III. OTRAS DISPOSICIONES

MINISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES CON LAS CORTES

9088 *Orden PJC/448/2025, de 6 de mayo, por la que se publica el Acuerdo del Consejo de Ministros de 6 de mayo de 2025, por el que se aprueban actuaciones para complementar las recogidas en el Plan Nacional de Ciberseguridad.*

El Consejo de Ministros, en su reunión de 6 de mayo de 2025, a propuesta de los Ministros para la Transformación Digital y de la Función Pública, de la Presidencia, Justicia y Relaciones con las Cortes, de Defensa y del Interior, ha aprobado un acuerdo por el que se aprueban actuaciones para complementar las recogidas en el Plan Nacional de Ciberseguridad.

Para general conocimiento, se dispone su publicación como anejo a la presente orden.

Madrid, 6 de mayo de 2025.–El Ministro de la Presidencia, Justicia y Relaciones con las Cortes, Félix Bolaños García.

ANEJO

Acuerdo por el que se aprueban actuaciones para complementar las recogidas en el Plan Nacional de Ciberseguridad

En la actualidad, la ciberseguridad se ha convertido en una prioridad esencial para los Gobiernos de todos los países por cuanto es herramienta clave para garantizar la soberanía de los Estados y la defensa de los valores democráticos, los derechos de la ciudadanía y la estabilidad y progreso de la economía.

Si bien los avances tecnológicos han traído aparejadas numerosas ventajas en todos los ámbitos, también han incrementado los riesgos y amenazas cibernéticas. Desde ataques para el secuestro digital de datos y petición de un posterior rescate (ransomware) hasta el espionaje cibernético, la necesidad de proteger las infraestructuras digitales del ámbito público y privado y los datos personales nunca ha sido tan urgente. Por ello, diversas organizaciones internacionales trabajan conjuntamente para desarrollar marcos de cooperación y compartir información crucial para impedir y mitigar estos ataques.

En España, la ciberseguridad ha tomado un papel preponderante en el desarrollo de políticas nacionales. Con el creciente número de ataques cibernéticos y la expansión de las infraestructuras digitales, el Gobierno ha adoptado diversas estrategias en los planos normativo y tecnológico para proteger sus sistemas y datos.

Así, la Estrategia Nacional de Ciberseguridad de 2019, aprobada por el Consejo de Seguridad Nacional el 12 de abril de 2019, formuló un objetivo general y cinco objetivos específicos, proponiendo para alcanzarlos, siete líneas de acción concretadas en 65 medidas que se desarrollan mediante el Plan Nacional de Ciberseguridad aprobado el 29 de marzo de 2022, todo ello en el marco político estratégico de referencia de la Política de Seguridad Nacional según la Estrategia de Seguridad Nacional 2021, aprobada por medio del Real Decreto 1150/2021, de 28 de diciembre.

El Plan Nacional de Ciberseguridad concretó un conjunto de actuaciones para avanzar del modo más eficiente y eficaz posible en el desarrollo de la ciberseguridad nacional. Sin embargo, desde la aprobación de dicho Plan se han producido notables y acelerados cambios en el escenario de la ciberseguridad, en primer lugar, por razón del

cve: BOE-A-2025-9088
Verificable en https://www.boe.es

intenso avance de la digitalización que desdibuja las fronteras entre lo digital y lo físico, entre lo civil y lo militar, a la vez que amplía la superficie de ataque aprovechable mediante acciones realizadas o auspiciadas por Gobiernos de potencias extranjeras así como por individuos que actuando por propia iniciativa o contratados por terceros dirigen su actuación maliciosa contra administraciones y toda suerte de entidades, empresas, individuos y dispositivos.

En segundo lugar, la evolución del contexto geopolítico, que demanda una mayor atención en materia de seguridad y defensa incluida la del ciberespacio, también ha coadyuvado a esos acelerados cambios, evidenciándose el incremento del nivel técnico de los ciberataques patrocinados por Gobiernos, así como del número de ellos llevados a cabo por ciberdelincuentes, unos y otros dirigidos a la disrupción de los servicios, a la sustracción, alteración o destrucción de datos e información, a la cadena de suministro y, particularmente, contra infraestructuras críticas civiles y militares de todo tipo.

Finalmente, la extensión de la utilización de la inteligencia artificial permite a los ciberatacantes sofisticar los ataques de manera más elaborada y personalizada; a la vez que el desarrollo de la computación cuántica y su potencial uso malintencionado plantea una seria amenaza, por lo que será ineludible abordar la transición a la criptografía postcuántica.

En este período, además, se han aprobado diferentes normas (con rango de ley y reglamentarias) en el marco configurado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que concibe el ciberespacio como un ámbito de especial interés de la misma, requiriendo, por tanto, y tal y como indica la referida norma, una atención específica por resultar un elemento básico para preservar los derechos y libertades y el bienestar de los ciudadanos así como para garantizar el suministro de los servicios y recursos esenciales. Así, se han aprobado el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y el Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G.

En la Unión Europea, destacan singularmente, la aprobación de la Directiva NIS 2 [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); del Reglamento de Ciberresiliencia (Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828]; y del Reglamento de Cibersolidaridad [Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694]. También, en el marco de la Estrategia Europea de Ciberseguridad de 2020, se adoptó en 2022 la Política de Ciberdefensa de la Unión Europea que incide en el impulso de las capacidades de ciberdefensa, la consolidación del ciberespacio como dominio de las operaciones militares, y la cooperación entre los Estados miembros de la Unión Europea.

En definitiva, por las razones anteriormente expuestas, es necesario complementar de forma urgente y prioritaria las actuaciones recogidas en el Plan Nacional de Ciberseguridad de acuerdo con el actual contexto estratégico, las obligaciones del marco regulador surgido tras la aprobación del Plan en 2022, las tendencias en materia de ciberseguridad y ciberdefensa, la necesidad de proteger la información, los servicios, y especialmente las infraestructuras críticas de todo tipo, así como las oportunidades y riesgos derivados de la extensión de tecnologías emergentes y disruptivas, tales como la inteligencia artificial, el cifrado y la computación cuántica. Todo ello para mejorar las

cve: BOE-A-2025-9088
Verificable en https://www.boe.es

capacidades de ciberseguridad y ciberdefensa de amplio espectro, abarcando conciencia situacional, prevención, detección, defensa, protección, respuesta, recuperación, y disuasión, todo ello con perspectiva articulada, de conjunto y de esfuerzo sostenido en el tiempo.

Estas medidas conforman un conjunto de actuaciones para avanzar del modo más eficiente y eficaz posible en el desarrollo de la ciberseguridad nacional, y tienen una interrelación clara con el Plan de Recuperación, Transformación y Resiliencia, y en especial en su Componente 11 (Inversión 1. Modernización de la Administración General del Estado).

En su virtud, a propuesta de los Ministros para la Transformación Digital y de la Función Pública, de la Presidencia, Justicia y Relaciones con las Cortes, de Defensa y del Interior, el Consejo de Ministros, en su reunión del día de mayo de 2025, acuerda:

Primero. *Actuaciones en materia de ciberseguridad complementarias a las recogidas en el Plan Nacional de Ciberseguridad.*

Se aprueban un conjunto de actuaciones en materia de ciberseguridad como complemento de las recogidas en el Plan Nacional de Ciberseguridad, aprobado por Acuerdo del Consejo de Ministros de 29 de marzo de 2022.

Dichas actuaciones al estar incluidas o relacionadas con el Plan de Recuperación, Transformación y Resiliencia, y en especial en su Componente 11 (Inversión 1. Modernización de la Administración General del Estado), se sujetarán a lo establecido en el Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia.

Segundo. *Presupuesto.*

La asignación presupuestaria necesaria para el cumplimiento de lo previsto en este acuerdo se consignará en el presupuesto del Ministerio de Defensa, Ministerio del Interior, Ministerio para la Transformación Digital y de la Función Pública y del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, con el desglose previsto en el anexo I.

Tercero. *Seguimiento de las actuaciones.*

De acuerdo con lo previsto en el artículo 7 del Real Decreto 210/2024, de 27 de febrero, por el que se establece la estructura orgánica básica del Ministerio para la Transformación Digital y de la Función Pública, corresponde a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales la dirección estratégica de las medidas de este acuerdo y el seguimiento de su cumplimiento, que llevará a cabo en los términos previstos en el anexo II a través de la Agencia Estatal de Administración Digital, que intervendrá de acuerdo con lo previsto en los artículos 5 y 18 de su Estatuto, aprobado por el Real Decreto 1118/2024, de 5 de noviembre.

Cuarto. *Plazo de ejecución.*

Dada su naturaleza crítica, las actuaciones se realizarán con la mayor celeridad posible.

Quinto. *Entrada en vigor.*

Este acuerdo surtirá efectos desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

cve: BOE-A-2025-9088
Verificable en https://www.boe.es

ANEXO I

Presupuesto por órgano u organismo público

Órgano u organismo público	Escenario inversión total-Por entidad – Euros	% del total
Agencia Estatal de Administración Digital.	178.065.472	15,39
Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID).	33.082.573	2,86
Red.es.	43.873.006	3,79
Departamento de Seguridad Nacional (presupuesto gestionado por el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes).	13.929.504	1,20
Centro Nacional de Inteligencia-Centro Criptológico Nacional.	381.049.445	32,93
Ministerio de Defensa.	318.000.000	27,48
Ministerio del Interior.	189.000.000	16,34
Total.	1.157.000.000	100,00

En concreto, por departamentos ministeriales:

a) Ministerio para la Transformación Digital y de la Función Pública (SETID, AEAD y Red.es) (255.021.051 €).
b) Ministerio de Defensa (CNI-CCN, MCCS y el propio Ministerio) (699.049.445 €).
c) Ministerio del Interior (189.000.000 €).
d) Ministerio de la Presidencia, Justicia y Relaciones con las Cortes (Departamento de Seguridad Nacional) (13.929.504 €).

ANEXO II

Modelo de seguimiento de las medidas del Acuerdo

En la ejecución de las actuaciones previstas en este acuerdo intervienen un conjunto de órganos y organismos y entidades del sector público que se encargarán de velar por la puesta en marcha de los diferentes proyectos; dichos órganos, organismos y entidades, cuando así convenga para la mejor ejecución de las actuaciones previstas, podrán emplear fórmulas de colaboración con las entidades integrantes del sector público empresarial. En concreto:

a) Ministerio para la Transformación Digital y de la Función Pública.

– Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID).
– Agencia Estatal de Administración Digital (AEAD).
– Red.es.
– Instituto Nacional de Ciberseguridad (INCIBE).

b) Ministerio de Defensa.

– Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC).
– Mando Conjunto del Ciberespacio (MCCE).
– Centro Nacional de Inteligencia-Centro Criptológico Nacional (CNI-CCN).

c) Ministerio del Interior (MIR).
d) Presidencia del Gobierno.

– Departamento de Seguridad Nacional (DSN).

cve: BOE-A-2025-9088
Verificable en https://www.boe.es

Por todo ello, y en aras de lograr una correcta gestión de los proyectos en tiempo y forma, se establece un modelo de seguimiento que se articula en dos niveles:

1.º) El seguimiento propio en cada órgano u organismo público responsable de la ejecución de la actuación, con la participación de los distintos actores implicados.

2.º) La coordinación y seguimiento estratégico de la totalidad del acuerdo que llevará a cabo la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales a través de la Agencia Estatal de Administración Digital (en adelante, AEAD).

Mecanismo de seguimiento.

– El seguimiento de los proyectos abarca los mecanismos de comunicación y coordinación involucrados en la actualización de reportes, interacción con los ministerios y elaboración de informes.

– La AEAD mantendrá reuniones bilaterales de seguimiento con carácter semanal con los órganos y organismos responsables de la ejecución de las actuaciones.

– La tercera semana de cada mes, los órganos y organismos responsables de la ejecución remitirán electrónicamente a la AEAD, en el formato que esta determine, la información sobre cada actuación relativa a:

- Avance en ejecución presupuestaria y mecanismos de contratación.
- Avance operativo.
- Avance y cumplimiento de objetivos.
- Elementos adicionales de coordinación, evaluación de impacto y riesgos.

Dicha información se integrará en un repositorio creado al efecto por la AEAD, a partir del cual se generarán los informes de seguimiento y se elaborará un cuadro de mando.

– La AEAD informará a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales del seguimiento de las actuaciones de este acuerdo, con la periodicidad que determine.

cve: BOE-A-2025-9088
Verificable en https://www.boe.es