos los demás —energía, finanzas, transporte y Administración—, cualquier ataque que comprometa un nodo relevante puede tener un efecto multiplicador sobre la economía y la seguridad nacional. Además, las campañas de desinformación se apoyan en estas plataformas, dificultando aún más su operación.

Del mismo modo, algunos comparecientes advirtieron de riesgos específicos en este sector derivados de su carácter de servicio crítico y de la complejidad técnica de sus redes. Entre ellos se mencionaron amenazas como el fraude y la suplantación de identidad, prácticas como el *SIM swapping*[17], vulnerabilidades asociadas a protocolos heredados de señalización y los retos de seguridad vinculados a la progresiva *cloudificación*[18] de la red y a arquitecturas abiertas como Open RAN[19]. Estas particularidades refuerzan la necesidad de enfoques sectoriales diferenciados en materia de ciberseguridad.

El ámbito financiero continúa siendo uno de los más atacados por motivación económica:

— Fiscalía señaló que el 83,4 % de los ciberdelitos registrados son estafas, muchas de ellas dirigidas a entidades bancarias o usuarios financieros.

— La Policía Nacional advirtió de la sofisticación del fraude digital impulsada por IA y del auge del *ransomware*, por importes económicos relativamente reducidos, pero con potenciales beneficios muy elevados. Esta dinámica acelera la proliferación de nuevas variantes y amplía el número de actores con capacidad para llevar a cabo ataques de alto impacto.

— Empresas de ciberseguridad describieron un panorama donde la automatización permite a un solo actor lanzar simultáneamente miles de intentos de fraude, manipular procesos de autenticación y generar *deepfakes* de voz para suplantar empleados.

cve: BOCG-15-CG-A-223

— También se destacó el papel de las criptomonedas tanto como señuelo para estafas de inversión como para el blanqueo de capitales derivado de ataques.

— La computación cuántica fue identificada como un riesgo estratégico para el cifrado financiero: varios comparecientes alertaron de que el descifrado futuro de comunicaciones protegidas hoy podría comprometer información bancaria sensible.

Por otro lado, la Administración Pública constituye, según diversas comparecencias, uno de los sectores más castigados y con menores recursos relativos. El Centro Criptológico Nacional (CCN-CERT) registró más de 100.000 incidentes en 2023, muchos de ellos dirigidos contra organismos estatales y autonómicos. También se recordaron ataques relevantes sufridos por organismos como la Agencia Tributaria, el Servicio Público de Empleo Estatal (SEPE) o la Dirección General de Tráfico. La fragmentación tecnológica, la disparidad de recursos entre administraciones y la dependencia de sistemas antiguos aumentan la exposición; asimismo, la falta de un registro unificado de incidentes dificulta el análisis global del riesgo.

Los representantes de los distintos operadores llamados a comparecer señalaron que las administraciones españolas son objetivos habituales de ciberespionaje, *hacktivismo* y campañas combinadas de ataque técnico y desinformación, especialmente en periodos de tensión política o internacional. Dada la cantidad de datos sensibles que manejan las Administraciones Públicas —incluyendo sanidad, educación, fiscalidad, identidad y seguridad—, cualquier intrusión puede generar consecuencias directas para la ciudadanía y comprometer la confianza institucional.

En conjunto, los datos aportados por los comparecientes muestran que el impacto en sectores críticos es generalizado, creciente y sistémico. La interdependencia entre energía, transporte, telecomunicaciones, finanzas y Administración Pública implica que una vulnerabilidad en cualquiera de ellos puede desencadenar efectos dominó en el resto, afectando al funcionamiento normal del país. La Ponencia coincide en la necesidad de reforzar la ciberseguridad de estos sectores no solo como una exigencia técnica, sino como un requisito para la estabilidad económica, la continuidad de los servicios esenciales y la protección efectiva de la ciudadanía.

7. Brechas y vulnerabilidades estructurales: fragilidades persistentes del ecosistema nacional de ciberseguridad

El análisis conjunto de las comparecencias pone de manifiesto que, más allá del incremento cuantitativo y cualitativo de las amenazas en el ciberespacio, persisten brechas estructurales que limitan la capacidad de respuesta del Estado, del sector privado y del conjunto de la sociedad. Estas vulnerabilidades no se refieren únicamente a carencias tecnológicas, sino a déficits organizativos, industriales, normativos y de capital humano, reiteradamente señalados por los comparecientes como factores que amplifican el impacto de los ataques.

Una de las debilidades más recurrentes identificadas es la **descoordinación** institucional. Diversos comparecientes subrayaron que el ecosistema español de ciberseguridad se articula a través de múltiples organismos con competencias concurrentes —Centro Criptológico Nacional, INCIBE, Mando Conjunto del Ciberespacio, Fuerzas y Cuerpos de Seguridad del Estado, Administraciones autonómicas y locales—, lo que dificulta una visión integrada del riesgo. Además, tal y como señalaron algunos comparecientes, actualmente no existe un sistema que permita conocer con precisión el número total de ciberincidentes que se producen diariamente en España, incluyendo a las empresas y organismos públicos que no estén incluidas en el Esquema Nacional de Seguridad (ENS). Aunque la Directiva NIS2[20] fue valorada positivamente como una oportunidad para avanzar en esta dirección, varios comparecientes coincidieron en que, a día de hoy, la información disponible sigue siendo parcial y dispersa. Algunos comparecientes ampliaron este diagnóstico señalando que, junto a la **descoordinación** organizativa, existe una creciente fragmentación tecnológica derivada de la incorporación acelerada y poco integrada de nuevos sistemas. Esta combinación, unida a la elevada interconectividad,

cve: BOCG-15-CG-A-223

genera un entorno especialmente vulnerable frente a amenazas asimétricas, que evolucionan con mayor rapidez que las estructuras encargadas de su gestión.

En paralelo, se identificó un déficit significativo de soberanía tecnológica. **Miembros** de empresas tecnológicas y del sector industrial coincidieron en señalar que una parte sustancial de las soluciones de ciberseguridad, infraestructuras *cloud*[21] y tecnologías críticas utilizadas en España y en Europa proceden de terceros países, principalmente de Estados Unidos, Israel y China. Esta dependencia fue señalada como un factor de vulnerabilidad estratégica, especialmente en un contexto de tensiones geopolíticas y de utilización del ciberespacio como dominio de confrontación. En este sentido, se insistió en la necesidad de reforzar una industria nacional y europea de ciberseguridad, así como de garantizar el control sobre hardware, software y datos, particularmente en sectores críticos y en la Administración pública.

Asimismo, en el curso de las comparecencias se planteó expresamente la conveniencia de identificar y gestionar el riesgo asociado a determinados proveedores tecnológicos en sectores críticos y en el ámbito de las administraciones públicas. Algunos comparecientes señalaron que la dependencia de proveedores considerados de alto riesgo puede generar vulnerabilidades relevantes desde el punto de vista de la seguridad nacional, tanto por la posible exposición de datos sensibles como por el control de infraestructuras esenciales En este contexto, se hizo referencia a precedentes existentes en otros ámbitos tecnológicos, como el despliegue de las redes 5G, donde se han aplicado criterios de evaluación del riesgo de los proveedores. A partir de dicha experiencia, se apuntó la conveniencia de definir listas o catálogos de proveedores considerados seguros o de confianza, basados en criterios objetivos de seguridad, fiabilidad, control del suministro y alineación con los intereses de seguridad nacional. Estos mecanismos permitirían orientar las decisiones de contratación pública y el despliegue tecnológico en sectores sensibles, reduciendo la exposición a riesgos derivados de dependencias estratégicas.

La falta de talento especializado constituye otra brecha estructural ampliamente reconocida. Cisco señaló que el 74 % de las empresas identifica la escasez de profesionales como su principal obstáculo en ciberseguridad, y que solo el 2 % de las organizaciones españolas alcanza un nivel maduro de preparación. Desde el ámbito institucional, la Fiscalía General del Estado expuso que la red de fiscales especializados en criminalidad informática ha crecido desde 26 miembros en 2011 hasta 168 fiscales en la actualidad, lo que evidencia un esfuerzo relevante, aunque insuficiente frente al crecimiento sostenido del fenómeno delictivo digital. Otros comparecientes alertaron sobre la dificultad de retener talento en el sector público, debido a la competencia salarial del sector privado, y sobre la necesidad de reforzar la formación desde etapas tempranas, la formación profesional y la capacitación continua.

La coordinación público-privada, aunque reconocida como esencial, fue descrita como insuficiente o desigual. Si bien se citaron ejemplos positivos de colaboración —como la cooperación con INCIBE, el CCN-CERT, la Red Nacional de SOC[22] o proyectos conjuntos con grandes operadores tecnológicos—, varios comparecientes coincidieron en que esta cooperación no está plenamente sistematizada ni alcanza de forma homogénea a todos los sectores y territorios. Se subrayó que gran parte de las capacidades técnicas, del conocimiento avanzado y de la innovación reside en el sector privado, lo que hace imprescindible una colaboración estructural y estable, especialmente en la gestión de crisis, la respuesta a incidentes y el intercambio de información sobre amenazas.

No obstante, algunos comparecientes advirtieron de las dificultades que plantea el actual marco de contratación pública para adaptarse a una amenaza cibernética en rápida y constante evolución. Se señaló que los procedimientos y la cultura de adquisición de servicios tecnológicos no siempre permiten incorporar con agilidad nuevas capacidades, actualizar soluciones o responder a cambios en el panorama de riesgos, lo que puede generar desfases entre las necesidades reales de protección y los medios disponibles.

Otra vulnerabilidad especialmente destacada es la debilidad de las pequeñas y medianas empresas (pymes). Tanto representantes del sector privado como de asociaciones profesionales señalaron que las pymes constituyen el eslabón más frágil del ecosistema

cve: BOCG-15-CG-A-223

digital español. Aunque representan la base del tejido productivo, carecen en muchos casos de recursos técnicos, económicos y humanos para cumplir adecuadamente con las exigencias de ciberseguridad. Se advirtió del riesgo de que la trasposición de la Directiva NIS2, si no va acompañada de apoyo técnico y formativo, genere una carga difícilmente asumible para estas empresas. INCIBE aportó datos que reflejan la magnitud del problema: más de 83.000 ciberincidentes gestionados en el sector privado en 2023, muchos de ellos con impacto directo en pequeñas organizaciones.

Finalmente, la carencia de mecanismos homogéneos de información y evaluación aparece como un problema transversal. La falta de un registro centralizado de incidentes, la diversidad de criterios de notificación y la desigual madurez de las organizaciones dificultan la elaboración de diagnósticos precisos y la adopción de políticas basadas en evidencia. Esta carencia fue señalada como especialmente problemática en la Administración Pública, donde el CCN-CERT gestionó más de 100.000 incidentes en 2023, incluidos 130 catalogados como críticos, sin que exista aún una visión consolidada que permita evaluar tendencias, impactos y lecciones aprendidas a escala nacional.

En conjunto, las comparecencias evidencian que las brechas y vulnerabilidades estructurales no son marginales, sino factores sistémicos que condicionan la eficacia de cualquier estrategia de ciberseguridad. La **descoordinación** institucional, la dependencia tecnológica, la escasez de talento, la limitada coordinación público-privada, la vulnerabilidad de las pymes y la falta de información integrada configuran un escenario en el que las amenazas digitales encuentran condiciones propicias para amplificar su impacto, tanto sobre la seguridad nacional como sobre la actividad económica y la protección de la ciudadanía.

8. Dimensión social y de derechos: ciudadanía, víctimas y garantías en el entorno digital.

Las comparecencias de la Ponencia pusieron de relieve que la ciberseguridad no puede abordarse únicamente desde una perspectiva técnica, operativa o estratégica, sino que presenta una dimensión social y de derechos fundamentales de creciente relevancia. Los expertos coincidieron en que el impacto del cibercrimen, la automatización tecnológica y el uso intensivo de datos afecta directamente a la ciudadanía, especialmente a colectivos vulnerables, y plantea desafíos sustantivos en términos de protección de las víctimas, garantías democráticas y confianza en las instituciones.

En relación con la protección de víctimas y ciudadanía, varios comparecientes subrayaron que el aumento de la ciberdelincuencia tiene consecuencias directas sobre personas físicas, más allá del daño económico o institucional. Desde la Fiscalía General del Estado se aportaron datos que reflejan esta realidad: en 2024, se incoaron 27.547 procedimientos judiciales por ciberdelitos, con un incremento del 14,58 % respecto al año anterior y superior al 60 % en comparación con 2020. La Fiscalía destacó que el 83,4 % de los casos corresponde a estafas digitales, un tipo delictivo que afecta de forma directa a ciudadanos particulares y que, por su visibilidad, genera un elevado impacto psicológico y social en las víctimas. Asimismo, se puso de manifiesto la dificultad de atender adecuadamente a las víctimas cuando los procedimientos son complejos, transnacionales o involucran múltiples afectados.

Un aspecto especialmente destacado fue el de las estafas emocionales y la baja tasa de denuncia. **Miembros** de asociaciones de víctimas, como la Asociación Nacional contra la Estafa con Manipulación Emocional (ANCEME), señalaron que solo una minoría de las personas afectadas por este tipo de delitos llega a denunciar, debido al sentimiento de vergüenza, la manipulación psicológica sufrida o la percepción de falta de respuesta eficaz. Se subrayó que estas estafas, basadas en vínculos afectivos simulados o en la explotación emocional, generan daños que trascienden lo económico y afectan gravemente a la salud mental y a la confianza personal. En este contexto, se insistió en la necesidad de reforzar la empatía y la formación de las Fuerzas y Cuerpos de Seguridad del Estado, así como de mejorar la atención a las víctimas desde el primer contacto institucional.

La vulnerabilidad de los menores en el entorno digital ocupó un lugar central en las intervenciones. La Fiscalía alertó del incremento tanto cuantitativo como cualitativo de los

cve: BOCG-15-CG-A-223

delitos contra la libertad sexual de menores en entornos digitales, incluyendo el *child grooming*, la producción y difusión de material de abuso sexual infantil y la organización de espectáculos pornográficos retransmitidos en vivo con menores, incluso en territorio nacional. Se destacó que estos delitos presentan especiales dificultades de detección y persecución, debido a su carácter oculto, transnacional y altamente tecnificado. Asimismo, se subrayó la necesidad de dotar a fiscales, jueces y cuerpos policiales de medios técnicos y formación especializada, valorándose positivamente iniciativas normativas como el anteproyecto de Ley de Protección Integral de los Menores en Internet. Otros comparecientes alertaron del uso de inteligencia artificial para generar contenidos falsos o manipulados, incluidos desnudos sintéticos de menores, lo que incrementa la gravedad y complejidad de estas conductas.

Por último, la transparencia algorítmica y las garantías democráticas fueron abordadas desde una perspectiva de derechos fundamentales por **miembros** de la sociedad civil. Colectivos ciudadanos advirtieron sobre los riesgos derivados del despliegue de sistemas automatizados de decisión, vigilancia preventiva, biometría y perfilado sin mecanismos adecuados de control democrático. Se señaló que la opacidad algorítmica dificulta que las personas afectadas comprendan, cuestionen o recurran decisiones que inciden directamente en sus derechos, comprometiendo principios como la presunción de inocencia, la proporcionalidad y la igualdad ante la ley. En este sentido, se reclamó la realización de evaluaciones de impacto en derechos humanos, la creación de registros públicos de algoritmos utilizados por las administraciones y el establecimiento de órganos de supervisión con participación de la sociedad civil. También se insistió en que la ciberseguridad no debe construirse desde una lógica exclusivamente securitaria, sino integrando la participación ciudadana, la rendición de cuentas y el principio de precaución.

En definitiva, las comparecencias evidenciaron que la dimensión social y de derechos constituye un eje transversal para la comprensión íntegra de la ciberseguridad contemporánea. La protección efectiva de las víctimas, la atención a las estafas emocionales, la salvaguarda de los menores y la garantía de transparencia y control democrático sobre las tecnologías emergentes son elementos indispensables para una estrategia de ciberseguridad que aspire no solo a proteger sistemas, sino también a preservar los derechos, la confianza institucional y la cohesión social en el entorno digital.

IV. CONCLUSIONES PRINCIPALES

Del conjunto de comparecencias celebradas en el seno de la Ponencia se desprende un diagnóstico compartido sobre la situación del entorno digital y los desafíos que plantea para la seguridad nacional, el funcionamiento de los servicios esenciales y la protección de la ciudadanía. Estas conclusiones no se articulan en torno a visiones individuales, sino que reflejan un diagnóstico compartido por **miembros** de las Fuerzas Armadas, Fuerzas y Cuerpos de seguridad, Administración Pública, sector privado, ámbito académico, operadores tecnológicos y sociedad civil. Todos ellos coincidieron en señalar la existencia de un riesgo sistémico creciente, derivado de la aceleración tecnológica, la expansión del cibercrimen y la consolidación del ciberespacio como un dominio estratégico de competencia permanente.

En primer lugar, los comparecientes han constatado que las amenazas digitales ya no pueden entenderse como incidentes aislados, sino como fenómenos estructurales que afectan simultáneamente a infraestructuras críticas, administraciones públicas, empresas y ciudadanos. El incremento sostenido de los ciberincidentes, la profesionalización del cibercrimen, la persistencia de amenazas avanzadas y el uso intensivo de tecnologías como la inteligencia artificial y, en perspectiva, la computación cuántica, configuran un escenario de presión continua que compromete la estabilidad operativa y la confianza en los sistemas digitales. Los datos aportados —como los más de 100.000 incidentes gestionados por el CCN en el sector público, los 83.000 incidentes en el sector privado o el incremento del 14,58 % en los procedimientos judiciales por ciberdelitos en 2024— evidencian que la amenaza no es coyuntural, sino estructural y en expansión. Esta

cve: BOCG-15-CG-A-223

caracterización del riesgo como transversal, acumulativo y persistente fue compartida de forma reiterada por los responsables de seguridad nacional, las Fuerzas y Cuerpos de Seguridad, el sector tecnológico y los operadores de servicios esenciales.

En segundo lugar, las intervenciones de los comparecientes pusieron de manifiesto que España dispone de capacidades relevantes en materia de ciberseguridad, tanto en el ámbito público como en el privado, incluyendo centros especializados, estructuras operativas, conocimiento técnico y experiencias de cooperación. No obstante, dichas capacidades aparecen dispersas, con distintos niveles de madurez, dependencia de marcos sectoriales o territoriales y ausencia de una visión plenamente integrada. Así, la coexistencia de múltiples actores con competencias en ciberseguridad —CCN, INCIBE, Mando Conjunto del Ciberespacio, fuerzas policiales, administraciones territoriales y operadores privados— ha permitido avances significativos, pero también ha generado solapamientos, duplicidades, ineficiencias, asimetrías territoriales y dificultades para obtener una visión integrada del riesgo y de la respuesta.

De ello se deriva la necesidad de reforzar la coordinación y avanzar hacia un marco común, tanto en términos estratégicos como operativos. De forma reiterada, los comparecientes reflejaron un amplio consenso sobre la importancia de articular mecanismos estables de cooperación interinstitucional, armonizar criterios entre niveles administrativos y consolidar espacios de colaboración público-privada que permitan compartir información, capacidades y buenas prácticas. Asimismo, han subrayado que la transposición y aplicación de marcos europeos, como la directiva NIS2, debe ir acompañada de una gobernanza clara, coherente y homogénea que evite solapamientos y vacíos de responsabilidad.

En tercer lugar, los comparecientes han destacado la prioridad estratégica de la soberanía tecnológica, entendida no solo como autonomía industrial, sino como capacidad de control, decisión y resiliencia sobre las tecnologías críticas que sustentan la seguridad digital. Buena parte de ellos alertó sobre la elevada dependencia de proveedores y tecnologías no europeas, especialmente en ámbitos clave como la ciberseguridad, las comunicaciones, la inteligencia artificial o la computación cuántica. Esta dependencia fue identificada como un factor de vulnerabilidad en un contexto de tensiones geopolíticas y de utilización del ciberespacio como instrumento de presión. En este contexto, se insistió en la necesidad de impulsar una base tecnológica propia, fomentar la industria nacional y europea y alinear las decisiones de inversión, contratación pública y regulación con objetivos de seguridad y soberanía; así como de garantizar el control sobre datos, sistemas y cadenas de suministro, especialmente en sectores críticos y en la Administración Pública.

En cuarto lugar, las comparecencias coincidieron en señalar la urgencia de reforzar la protección del ciudadano como eje central de las políticas de ciberseguridad. Las estafas digitales, la manipulación emocional, la explotación sexual de menores, la suplantación de identidad y la desinformación fueron identificadas como amenazas con un impacto directo y cotidiano sobre las personas, que generan daños económicos, psicológicos y sociales significativos. En este sentido, se destacó la necesidad de mejorar la atención a las víctimas, reducir las barreras a la denuncia, reforzar la formación y la concienciación, y garantizar que el desarrollo tecnológico se acompaña de salvaguardas efectivas de los derechos fundamentales**, planificando políticas de ciberseguridad centradas en la ciudadanía y la tradición de libertades públicas de la UE.**

En quinto lugar, las diferentes comparecencias pusieron de relieve la insuficiencia del marco jurídico-normativo actual para abordar algunas de las formas más recientes y sofisticadas de ciberdelincuencia. La Fiscalía General del Estado y otros comparecientes señalaron las limitaciones del Código Penal actual para abordar fenómenos como el *crime as a service*, las estafas complejas, el uso de criptomonedas o determinadas conductas facilitadas por la inteligencia artificial. En paralelo, se subrayó la importancia de reforzar las capacidades policiales y judiciales, tanto en medios técnicos como en formación especializada, para garantizar una persecución eficaz de estos delitos en un entorno transnacional. La lucha contra el cibercrimen fue presentada como una tarea estructural que requiere continuidad, especialización y respaldo normativo específico.

cve: BOCG-15-CG-A-223

En sexto y último lugar, varias intervenciones apuntaron a la necesidad de un modelo de financiación estable o de «financiación basal» que permita sostener en el tiempo las capacidades de ciberseguridad, tanto en el sector público como en los ecosistemas de innovación, formación e investigación. Varios expertos coincidieron en que las inversiones puntuales o ligadas a programas temporales no son suficientes para afrontar amenazas permanentes y en constante evolución. Por eso, más allá de programas concretos o fondos extraordinarios, los comparecientes destacaron la conveniencia de asegurar recursos estables para la protección de infraestructuras críticas, la modernización tecnológica de la Administración, la formación de profesionales, la retención de talento y el apoyo a pymes, evitando que la ciberseguridad dependa exclusivamente de iniciativas coyunturales o reactivas. **Ello exigiría, como muchos de los comparecientes reseñaron, políticas sistemáticas de ciencia y tecnología.**

En definitiva, las conclusiones de la Ponencia ponen de relieve que el principal desafío no radica únicamente en la existencia de amenazas, sino en la capacidad colectiva para identificarlas, priorizarlas y afrontarlas de forma coherente y coordinada, con especial atención tanto a la seguridad nacional como a la protección efectiva de la ciudadanía. Por todo ello, se propone que la ciberseguridad sea abordada como una política pública estructural, integrada en la seguridad nacional, la protección de derechos y la competitividad económica. Así, la combinación de riesgo creciente, capacidades existentes pero fragmentadas y brechas persistentes exige una respuesta coordinada, sostenida y centrada tanto en la resiliencia del Estado como en la protección efectiva de la ciudadanía.

V. RECOMENDACIONES

1. Recomendaciones tecnológicas.

Las comparecencias ponen de manifiesto un elevado grado de convergencia en torno a la necesidad de anticipar, reforzar y modernizar las capacidades tecnológicas de ciberseguridad, especialmente ante el impacto combinado de la inteligencia artificial y la computación cuántica.

En primer lugar, existe un consenso amplio sobre la urgencia de acelerar la transición hacia la criptografía poscuántica. Diversos comparecientes han subrayado que, aunque todavía no **se conozca la existencia de** un ordenador cuántico criptográficamente relevante, la amenaza es ya presente debido a la práctica de capturar información hoy para descifrarla en el futuro, lo que obliga a proteger desde ahora los datos cuya vida útil se extiende durante años. En este sentido, se recomienda iniciar de forma inmediata procesos de identificación de los sistemas y servicios que utilizan criptografía asimétrica, priorizando aquellos que protegen información sensible o infraestructuras críticas, y planificar una transición ordenada hacia algoritmos resistentes a la computación cuántica, siguiendo los estándares internacionales ya publicados por el NIST y las recomendaciones del Centro Criptológico Nacional. Algunos comparecientes insisten, además, en que esta transición debe ser gradual e híbrida, permitiendo la convivencia temporal de algoritmos clásicos y poscuánticos para no comprometer la continuidad de los servicios esenciales.

En todo caso, se pone de manifiesto que cualquier estrategia de transición hacia criptografía postcuántica debe partir necesariamente de un inventario completo de los sistemas, protocolos y algoritmos criptográficos en uso, tanto en la protección de datos en reposo como en las comunicaciones. Este ejercicio previo es considerado esencial para priorizar activos críticos, planificar la migración y evitar riesgos operativos durante el proceso. **Y debe garantizarse con un conocimiento previo mapeando en forma de cartografía y análisis institucional la estructura global que afecta a la ciberseguridad.**

En segundo lugar, los expertos coinciden en recomendar un uso intensivo y estratégico de la inteligencia artificial aplicada a la ciberseguridad, tanto para la detección temprana de amenazas como para la automatización de la respuesta a incidentes. Se destaca que la integración de IA en los centros de operaciones de seguridad permite pasar de modelos reactivos a enfoques proactivos, reducir la carga manual de los analistas y acelerar los

cve: BOCG-15-CG-A-223

tiempos de respuesta, disminuyendo así el impacto de los incidentes. Asimismo, se señala que la IA puede contribuir a mitigar el déficit de talento, al incorporar conocimiento experto directamente en las herramientas de seguridad y facilitar la toma de decisiones por parte de equipos menos especializados.

En tercer lugar, con respecto al refuerzo de la soberanía tecnológica, existe consenso acerca de la necesidad de impulso a capacidades industriales y tecnológicas propias. Algunos comparecientes sostienen de forma explícita que España dispone de talento suficiente para desarrollar soluciones avanzadas de ciberseguridad, pero alertan del riesgo de que estas capacidades sean absorbidas por multinacionales extranjeras si no existe una política decidida de inversión y apoyo a la industria nacional.

En esta línea, se recomienda fomentar la creación y consolidación de empresas españolas de ciberseguridad, así como priorizar tecnologías desarrolladas en el ámbito europeo o nacional cuando sea posible, especialmente en sectores sensibles para la seguridad nacional. Del mismo modo, la localización en territorio nacional de infraestructuras tecnológicas estratégicas, centros de análisis de amenazas y capacidades avanzadas de ciberseguridad contribuye de forma directa a la soberanía digital, a la retención de talento y al fortalecimiento del ecosistema nacional.

En cuarto lugar, algunos comparecientes sugieren la conveniencia de simplificar las arquitecturas tecnológicas, reducir la fragmentación de herramientas y avanzar hacia plataformas integradas que faciliten la gestión, la automatización y la respuesta coordinada a incidentes.

Otros, sin embargo, advierten implícitamente del riesgo de una excesiva concentración tecnológica, señalando la importancia de evitar dependencias críticas de un único proveedor o tecnología. Desde esta perspectiva, se recomienda mantener una diversidad controlada de soluciones, que incremente la resiliencia y reduzca el impacto de fallos sistémicos o vulnerabilidades explotables de forma masiva.

Por otro lado, varios expertos proponen incrementar de forma sostenida la inversión en infraestructuras digitales y de ciberseguridad, tanto en el ámbito civil como en el de la defensa; señalando que la tecnología comercial de alto nivel, basada en estándares abiertos y soluciones *best of breed*[23], constituye un factor crítico para el éxito de los programas de seguridad.

Se advierte, no obstante, de que la actualización tecnológica se enfrenta a ciclos de vida largos en infraestructuras críticas, lo que refuerza la necesidad de anticipación y planificación temprana, especialmente en materia criptográfica.

En quinto y último lugar, se formulan recomendaciones orientadas a potenciar la colaboración tecnológica entre sector público, sector privado y ámbito académico. Se destaca el valor de los proyectos piloto, los entornos de validación real y la cooperación con organismos públicos para probar nuevas tecnologías antes de su despliegue generalizado, como vía para reducir riesgos y acelerar la adopción de soluciones avanzadas. Asimismo, algunos comparecientes sugieren reforzar el papel de las universidades y de los programas de investigación aplicada en ciberseguridad y tecnologías de uso dual, con el objetivo de transferir conocimiento al tejido productivo y fortalecer las capacidades nacionales a medio y largo plazo.

En definitiva, se recomienda:

— Acelerar la transición hacia la criptografía poscuántica, ante la amenaza futura para datos cuya vida útil se extiende durante años, iniciando la identificación prioritaria de sistemas críticos y sensibles.

— Planificar una migración gradual e híbrida hacia algoritmos poscuánticos, permitiendo la convivencia temporal con la criptografía clásica para garantizar la continuidad de los servicios esenciales.

— Integrar de forma intensiva y estratégica la inteligencia artificial en la detección, análisis y respuesta a incidentes de ciberseguridad, con el fin de mejorar la anticipación, reducir tiempos de reacción y mitigar la escasez de talento.

cve: BOCG-15-CG-A-223

— Acompañar el despliegue de inteligencia artificial con medidas específicas de seguridad y control, especialmente en entornos críticos, ante su potencial uso malintencionado.

— Impulsar la soberanía tecnológica, fomentando capacidades industriales y tecnológicas propias y evitando la pérdida de talento nacional hacia actores externos.

— Simplificar y racionalizar las arquitecturas tecnológicas, reduciendo la fragmentación de herramientas, sin generar dependencias críticas de un único proveedor.

— Incrementar de forma sostenida la inversión en infraestructuras digitales y de ciberseguridad, teniendo en cuenta los largos ciclos de vida tecnológica en infraestructuras críticas.

— **Desarrollar un «Programa de Atribución», como conjunto organizado de capacidades técnicas, jurídicas y estratégicas que permite a un Estado —o a una organización— determinar con un grado razonable de certeza la autoría de un ciberataque.**

2. Recomendaciones institucionales.

Las comparecencias coinciden en atribuir a las instituciones públicas un papel central e insustituible en la configuración del ecosistema nacional de ciberseguridad. No obstante, las recomendaciones formuladas muestran distintos énfasis sobre cómo deben ejercer ese liderazgo, qué funciones deben priorizar y hasta dónde debe llegar la intervención pública.

En primer lugar, un bloque significativo de comparecientes recomienda que el Estado asuma un liderazgo estratégico claro, evitando la dispersión institucional y la superposición de competencias. Se insiste en la necesidad de definir con precisión qué organismos son responsables de qué funciones, especialmente en materia de prevención, respuesta a incidentes, supervisión normativa y cooperación internacional.

Desde esta perspectiva, se propone que las instituciones públicas actúen como arquitectos del sistema, estableciendo marcos comunes, estándares mínimos y mecanismos de coordinación estables entre ministerios, agencias especializadas, comunidades autónomas y entidades locales. La recomendación no se limita a mejorar la cooperación informal, sino a institucionalizarla mediante estructuras permanentes, con capacidad de decisión y continuidad temporal.

Frente a esta visión, otros comparecientes, sin cuestionar la necesidad de coordinación, ponen el acento en no ralentizar la acción operativa mediante una excesiva recentralización, defendiendo que determinados organismos técnicos ya cuentan con experiencia suficiente y deben conservar autonomía funcional para responder con agilidad a incidentes concretos. Esta diferencia no es de fondo, sino de grado y modelo de gobernanza.

En segundo lugar, existe una recomendación ampliamente compartida de que las instituciones públicas no se limiten a transponer directivas europeas, sino que lo hagan de manera clara, coherente y adaptada a la realidad operativa del país. En este sentido, varios comparecientes subrayan que la eficacia normativa depende menos de la ambición del texto legal y más de su comprensibilidad, aplicabilidad y capacidad de supervisión real.

Algunos expertos recomiendan que las Administraciones Públicas acompañen la normativa de instrumentos de apoyo práctico, especialmente para sectores con menor capacidad técnica. Otros van más e insisten en que los marcos normativos deben permitir ajustes en su aplicación para evitar que el cumplimiento formal sustituya a la seguridad efectiva.

Como matiz diferenciador, ciertos comparecientes del ámbito empresarial alertan de que una sobrerregulación o una trasposición excesivamente rígida puede generar efectos contraproducentes, como el cumplimiento meramente formal o la exclusión de actores pequeños del sistema. Desde esta posición se recomienda a las instituciones públicas priorizar la eficacia sobre la exhaustividad normativa.

En tercer lugar, varios comparecientes coinciden en que las instituciones públicas deben reforzar de forma decidida sus capacidades de supervisión e inspección, señalando que la ausencia de controles efectivos debilita cualquier marco normativo. Se recomienda dotar a los organismos competentes de medios humanos, técnicos y presupuestarios suficientes para ejercer estas funciones de manera homogénea en todo el territorio.

cve: BOCG-15-CG-A-223

No obstante, se aprecian diferencias en el énfasis: mientras algunos consideran que la prioridad debe ser el acompañamiento y la mejora progresiva del cumplimiento, otros sostienen que sin una capacidad sancionadora creíble, el sistema pierde eficacia disuasoria. Esta divergencia refleja dos aproximaciones distintas: una más pedagógica y otra más coercitiva, ambas presentes en las comparecencias.

En cuarto lugar, se recomienda de manera clara y reiterada a las instituciones públicas situar al ciudadano en el centro de las políticas de ciberseguridad, no solo como usuario a proteger, sino como sujeto de derechos. Se subraya la necesidad de mejorar los mecanismos de atención a víctimas, simplificar los canales de denuncia y garantizar un trato empático y especializado por parte de las administraciones y las fuerzas de seguridad.

Algunos comparecientes proponen que las instituciones públicas asuman un papel activo en la prevención mediante campañas de concienciación sostenidas, no puntuales, y adaptadas a colectivos específicos. Otros inciden en la necesidad de reforzar la formación especializada de jueces, fiscales y policías, recomendando que esta formación sea estructural y no dependiente de iniciativas aisladas.

En quinto lugar, una recomendación institucional concreta y relevante es la creación o consolidación de mecanismos públicos de registro de incidentes de ciberseguridad, que permitan disponer de una visión real y agregada del fenómeno. Varios comparecientes señalan que sin datos fiables, comparables y centralizados, las políticas públicas se diseñan sobre percepciones parciales. Del mismo modo, se recomendó preservar y reforzar el principio de «ventanilla única» sectorial para la notificación de incidentes de ciberseguridad, de modo que las entidades afectadas dispongan de canales claros y coordinados para comunicar incidentes sin generar duplicidades ni cargas administrativas adicionales.

Algunos comparecientes señalaron la ausencia de un registro completo y homogéneo de ciberincidentes, apuntando a la directiva NIS2 como un instrumento que podría contribuir a subsanar esta carencia. Aunque no se plantearon modelos concretos, las comparecencias evidenciaron la necesidad de avanzar hacia sistemas de registro más completos y fiables.

En sexto lugar, existe consenso en que la colaboración público-privada debe reforzarse, pero las recomendaciones difieren en el modelo institucional. Algunos comparecientes defienden la creación de marcos formales, estables y reglados. Otros, sin embargo, recomiendan preservar espacios de cooperación flexible, alertando de que un exceso de formalización puede dificultar el intercambio ágil de información sensible; una divergencia que puede reflejar una tensión entre seguridad jurídica y operatividad.

En séptimo y último lugar, varios comparecientes recomiendan que las instituciones públicas avancen hacia modelos de financiación estables y estructurales, evitando depender exclusivamente de convocatorias puntuales o fondos extraordinarios. Se subraya que la ciberseguridad requiere continuidad presupuestaria, tanto para mantener capacidades como para retener talento. Aquí también se aprecian matices: mientras algunos reclaman un incremento sostenido del gasto público, otros ponen el acento en optimizar la inversión existente, priorizando proyectos con impacto operativo directo.

En definitiva, se recomienda:

— Reforzar el liderazgo estratégico del Estado, evitando la dispersión institucional y clarificando responsabilidades en prevención, respuesta, supervisión y cooperación internacional.

— **Impulsar la trasposición de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (NIS 2) al ordenamiento jurídico español, para acelerar la creación del Centro Nacional de Ciberseguridad.**

— Establecer marcos comunes y mecanismos estables de coordinación entre administraciones, organismos especializados y niveles territoriales.

cve: BOCG-15-CG-A-223

— Garantizar una trasposición normativa clara, coherente y operativa, adaptada a la realidad del tejido productivo y evitando enfoques excesivamente rígidos.

— Acompañar la normativa con instrumentos prácticos de apoyo, especialmente para sectores con menor capacidad técnica.

— Reforzar las capacidades de supervisión e inspección, dotando a los organismos competentes de medios suficientes y homogéneos.

— Situar al ciudadano y a las víctimas en el centro de las políticas públicas de ciberseguridad, mejorando la atención, la denuncia y el trato especializado.

— Impulsar campañas de concienciación sostenidas y reforzar la formación estructural de jueces, fiscales y fuerzas de seguridad.

— Avanzar hacia sistemas de registro de ciberincidentes más completos y fiables, apoyándose en el marco de la NIS2.

— Evolucionar hacia modelos de financiación estables y estructurales, evitando la dependencia de fondos puntuales.

— **Impulsar todas las modificaciones legislativas necesarias para fortalecer el papel del Estado en ciberseguridad a través de la concentración de las competencias en dicha materia y siguiendo los principios básicos de unidad de acción y eficiencia.**

— **Impulsar la creación de empresas privadas nacionales especializadas en el ámbito de la ciberseguridad.**

— **Definir una nueva Estrategia de Seguridad Nacional que integre Defensa, Interior e Inteligencia, con el objeto de prevenir y evitar eficazmente cualquier peligro, amenaza o agresión contra la independencia o la integridad territorial de España, los intereses nacionales, las infraestructuras críticas, ciberseguridad y soberanía de datos, soberanía industrial y energética, recursos naturales, así como la estabilidad del Estado de Derecho y sus instituciones.**

— **Promover la cooperación público-privada en la lucha contra la ciberdelincuencia.**

3. Recomendaciones sociales.

Las comparecencias incorporaron un conjunto de recomendaciones sociales expresas, centradas principalmente en la protección de las víctimas, la prevención del delito, la formación ciudadana y la salvaguarda de derechos fundamentales en el entorno digital.

En primer lugar, en relación con la protección de las víctimas, varios comparecientes recomiendan mejorar la atención institucional a las personas afectadas por ciberdelitos, subrayando la necesidad de un trato empático y especializado. **Miembros** de asociaciones de víctimas señalaron expresamente que muchas personas no denuncian por vergüenza, culpabilidad o falta de comprensión por parte del entorno institucional, y recomiendan que las Fuerzas y Cuerpos de Seguridad del Estado reciban formación específica para atender adecuadamente a las víctimas, especialmente en casos de estafas emocionales y fraude digital. Esta recomendación se formuló de manera explícita, vinculándola a la necesidad de generar confianza y facilitar la denuncia.

En segundo lugar, en el ámbito de la prevención y concienciación ciudadana, varios comparecientes recomiendan reforzar la alfabetización digital desde edades tempranas, señalando que la formación es una herramienta esencial para reducir la vulnerabilidad frente al fraude, la desinformación y otros delitos digitales. Se propone expresamente incorporar contenidos de ciberseguridad en el sistema educativo, así como desarrollar programas de formación dirigidos a la población general y a colectivos especialmente expuestos. Esta recomendación es formulada tanto desde el sector privado como desde asociaciones y expertos en criminalidad digital.

En este sentido, algunos comparecientes aportaron referencias a experiencias comparadas en otros países europeos. Se mencionaron iniciativas desarrolladas en Francia, Alemania, Reino Unido e Italia que combinan campañas masivas de concienciación, simulaciones prácticas de phishing, guías sencillas para la ciudadanía y la implicación de entidades financieras y organismos públicos. Estas experiencias ponen de relieve la eficacia

cve: BOCG-15-CG-A-223

de enfoques sostenidos en el tiempo, adaptados a distintos públicos y articulados en torno a hitos comunes como el Mes Europeo de la Ciberseguridad.

En tercer lugar, respecto a las estafas emocionales, se recomienda visibilizar socialmente este fenómeno, evitando la estigmatización de las víctimas. Desde asociaciones especializadas se insiste en que este tipo de delitos debe ser reconocido como una forma específica de criminalidad digital, con un fuerte componente psicológico, y se recomienda que las campañas de sensibilización expliquen sus mecanismos para prevenir nuevos casos. Asimismo, se destaca la conveniencia de fomentar una mayor empatía social hacia las personas afectadas.

En cuarto lugar, en relación con la protección de menores, la Fiscalía y otros comparecientes recomiendan reforzar las medidas de prevención y detección de delitos sexuales en entornos digitales, subrayando la necesidad de dotar a los operadores jurídicos y policiales de medios adecuados. Se valoró positivamente la adopción de iniciativas normativas orientadas a la protección integral de los menores en Internet y se recomienda continuar avanzando en este ámbito. Asimismo, se señala la importancia de la formación de familias, docentes y profesionales que trabajan con menores, como elemento clave de prevención.

En quinto lugar, en cuanto a la gobernanza de la tecnología y los derechos fundamentales, **miembros** de la sociedad civil recomiendan incorporar la participación ciudadana en el diseño de políticas públicas relacionadas con la inteligencia artificial y la ciberseguridad. Se propone de manera expresa la creación de espacios de participación y órganos consultivos con presencia de organizaciones sociales, así como la realización de evaluaciones de impacto en derechos humanos antes del despliegue de tecnologías sensibles. Estas recomendaciones se formulan con el objetivo de garantizar la transparencia, la rendición de cuentas y la protección de colectivos vulnerables.

En sexto y último lugar, se recomienda incrementar la transparencia en el uso de sistemas algorítmicos por parte de las Administraciones Públicas, proponiéndose la creación de registros públicos de algoritmos y mecanismos de supervisión ética independientes. Estas propuestas se presentan como medidas necesarias para asegurar que la ciberseguridad y el uso de tecnologías avanzadas no erosionen derechos fundamentales ni principios democráticos.

En definitiva, se recomienda:

— Mejorar la protección y atención a las víctimas de ciberdelitos, incorporando formación específica y enfoque empático en los cuerpos policiales.

— Combatir la infradenuncia, especialmente en estafas emocionales, mediante sensibilización social y eliminación del estigma.

— Reforzar la alfabetización digital desde edades tempranas e incorporar contenidos de ciberseguridad en el sistema educativo.

— Visibilizar y prevenir de forma específica las estafas emocionales, reconociendo su componente psicológico.

— Intensificar las medidas de protección de menores en entornos digitales, reforzando la prevención, detección y medios de investigación.

— Incorporar la participación de la sociedad civil en el diseño de políticas de ciberseguridad e inteligencia artificial.

— Garantizar la transparencia algorítmica, mediante registros públicos, evaluaciones de impacto en derechos humanos y supervisión ética independiente.

4. Recomendaciones económicas y de mercado.

Las comparecencias incluyeron un conjunto de recomendaciones económicas y de mercado explícitas, centradas en el funcionamiento del sector de la ciberseguridad, la contratación pública, el tejido empresarial (especialmente las pymes) y el desarrollo de una industria nacional competitiva.

En primer lugar, una de las recomendaciones más reiteradas se refiere a la necesidad de reformar los criterios de contratación pública de servicios tecnológicos y de ciberseguridad.

cve: BOCG-15-CG-A-223

Varios comparecientes señalan de forma expresa que no debería primarse el precio como criterio principal en los procedimientos de contratación, advirtiendo de que el ahorro económico a corto plazo puede resultar contraproducente en términos de seguridad, calidad del servicio y resiliencia. Se recomienda que las Administraciones Públicas valoren de manera prioritaria la calidad técnica, la solvencia del proveedor, la continuidad del servicio y la capacidad de respuesta ante incidentes, especialmente en sectores críticos y servicios esenciales.

En segundo lugar, algunos comparecientes recomiendan adaptar los procedimientos de contratación pública para facilitar el acceso de pequeñas y medianas empresas al mercado de la ciberseguridad. Algunos de ellos señalaron que los contratos públicos suelen configurarse en lotes de gran dimensión, lo que dificulta o impide la participación de empresas pequeñas y medianas, incluidas aquellas que desarrollan tecnología española con alto valor añadido. Asimismo, se advirtió de que, en los procedimientos de contratación, el criterio económico —especialmente el precio de la oferta— suele tener un peso determinante, lo que puede resultar contraproducente en sectores críticos desde el punto de vista de la seguridad, al priorizar el menor coste frente a la calidad técnica, la resiliencia de las soluciones o la solvencia del proveedor. A partir de estas consideraciones, los comparecientes pusieron de relieve la conveniencia de ajustar los mecanismos de contratación pública para favorecer una mayor concurrencia, permitir la participación de empresas nacionales de menor tamaño y asegurar que los criterios técnicos y de seguridad tengan un peso adecuado en la adjudicación de contratos en ámbitos sensibles.

De forma expresa, se propone dividir los contratos en lotes más pequeños, de modo que las pymes puedan concurrir a licitaciones que actualmente quedan fuera de su alcance por volumen o requisitos desproporcionados. Esta recomendación es formulada como una medida concreta para fomentar la competencia, diversificar proveedores y evitar una excesiva concentración del mercado.

En tercer lugar, otra recomendación relevante se centró en la ordenación del sector de la ciberseguridad, que algunos comparecientes describieron como **descoordinado** y carente de mecanismos homogéneos de acreditación. Se recomienda establecer sistemas de acreditación profesional y empresarial, con el objetivo de diferenciar a los proveedores cualificados, elevar los estándares del mercado y generar confianza tanto en clientes públicos como privados. Esta propuesta se vincula expresamente a la necesidad de evitar prácticas oportunistas y de garantizar que las inversiones en ciberseguridad generen valor real.

En cuarto lugar, en relación con las pequeñas y medianas empresas, varios comparecientes recomiendan articular incentivos económicos y mecanismos de apoyo que faciliten la adopción de medidas de ciberseguridad. Se subrayó que las pymes constituyen la base del tejido productivo, pero carecen a menudo de recursos suficientes para asumir los costes de protección digital. En este contexto, se propone que las políticas públicas incorporen incentivos que favorezcan la inversión en seguridad, evitando que el cumplimiento normativo se convierta en una carga inasumible.

En quinto lugar, se proponen recomendaciones orientadas a evitar la concentración tecnológica en un único proveedor, tanto en el ámbito público como en el privado. Algunos comparecientes advirtieron del riesgo que supone depender de un solo suministrador para servicios críticos, recomendando diversificar proveedores y promover arquitecturas tecnológicas que reduzcan vulnerabilidades sistémicas derivadas de fallos o incidentes en una única plataforma.

En sexto lugar, otra recomendación económica explícita se refiere a la retención del talento en el sector público y en el ecosistema nacional de ciberseguridad. Varios comparecientes señalaron que la competencia del mercado privado y de empresas internacionales dificulta la permanencia de profesionales cualificados en organismos públicos y empresas nacionales. En este sentido, se recomienda revisar las condiciones económicas y profesionales, así como articular incentivos que permitan atraer y retener talento, especialmente en áreas críticas. En cualquier caso, la profesionalización del sector de la ciberseguridad no debe apoyarse únicamente en la acreditación individual de profesionales, sino también en el fortalecimiento organizativo de las empresas, la adopción

cve: BOCG-15-CG-A-223

de buenas prácticas comunes y el desarrollo de modelos de madurez que permitan ordenar el sector de forma coherente y sostenible.

En séptimo y último lugar, algunos comparecientes alertaron sobre el riesgo de una burbuja especulativa en el sector de la ciberseguridad, impulsada por fondos de inversión que no siempre generan valor sostenible. Por ello, se recomienda orientar las políticas económicas hacia el desarrollo de capacidades reales y duraderas, priorizando proyectos que refuercen la autonomía tecnológica, la calidad del empleo y la estabilidad del mercado, frente a estrategias de corto plazo.

En definitiva, se recomienda:

— Reformar la contratación pública tecnológica, evitando que el precio sea el criterio principal y priorizando calidad, solvencia y resiliencia.

— Facilitar el acceso de pymes al mercado público de ciberseguridad mediante la división de contratos en lotes más pequeños.

— Ordenar el sector mediante sistemas de acreditación profesional y empresarial, elevando estándares y confianza.

— Articular incentivos económicos que permitan a las pymes adoptar medidas de ciberseguridad sin cargas desproporcionadas.

— Evitar la concentración tecnológica excesiva y diversificar proveedores en servicios críticos.

— Mejorar la retención de talento, revisando condiciones económicas y profesionales en el sector público y **nacional**.

— Orientar las políticas económicas hacia el desarrollo de capacidades reales y sostenibles, evitando dinámicas especulativas de corto plazo.

— Avanzar hacia la definición de listas o catálogos de proveedores tecnológicos seguros o de confianza para su utilización en sectores críticos y en el ámbito de las Administraciones Públicas, tomando como referencia experiencias previas como el despliegue de las redes 5G y aplicando criterios objetivos de evaluación del riesgo, fiabilidad del suministro y protección de la seguridad nacional.

— **Impulsar la economía social de la ciberseguridad y el cooperativismo en el desarrollo tecnológico para las pymes.**

— **Aumentar los recursos, tanto materiales como de personal, de los organismos del Estado que tienen competencias en materia de ciberseguridad, en especial del Centro Criptológico Nacional.**

5. Recomendaciones estratégicas.

Las comparecencias de la Ponencia incorporan un conjunto limitado pero significativo de recomendaciones de carácter estratégico, formuladas de manera expresa por distintos comparecientes desde ámbitos institucionales, operativos y tecnológicos. Estas recomendaciones no se refieren a instrumentos concretos ni a medidas sectoriales, sino a cómo debe concebirse, priorizarse y sostenerse la política de ciberseguridad en su conjunto, y aportan un valor añadido al informe al situar las decisiones en un marco de largo alcance.

En primer lugar, varios comparecientes recomiendan abordar la ciberseguridad como una política de Estado y un elemento estructural de la seguridad nacional, y no como un ámbito técnico o sectorial. Desde el ámbito de la Defensa, la Seguridad Nacional y los operadores críticos se afirmó de forma expresa que el ciberespacio constituye un dominio estratégico del que dependen el funcionamiento del país, la continuidad de los servicios esenciales y la protección de la ciudadanía. En este sentido, se recomienda integrar la ciberseguridad en los marcos generales de seguridad y defensa, evitando enfoques fragmentados o coyunturales.

En segundo lugar, se formula la recomendación de adoptar una visión integral y transversal del ecosistema de ciberseguridad, superando la separación entre ámbitos civiles y militares, públicos y privados, nacionales y supranacionales. Varios comparecientes señalaron expresamente que las amenazas digitales no respetan compartimentos

cve: BOCG-15-CG-A-223

organizativos ni fronteras administrativas, y que la respuesta debe articularse de manera coordinada entre Administraciones, Fuerzas de Seguridad, sector privado y socios internacionales. Esta recomendación estratégica se plantea como un principio rector para el diseño de políticas y estructuras, más allá de mecanismos concretos de coordinación ya tratados en otros apartados.

En tercer lugar, diversos expertos recomiendan priorizar la anticipación estratégica frente a la reacción, subrayando que el principal riesgo no reside únicamente en las amenazas existentes, sino en la falta de preparación ante amenazas previsibles. En particular, se señaló que no prepararse a tiempo frente a tecnologías emergentes como la computación cuántica o la inteligencia artificial supone una desventaja estratégica frente a actores tecnológicos. Esta recomendación se formula explícitamente en términos de enfoque: la ciberseguridad debe basarse en la previsión y la planificación a medio y largo plazo, y no únicamente en la gestión reactiva de incidentes.

En cuarto lugar, se reitera como recomendación estratégica la alineación de la política nacional de ciberseguridad con los marcos europeos e internacionales, especialmente en el ámbito de la Unión Europea y de la OTAN. Algunos comparecientes subrayan la importancia de actuar de forma coherente con las estrategias, estándares y marcos de cooperación existentes, evitando soluciones aisladas que dificulten la interoperabilidad o la cooperación internacional. Esta alineación se recomienda tanto desde una perspectiva de eficacia operativa como de posicionamiento estratégico de España en el entorno internacional.

En quinto lugar, varios comparecientes destacan la Red Nacional de SOC **(Centros de Operaciones de Seguridad)** como un activo clave para la defensa proactiva del país, al facilitar el intercambio de información técnica, indicadores de compromiso y alertas tempranas entre organismos públicos y proveedores tecnológicos. Asimismo, se subraya la importancia de consolidar su conexión con iniciativas europeas, como la futura Red Europea de SOC, para reforzar la capacidad de detección y respuesta frente a amenazas transnacionales.

En sexto y último lugar, se formula la recomendación de garantizar la continuidad temporal y la estabilidad de las políticas de ciberseguridad, evitando enfoques discontinuos o dependientes de coyunturas concretas. Varios comparecientes advirtieron de que las amenazas digitales son permanentes y evolucionan de forma constante, por lo que las respuestas basadas en programas puntuales, proyectos aislados o reacciones tras incidentes resultan insuficientes. En este contexto, se recomienda dotar a la ciberseguridad de una planificación sostenida en el tiempo, con prioridades claras y recursos estables, como condición necesaria para la eficacia estratégica.

En definitiva, se recomienda:

— Tratar la ciberseguridad como una política de Estado, integrada en la seguridad nacional y no como un ámbito técnico sectorial.

— Adoptar una visión integral y transversal del ecosistema de ciberseguridad, superando compartimentos administrativos y organizativos.

— Priorizar la anticipación estratégica frente a la reacción, especialmente ante tecnologías emergentes.

— Alinear la política nacional con los marcos europeos e internacionales (UE y OTAN), garantizando interoperabilidad y coherencia.

— Asegurar la continuidad temporal y estabilidad de las políticas de ciberseguridad, con planificación sostenida y recursos estables.

— **Promover en el seno de la Unión Europea la adopción de medidas destinadas a reforzar la ciberseguridad de las redes e instituciones públicas de los Estados miembros frente a posibles ataques cibernéticos efectuados por parte de potencias o actores extranjeros.**

— **Prohibir la adjudicación de contratos de servicios que afecten a la Seguridad Nacional a empresas que sean consideradas como «proveedores de alto riesgo», siguiendo la Comunicación de la Comisión Europea C (2023) 4049 y la propuesta de revisión de la Cybersecurity Act (CSA) presentada por la Comisión Europea el 20 de enero de 2026.**

cve: BOCG-15-CG-A-223

VI. RELACIÓN DE COMPARECIENTES

Los contenidos expuestos en el presente Informe derivan del amplio programa de comparecencias recogido en los trabajos de la Ponencia, con el objetivo de recabar aportaciones expertas, plurales y complementarias sobre las amenazas en el ciberespacio en la era de la inteligencia artificial y de la computación cuántica.

A tal efecto, fueron llamados a comparecer responsables institucionales, **miembros** de las Fuerzas Armadas y de las Fuerzas y Cuerpos de Seguridad del Estado, directivos de empresas tecnológicas y operadores de infraestructuras críticas, así como **miembros** de organizaciones de la sociedad civil y expertos independientes.

Esta diversidad de perfiles permitió abordar el fenómeno desde una perspectiva integral, incorporando dimensiones estratégicas, operativas, económicas, jurídicas y sociales. A efectos expositivos y metodológicos, los comparecientes se agrupan a continuación en función de su adscripción profesional, sin perjuicio del carácter transversal de muchas de las aportaciones realizadas.

Con respecto a RESPONSABLES INSTITUCIONALES:

— D. Félix Barrio Juárez. Director General del Instituto Nacional de Ciberseguridad de España (INCIBE).

— General de Brigada Dña. Loreto Gutiérrez Hurtado. Directora del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno.

— Dña. María Elvira Tejada de la Fuente. Fiscal de Sala Coordinadora contra la Criminalidad Informática de la Fiscalía General del Estado.

Con respecto a **MIEMBROS** DE LAS FUERZAS ARMADAS Y DE LAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO:

— Vicealmirante D. Francisco Javier Roca Rivera. Comandante del Mando Conjunto del Ciberespacio.

— Capitán de Fragata D. Luis de Medina Redondo. Consejero Adjunto de Defensa para Asuntos Digitales (C3) de la Representación Permanente de España ante la OTAN.

— Coronel D. Juan Rodríguez Álvarez de Sotomayor. Jefe del Departamento contra el Cibercrimen de la Guardia Civil.

— Dña. Laura Baos Espada. Jefa de Brigada Operativa en la Comisaría General de Información de la Policía Nacional.

Con respecto a DIRECTIVOS DE EMPRESAS TECNOLÓGICAS Y OPERADORES DE INFRAESTRUCTURAS CRÍTICAS:

— D. Mikel Díez. Director de IBM Quantum España y Portugal.

— D. Joan Farnós. Responsable de Innovación y Tecnologías Duales del Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC-CNS).

— D. Marc Sarrias. Director General de Palo Alto Networks para España y Portugal.

— D. Mario García Setién. Director General de Check Point para España y Portugal.

— D. David Fernández Granado. Director de Ciberseguridad de Prosegur.

— **D. Jorge Blanco. Director de la oficina del CISO de Google Cloud en Iberia y Latinoamérica.**

— **D. Andreu Vilamitjana. Director General de España y Portugal de CISCO.**

— D. Jorge Coronado Díaz. Fundador y *CEO* de Quantika14.

— D. José Miguel Rosell Tejada. Socio fundador y *CEO* de S2 Grupo.

— D. Francisco Javier Amores García. Director de Ciberseguridad de MasOrange.

— Dña. María Jesús Almazor Marsal. *Chief Operating Officer* (COO) para España y América de Telefónica Tech.

— D. Roberto Espina Manchón. Director Global de Ciberseguridad de IndraMind.

cve: BOCG-15-CG-A-223

Con respecto a **MIEMBROS** DE ORGANIZACIONES DE LA SOCIEDAD CIVIL Y EXPERTOS INDEPENDIENTES:

— D. Roberto Baratta. Presidente de la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum).

— Dña. Judith Membrives i Llorens. Representante y portavoz de la coalición Inteligencia Artificial Ciudadana (IA Ciudadana).

— Dña. Blanca Frías. Presidenta de la Asociación Nacional contra la Estafa con Manipulación Emocional (ANCEME).

— Dña. Paz Velasco de la Fuente. Jurista, criminóloga y experta en criminalidad digital.

---

[1] Véase *SECCIÓN VI: Relación de comparecientes.*

[2] Ciberataque de suplantación de identidad donde delincuentes se hacen pasar por entidades legítimas (bancos, redes sociales) mediante correos, mensajes o llamadas fraudulentas para engañar a las víctimas y robarles información confidencial (contraseñas, datos bancarios) o instalar malware, utilizando la ingeniería social para generar urgencia y conseguir que la víctima revele sus datos en sitios web falsos.

[3] Amenaza persistente avanzada, también conocida por sus siglas en inglés, APT (*Advanced Persistent Threat*). Término que alude al conjunto de procesos informáticos sigilosos orquestados por actores sofisticados (a menudo patrocinados por Estados) para infiltrarse en redes, robar datos valiosos o sabotear sistemas sin ser detectados, usando técnicas como *phishing* o *malware* personalizado para lograr sus objetivos durante meses o años.

[4] Conjunto de conductas y acciones emprendidas por adultos a través de Internet con el objetivo deliberado de ganarse la amistad de menores de edad, creando una conexión emocional con los mismos, con el fin de ganarse su confianza y poder chantajear emocionalmente y abusar sexualmente de ellos. En algunos casos se puede buscar la introducción del menor al mundo de la prostitución infantil o la producción de material pornográfico.

[5] Tecnología Operativa (OT): *hardware* y *software* que monitoriza y controla sistemas físicos y procesos industriales (como fábricas, energía, transporte). A diferencia de la IT (Tecnología de la Información) que gestiona datos; la OT se enfoca en la fiabilidad, disponibilidad y seguridad de las operaciones físicas.

[6] Programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado para luego pedir un rescate a cambio del acceso al mismo. En 2023, el INCIBE gestionó 621 incidentes de este tipo, en un contexto de incremento global del 73 %. Se destacó que un 83 % de las víctimas optaron por pagar el rescate, y que dos variantes concretas, *LockBit* y *BlackCat*, concentraron conjuntamente el 38 % de los ataques registrados, lo que evidencia un elevado grado de concentración y profesionalización de esta amenaza.

[7] Vídeos, imágenes o audios que han sido manipulados, normalmente con el objetivo de suplantar la identidad de alguien. Utilizando inteligencia artificial (IA), los ciberdelincuentes pueden superponer el rostro de una persona o clonar su voz para que parezca que dice o hace algo que no se corresponde con la realidad.

[8] *National Institute of Standards and Technology*, agencia pública dependiente del Departamento de Comercio de los Estados Unidos.

[9] Algunos comparecientes aportaron, además, propuestas metodológicas concretas para abordar esta transición. En particular, se destacó la conveniencia de adoptar estrategias denominadas «cripto-ágiles», basadas en un proceso ordenado que incluya, en primer lugar, un inventario completo de activos, sistemas y servicios que utilizan criptografía; en segundo término, la definición de una estrategia de priorización y selección de algoritmos; posteriormente, fases de prueba e interoperabilidad entre soluciones de distintos fabricantes; y, finalmente, un despliegue progresivo que permita la convivencia temporal de algoritmos clásicos y poscuánticos. Este enfoque permitiría minimizar riesgos y evitar interrupciones en servicios esenciales.

[10] *Quantum Key Distribution* (Distribución cuántica de claves): tecnología de ciberseguridad que utiliza los principios de la física cuántica para generar y distribuir claves de cifrado.

[11] Centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

[12] El *ransomware* como servicio (RaaS) es un modelo de negocio de ciberdelincuencia que permite a los desarrolladores de *ransomware* escribir y vender código dañino o *malware* a otros *hackers* para que inicien sus propios ataques de *ransomware* mediante el uso de su software.

[13] Técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima —red social, banco, institución pública, etc.— con el objetivo de robarle información privada o realizarle un cargo económico.

[14] Estafa de ingeniería social por teléfono donde los atacantes se hacen pasar por entidades de confianza (bancos, agencias tributarias, soporte técnico) para engañar a la víctima y robar información confidencial (contraseñas, datos bancarios) o conseguir que realice acciones perjudiciales.

[15] Red de dispositivos infectados con *malware* (ordenadores, domótica, móviles) controlados remotamente por un ciberdelincuente para realizar ataques coordinados a gran escala, como ataques DDoS, envío masivo de

cve: BOCG-15-CG-A-223

spam, robo de datos o minería ilegal de criptomonedas, sin que los propietarios se den cuenta, usando un servidor centralizado para dar órdenes.

[16] *Distributed Denial of Service*: ciberataque malicioso que inunda un servidor, sitio web o red con un volumen masivo de tráfico de internet desde múltiples fuentes (una red de dispositivos comprometidos, o *botnet*) para sobrecargarlo y hacer que deje de funcionar, impidiendo el acceso a usuarios legítimos.

[17] Duplicación fraudulenta de la tarjeta SIM de un teléfono móvil que permite al atacante acceder al servicio telefónico de la víctima. De ese modo, puede llevar a cabo todo tipo de acciones que requieran una autenticación de múltiples factores.

[18] Proceso de migración de recursos, aplicaciones y datos de sistemas locales a la computación en la nube (Cloud Computing), un modelo que ofrece servicios de TI bajo demanda a través de Internet, como almacenamiento, servidores y software, eliminando la necesidad de gestionar infraestructuras físicas propias y pagando solo por lo que se usa, lo que impulsa la flexibilidad, escalabilidad y modernización digital de las empresas.

[19] Concepto de arquitectura de red móvil que desagrega el hardware del software mediante el uso de interfaces abiertas e interoperables. Esto permite a los operadores combinar componentes (como antenas y unidades de procesamiento) de distintos proveedores en una misma estación base, rompiendo con el modelo tradicional de sistemas cerrados y propietarios de un único fabricante.

[20] La Directiva NIS2 (Network and Information Security Directive 2) es una legislación de la Unión Europea que actualiza y amplía la Directiva NIS original para elevar el nivel de ciberseguridad en toda la UE, cubriendo más sectores críticos como energía, transporte, salud e infraestructuras digitales, imponiendo requisitos más estrictos de gestión de riesgos, seguridad en la cadena de suministro y notificación de incidentes, y afectando principalmente a medianas y grandes empresas para asegurar la resiliencia de servicios esenciales ante ciberataques.

[21] Conjunto de recursos físicos y de software (servidores, almacenamiento, redes, virtualización) que un proveedor de servicios en la nube (como AWS, Azure, GCP) gestiona en sus centros de datos, ofreciéndolos a través de Internet bajo demanda, permitiendo a las empresas pagar por uso, escalar recursos fácilmente y acceder a servicios informáticos sin grandes inversiones iniciales en hardware local. Es la base del *cloud computing*, proporcionando flexibilidad, escalabilidad y rentabilidad para aplicaciones y datos.

[22] Iniciativa en España, coordinada por el Centro Criptológico Nacional (CCN-CERT), que conecta los centros de ciberseguridad públicos para compartir información de amenazas en tiempo real, permitiendo una respuesta coordinada y más efectiva contra los ciberataques, fortaleciendo la ciberseguridad nacional.

[23] Estrategia para seleccionar las herramientas o *software* líderes y más especializados para cada función específica dentro de una empresa, en lugar de optar por una solución única y generalista («todo en uno») de un solo proveedor, permitiendo mayor personalización, especialización y rendimiento en áreas clave como la gestión de relaciones con clientes (CRM), gestión de almacenes (SGA) o recursos humanos, aunque requiere integración entre sistemas.

cve: BOCG-15-CG-A-223

A la Mesa de la Comisión Mixta de Seguridad Nacional

El Grupo Parlamentario Plurinacional SUMAR, de acuerdo con lo establecido en el Reglamento de la Cámara, presenta las siguientes propuestas de modificación a la Ponencia de análisis de las amenazas en el ciberespacio, en la era de la Inteligencia Artificial y la Computación Cuántica, para la elaboración de un informe de riesgos y recomendaciones de mejora.

Palacio del Congreso de los Diputados, 11 de febrero de 2026.— **Txema Guijarro García**, Portavoz sustituto Grupo Parlamentario Plurinacional SUMAR.

PROPUESTA NÚM. 1

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

I. Introducción

1. Objeto del Informe

El presente informe tiene por objeto presentar y reflejar de manera sistemática las conclusiones de la Ponencia de Análisis de las Amenazas en el Ciberespacio, en la Era de la Inteligencia Artificial y de la Computación Cuántica, así como **formular recomendaciones de mejora en el ámbito de la seguridad nacional, la protección de las infraestructuras críticas, el funcionamiento de las instituciones públicas y la salvaguarda de la ciudadanía a partir de una nueva visión socializada y amplia de ciberseguridad.**

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 2

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

II. ANÁLISIS DE LA COYUNTURA ACTUAL: LA TRANSFORMACIÓN DEL ENTORNO DIGITAL

1. Contexto general: aceleración tecnológica, aumento del cibercrimen y riesgos para la seguridad nacional y la ciudadanía

[…]

La digitalización ha alcanzado todos los estratos: administraciones, servicios esenciales, infraestructuras críticas, pymes, ciudadanos y hogares conectados. Esta integración conlleva dos efectos simultáneos: el incremento, por un lado, de la eficiencia, conectividad, capacidad de procesamiento y generación de datos; pero al mismo tiempo se produce una exposición total a ataques en cualquier punto de la

cve: BOCG-15-CG-A-223

red. Esta realidad hace imprescindible **la coordinación público-privada y fortalecer y priorizar la cooperación pública-pública a escala estatal y paneuropea.**

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 3

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

III. DIAGNÓSTICO GENERAL-AMENAZAS

2. APT, Actores Estatales y hacktivismo: ciberconflicto y operaciones encubiertas

La inmensa mayoría de comparecientes alertaron de que las amenazas más sofisticadas proceden de grupos de ciberinteligencia vinculados a Estados. Se mencionan de forma reiterada las llamadas APT (Advanced Persistent Threat, o Amenazas persistentes avanzadas); en especial las de origen ruso, chino, iraní y norcoreano, cuyas actividades incluyen espionaje político, militar y económico, robo de propiedad intelectual, exploración persistente de vulnerabilidades en infraestructuras críticas y operaciones de desinformación coordinadas con intrusiones técnicas. Pero también de Estados Unidos que desde Echelon a nuestros días es una amenaza manifiesta para la UE y nuestro país.

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 4

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

5. Desinformación y propaganda: erosión social y riesgo democrático

La desinformación fue identificada como una amenaza estratégica de primer orden. Los comparecientes coincidieron en que las campañas de influencia digital se han convertido en un instrumento geopolítico y criminal de enorme impacto. Además, la IA generativa permite producir contenido falso a escala industrial: imágenes, vídeos, voces sintéticas y narrativas automatizadas capaces de manipular percepciones y decisiones.

Los principales protagonistas de esta modalidad delictiva recaen en actores estatales con objetivos geopolíticos. Concretamente, Rusia lleva a cabo campañas globales bien financiadas, según algunos comparecientes, con presupuestos que podrían alcanzar la escala de miles de millones de dólares. Sus operaciones incluyen manipulación algorítmica, amplificación de narrativas, ataques coordinados

cve: BOCG-15-CG-A-223

de DDoS16 y desinformación. Otros países mencionados fueron China o Irán. **Y de forma determinante Estados Unidos cuyas empresas y el NSA del Brexit a la nueva administración del Presidente Trump, se traduce en una clara hegemonía y control de la ciberseguridad como principal amenaza para nuestro país y la UE.**

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 5

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

IV. CONCLUSIONES PRINCIPALES.

En tercer lugar, **los comparecientes han destacado la prioridad estratégica de la soberanía tecnológica, entendida no solo como autonomía industrial, sino como capacidad de control, decisión y resiliencia sobre las tecnologías críticas que sustentan la seguridad digital. Buena parte de ellos alertó sobre la elevada dependencia de proveedores y tecnologías no europeas, especialmente en ámbitos clave como la ciberseguridad, las comunicaciones, la inteligencia artificial o la computación cuántica. Esta dependencia fue identificada como un factor de vulnerabilidad en un contexto de tensiones geopolíticas y de utilización del ciberespacio como instrumento de presión principalmente de Estados Unidos e Israel.** En este contexto, se insistió en la necesidad de impulsar una base tecnológica propia, fomentar la industria nacional y europea y alinear las decisiones de inversión, contratación pública y regulación con objetivos de seguridad y soberanía; así como de garantizar el control sobre datos, sistemas y cadenas de suministro, especialmente en sectores críticos y en la Administración Pública.

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 6

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

En cuarto lugar, las comparecencias coincidieron en señalar la urgencia de reforzar la protección del ciudadano como eje central de las políticas de ciberseguridad. Las estafas digitales, la manipulación emocional, la explotación sexual de menores, la suplantación de identidad y la desinformación fueron identificadas como amenazas con un impacto directo y cotidiano sobre las personas, que generan daños económicos, psicológicos y sociales significativos. En este sentido, se destacó la necesidad de mejorar la atención a las víctimas, reducir las barreras a la denuncia, reforzar la formación y la concienciación, y garantizar que el desarrollo tecnológico se acompaña de salvaguardas efectivas de los derechos

cve: BOCG-15-CG-A-223

fundamentales, **planificando políticas de ciberseguridad centradas en la ciudadanía y la tradición de libertades públicas de la UE.**

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 7

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

En sexto y último lugar, varias intervenciones apuntaron a la necesidad de un modelo de financiación estable o de **«financiación basal**» que permita sostener en el tiempo las capacidades de ciberseguridad, tanto en el sector público como en los ecosistemas de innovación, formación e investigación. Varios expertos coincidieron en que las inversiones puntuales o ligadas a programas temporales no son suficientes para afrontar amenazas permanentes y en constante evolución. Por eso, más allá de programas concretos o fondos extraordinarios, los comparecientes destacaron la conveniencia de asegurar recursos estables para la protección de infraestructuras críticas, la modernización tecnológica de la Administración, la formación de profesionales, la retención de talento y el apoyo a pymes, evitando que la ciberseguridad dependa exclusivamente de iniciativas coyunturales o reactivas. **Ello exigiría, como muchos de lso comparecientes reseñaron, políticas democráticas y sistemáticas de ciencia y y tecnología.**

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 8

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

V. RECOMENDACIONES

1. Recomendaciones TECNOLÓGICAS.

En todo caso, se pone de manifiesto que cualquier estrategia de transición hacia criptografía postcuántica debe partir necesariamente de un inventario completo de los sistemas, protocolos y algoritmos criptográficos en uso, tanto en la protección de datos en reposo como en las comunicaciones. Este ejercicio previo es considerado esencial para priorizar activos críticos, planificar la migración y evitar riesgos operativos durante el proceso. **Y debe garantizarse con un conocimiento previo mapeando en forma de cartografía y análisis institucional la estructura global que afecta a la ciberseguridad.**

cve: BOCG-15-CG-A-223

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 9

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

En esta línea, **se recomienda fomentar la creación y consolidación de empresas españolas de ciberseguridad, así como priorizar tecnologías desarrolladas en el ámbito europeo o nacional cuando sea posible, especialmente en sectores sensibles para la seguridad nacional impulsando empresas públicas o de capital mixto con participacion mayoritaria del Estado evitando el modelo dominante liderado por Palantir Technologies.** Del mismo modo, la localización en territorio nacional de infraestructuras tecnológicas estratégicas, centros de análisis de amenazas y capacidades avanzadas de ciberseguridad contribuye de forma directa a la soberanía digital, a la retención de talento y al fortalecimiento del ecosistema nacional.

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 10

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

4. Recomendaciones ECONÓMICAS Y DE MERCADO.

En definitiva, SE RECOMIENDA:

— Reformar la contratación pública tecnológica, evitando que el precio sea el criterio principal y priorizando calidad, solvencia y resiliencia.

— Facilitar el acceso de pymes al mercado público de ciberseguridad mediante la división de contratos en lotes más pequeños.

— Ordenar el sector mediante sistemas de acreditación profesional y empresarial, elevando estándares y confianza.

— Articular incentivos económicos que permitan a las pymes adoptar medidas de ciberseguridad sin cargas desproporcionadas.

— Evitar la concentración tecnológica excesiva y diversificar proveedores en servicios críticos.

— Mejorar la retención de talento, revisando condiciones económicas y profesionales en el sector público y nacional.

— Orientar las políticas económicas hacia el desarrollo de capacidades reales y sostenibles, evitando dinámicas especulativas de corto plazo.

— Avanzar hacia la definición de listas o catálogos de proveedores tecnológicos seguros o de confianza para su utilización en sectores críticos y en el ámbito de las Administraciones Públicas, tomando como referencia experiencias previas como el

cve: BOCG-15-CG-A-223

despliegue de las redes 5G y aplicando criterios objetivos de evaluación del riesgo, fiabilidad del suministro y protección de la seguridad nacional.

— Impulsr La economía social de la ciberseguridad y el cooperativismo en el desarrollo tecnológico para las PYMES.

JUSTIFICACIÓN

Mejora del conjunto del informe.

PROPUESTA NÚM. 11

Grupo Parlamentario Plurinacional SUMAR

Propuesta de modificación:

5. Recomendaciones ESTRATÉGICAS.

En definitiva, SE RECOMIENDA:

— Tratar la ciberseguridad como una política de Estado, integrada en la seguridad nacional y no como un ámbito técnico sectorial.

— Adoptar una visión integral y transversal del ecosistema de ciberseguridad, superando compartimentos administrativos y organizativos.

— Priorizar la anticipación estratégica frente a la reacción, especialmente ante tecnologías emergentes.

Alinear la política nacional con los marcos europeos e internacionales de la UE, trascendiendo el marco de la Alianza Atlántica en el marco de la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la actualización de la política común de seguridad y defensa con miras a una visión de la ciberseguridad humana, integral y no dependiente. Cultura de Paz: Apuesta por mecanismos civiles de prevención de conflictos y el desarrollo de la Ley de Cultura de Paz.

— Cooperación Multilateral: Reforzar la cooperación con el «Sur Global» (especialmente Latinoamérica y Asia-Pacífico) y potenciar la OSCE a fin de ampliar la red de proveedores distintos a EEUU e Israel con países de los BRICS complementariamente a la estrategia prioritaria **del desarrollo industrial y la autonomía estratégica de España y la UE**.garantizando interoperabilidad y coherencia.

— Asegurar la continuidad temporal y estabilidad de las políticas de ciberseguridad, con planificación sostenida y recursos estables.

— Y promover la debida transparencia de toda inversión extranjera que afecte a la ciberseguridad a fin de evitar hubs de defensa, como en Aragón, que están diseñados al margen de los intereses estratégicos del país.

JUSTIFICACIÓN

Mejora del conjunto del informe.

A la Mesa de la Comisión Mixta de Seguridad Nacional

El Grupo Parlamentario VOX, de acuerdo con lo establecido en el Reglamento de la Cámara, presenta las siguientes propuestas de modificación a la Ponencia de análisis de

cve: BOCG-15-CG-A-223

las amenazas en el ciberespacio, en la era de la Inteligencia Artificial y la Computación Cuántica, para la elaboración de un informe de riesgos y recomendaciones de mejora.

Palacio del Congreso de los Diputados, 20 de febrero de 2026.—**José María Figaredo Álvarez-Sala**, Portavoz adjunto Grupo Parlamentario VOX.

PROPUESTA NÚM. 12

Grupo Parlamentario VOX

Propuesta de modificación:

Prohibir la adjudicación de contratos de servicios que afecten a la Seguridad Nacional a empresas que sean consideradas como «proveedores de alto riesgo», siguiendo la Comunicación de la Comisión Europea C(2023) 4049 y la propuesta de revisión de la Cybersecurity Act (CSA) presentada por la Comisión Europea el pasado 20 de enero.

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los

cve: BOCG-15-CG-A-223

diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

PROPUESTA NÚM. 13

Grupo Parlamentario VOX

Propuesta de modificación:

Aumentar los recursos, tanto materiales como de personal, de los organismos del Estado que tienen competencias en materia de ciberseguridad, en especial del Centro Criptológico Nacional.

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en

cve: BOCG-15-CG-A-223

general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

PROPUESTA NÚM. 14

Grupo Parlamentario VOX

Propuesta de modificación:

Impulsar todas las modificaciones legislativas necesarias para fortalecer el papel del Estado en ciberseguridad a través de la concentración de las competencias en dicha materia y siguiendo los principios básicos de unidad de acción y eficiencia.

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le

cve: BOCG-15-CG-A-223

sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

PROPUESTA NÚM. 15

Grupo Parlamentario VOX

Propuesta de modificación:

Definir una nueva Estrategia de Seguridad Nacional que integre Defensa, Interior e Inteligencia, con el objeto de prevenir y evitar eficazmente cualquier peligro, amenaza o agresión contra la independencia o la integridad territorial de España, los intereses nacionales, las infraestructuras críticas, ciberseguridad y soberanía de datos, soberanía industrial y energética, recursos naturales, así como la estabilidad del Estado de Derecho y sus instituciones.

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados

cve: BOCG-15-CG-A-223

a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

PROPUESTA NÚM. 16

Grupo Parlamentario VOX

Propuesta de modificación:

> Promover en el seno de la Unión Europea la adopción de medidas destinadas a reforzar la ciberseguridad de las redes e instituciones públicas de los Estados miembros frente a posibles ataques cibernéticos efectuados por parte de potencias o actores extranjeros.

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el

cve: BOCG-15-CG-A-223

suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

PROPUESTA NÚM. 17

Grupo Parlamentario VOX

Propuesta de modificación:

Desarrollar un «Programa de Atribución» que permita facilitar la identificación de la autoría de actos y/o actuaciones en el ciberespacio tipificados como delitos.

cve: BOCG-15-CG-A-223

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

cve: BOCG-15-CG-A-223

PROPUESTA NÚM. 18

Grupo Parlamentario VOX

Propuesta de modificación:

Impulsar la creación de empresas privadas nacionales especializadas en el ámbito de la ciberseguridad.

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen

cve: BOCG-15-CG-A-223

sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

PROPUESTA NÚM. 19

Grupo Parlamentario VOX

Propuesta de modificación:

Promover la cooperación público-privada en la lucha contra la ciberdelincuencia.

JUSTIFICACIÓN

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional («Ley de Seguridad Nacional o LSN») considera ámbitos de especial interés para la Seguridad Nacional «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales» (Art. 10). Así, la LSN elabora un listado de ámbitos entre los que destaca, en primer lugar, la ciberseguridad.

La ya citada LSN al nació con el propósito de coordinar las respuestas de las Administraciones Públicas ante las nuevas amenazas y riesgos a las que se enfrenta nuestro país. Como señala la Exposición de Motivos de la referida Ley, concretamente su párrafo séptimo, «la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral».

Así, estas respuestas del Estado deben observar una serie de principios básicos, tales como la Unidad de acción y eficiencia. En este mismo sentido, cabe mencionar que la plétora de organismos de ámbito autonómico en este sector, tales como la Agencia de Ciberseguridad de Cataluña, o la Agencia Vasca de Ciberseguridad, no hace sino debilitar el principio de unidad de acción, indispensable para que nuestro sistema de ciberdefensa sea eficaz y eficiente. De hecho, la proliferación de estos organismos genera una duplicidad de funciones que sufre el contribuyente. Asimismo, también dificulta la necesaria coordinación que debe ejercer el Gobierno, que ya resulta compleja de por sí, si le sumamos —como mínimo— otros organismos regionales. Más si cabe, cuando en la actuación de determinados gobiernos regionales se aprecia no ya la ausencia de la necesaria lealtad hacia el conjunto de las instituciones nacionales, sino un explícito propósito de acabar con la misma existencia de España.

Así pues, ante el riesgo que supone para España la posibilidad de que alguna potencia o actor internacional pueda poner en riesgo la ciberseguridad de nuestras redes y, en general, el correcto funcionamiento de nuestras instituciones a través de ataques cibernéticos, el Gobierno español tiene la obligación de mejorar sus protocolos de ciberseguridad al objeto de evitar futuros ataques de estas características. A mayor abundamiento, y ante el crecimiento importante de los ataques cibernéticos que ha sufrido España durante los últimos años. se torna fundamental potenciar la unidad de acción en el Sistema Nacional de Seguridad Nacional, así como reforzar la coordinación entre los diversos organismos que tienen competencia en la materia. Sin embargo, esta necesaria actualización de nuestros sistemas de ciberdefensa requiere una mayor financiación y compromiso por parte del Estado. Por último, también urge que el Gobierno tome las medidas necesarias para evitar que aquellos contratos que afectan a la Seguridad Nacional no se han adjudicados a empresas que puedan suponer un riesgo para la soberanía nacional y la independencia de los españoles. Resulta perentorio que, en un ámbito de

cve: BOCG-15-CG-A-223

especial interés de la Seguridad Nacional, como es la ciberseguridad, se tomen en cuenta las advertencias de nuestros países socios y aliados.

Finalmente, conviene recalcar que la ciberseguridad es una cuestión de Estado, que requiere de unidad de acción, concienciación de la sociedad en su conjunto e inversión suficiente para poder prevenir y anticipar las posibles amenazas y riesgos que se ciernen sobre nuestro país. Así, la proactividad y la anticipación se torna esencial al contar el agresor con el beneficio del factor sorpresa en modo, lugar y tiempo.

A la Mesa de la Comisión Mixta de Seguridad Nacional

El Grupo Parlamentario Socialista, de acuerdo con lo establecido en el Reglamento de la Cámara, presenta las siguientes propuestas de modificación a la Ponencia de análisis de las amenazas en el ciberespacio, en la era de la Inteligencia Artificial y la Computación Cuántica, para la elaboración de un informe de riesgos y recomendaciones de mejora.

Palacio del Congreso de los Diputados, 20 de febrero de 2026.—**Montse Mínguez García**, Portavoz adjunto Grupo Parlamentario Socialista.

PROPUESTA NÚM. 20

Grupo Parlamentario Socialista

La propuesta de modificación n.º 20 del Grupo Parlamentario Socialista fue retirada por escrito del Grupo con fecha de 20 de febrero de 2026.

PROPUESTA NÚM. 21

Grupo Parlamentario Socialista

Propuesta de modificación:

> El elemento central que vertebra este diagnóstico es la aceleración tecnológica. Tal y como señalaron los diferentes comparecientes, la velocidad de evolución de la tecnología ha comprimido los ciclos de cambio: procesos que antes requerían años ahora se transforman en cuestión de meses. La inteligencia artificial (IA) generativa, las nuevas ~~arquitecturas de red~~ **tecnologías de telecomunicacione**s, la computación cuántica, la expansión de dispositivos conectados y la automatización masiva han creado un entorno dinámico donde la capacidad ofensiva crece más rápido que la defensiva, exponiendo a la sociedad a riesgos sin precedentes. (Pág. 8)

JUSTIFICACIÓN

Mejora técnica.

cve: BOCG-15-CG-A-223

PROPUESTA NÚM. 22

Grupo Parlamentario Socialista

Propuesta de modificación:

Del mismo modo, operadores privados y empresas proveedoras de software y hardware confirmaron la magnitud del fenómeno: compañías como MasOrange o Telefónica registran diariamente ~~millones~~ **miles** de intentos de intrusión, y empresas internacionales como Cisco, Palo Alto Networks o Check Point detectan cientos de miles de millones de eventos globales al día. La infraestructura crítica española ha sido objeto de campañas de hacktivismo prorruso, ataques a cadenas de suministro, explotación de vulnerabilidades en servicios esenciales y actividad de ataques APT ligados a Rusia, China, Irán y Corea del Norte. En este último caso, la infiltración laboral mediante identidades sintéticas ha sido señalada como una amenaza emergente y especialmente peligrosa, pues combina ingeniería social, acceso interno y exfiltración silenciosa. (Pág. 9)

JUSTIFICACIÓN

Mejora técnica.

PROPUESTA NÚM. 23

Grupo Parlamentario Socialista

Propuesta de modificación:

Además, organismos públicos han identificado más de cuatro millones de dispositivos vulnerables en el territorio nacional, y expertos del sector privado subrayaron la elevada exposición de España en el contexto internacional,~~ señalando que nuestro país se sitúa entre los diez Estados que más ciberataques reciben a nivel mundial, ocupando concretamente la octava posición~~. (No existen cifras oficiales homologables sobre estos datos) (Pág.9)

JUSTIFICACIÓN

Mejora técnica.

PROPUESTA NÚM. 24

Grupo Parlamentario Socialista

Propuesta de modificación:

En este contexto, algunos comparecientes aportaron datos que permiten dimensionar con precisión la magnitud del fenómeno en España. En 2023, el INCIBE-CERT gestionó un total de 266.594 incidentes de ciberseguridad, lo que supuso un incremento del 24 % respecto al año anterior. **Sin embargo, resulta importante resaltar que se están mezclando 2 conceptos: cibercrimen y ciberincidentes. Respecto al primero las estadísticas oficiales son las del Mº del Interior y la Fiscalía en su informe Anual. Respecto al segundo estos ciberincidentes engloban hechos que pueden ser considerados como cibercrimen, pero también otros incidentes que no lo son (por ejemplo, fallos**

cve: BOCG-15-CG-A-223

software, fallos humanos, hechos no delictivos,...). La gran mayoría de estos incidentes afectaron a ciudadanía y empresas, si bien también se registraron incidencias relevantes en la red académica y, de forma específica, en operadores críticos y esenciales. (Pág. 15)

JUSTIFICACIÓN

Mejora técnica.

PROPUESTA NÚM. 25

Grupo Parlamentario Socialista

Propuesta de modificación:

Los *hacktivistas* operan **normalmente**, mediante técnicas simples pero masivas, aprovechando herramientas automatizadas accesibles y voluntarios distribuidos globalmente. Este fenómeno se intensifica en momentos de tensión internacional, procesos electorales o aprobación de leyes sensibles. En este sentido, determinadas campañas de hacktivismo, si bien presentan un impacto técnico limitado, buscan deliberadamente un elevado impacto mediático y reputacional. Este tipo de ataques, frecuentemente materializados mediante acciones de denegación de servicio, adquieren especial relevancia en contextos de tensión geopolítica, al amplificar narrativas y generar efectos desestabilizadores desproporcionados respecto a su complejidad técnica. (Pág. 17)

JUSTIFICACIÓN

Mejora técnica.

PROPUESTA NÚM. 26

Grupo Parlamentario Socialista

Propuesta de modificación:

Por otro lado, el sector de telecomunicaciones fue descrito por los operadores como el «sistema nervioso» del conjunto del país. Empresas como MasOrange o Telefónica reportaron que reciben diariamente ~~millones~~ **miles** de intentos de intrusión, afectando a redes móviles, fibra, infraestructura *cloud* y servicios gestionados. Cisco señaló que, a escala global, detecta más de 800.000 millones de amenazas al día, lo que da una medida del entorno en el que operan las telecomunicaciones españolas. Debido a que este sector da servicio a todos los demás —energía, finanzas, transporte y Administración—, cualquier ataque que comprometa un nodo relevante puede tener un efecto multiplicador sobre la economía y la seguridad nacional. Además, las campañas de desinformación se apoyan en estas plataformas, dificultando aún más su operación. (Pág. 22)

JUSTIFICACIÓN

Mejora técnica.

cve: BOCG-15-CG-A-223

PROPUESTA NÚM. 27

Grupo Parlamentario Socialista

Propuesta de modificación:

En primer lugar, existe un consenso amplio sobre la urgencia de acelerar la transición hacia la criptografía poscuántica. Diversos comparecientes han subrayado que, aunque todavía no ~~existía~~ **se conozca la existencia de** un ordenador cuántico criptográficamente relevante, la amenaza es ya presente debido a la práctica de capturar información hoy para descifrarla en el futuro, lo que obliga a proteger desde ahora los datos cuya vida útil se extiende durante años. En este sentido, se recomienda iniciar de forma inmediata procesos de identificación de los sistemas y servicios que utilizan criptografía asimétrica, priorizando aquellos que protegen información sensible o infraestructuras críticas, y planificar una transición ordenada hacia algoritmos resistentes a la computación cuántica, siguiendo los estándares internacionales ya publicados por el NIST y las recomendaciones del Centro Criptológico Nacional. Algunos comparecientes insisten, además, en que esta transición debe ser gradual e híbrida, permitiendo la convivencia temporal de algoritmos clásicos y poscuánticos para no comprometer la continuidad de los servicios esenciales. (Pág. 35)

JUSTIFICACIÓN

Mejora técnica.

PROPUESTA NÚM. 28

Grupo Parlamentario Socialista

Propuesta de modificación:

En definitiva, **SE RECOMIENDA**:

— **Reforzar el liderazgo estratégico del Estado, evitando la dispersión institucional y clarificando responsabilidades** en prevención, respuesta, supervisión y cooperación internacional.

— **Impulsar la trasposición de la Directiva NIS al ordenamiento jurídico español, para acelerar la creación del Centro Nacional de Ciberseguridad.** (pág. 41)

JUSTIFICACIÓN

Mejora técnica.

cve: BOCG-15-CG-A-223