III. OTRAS DISPOSICIONES

MINISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES CON LAS CORTES

10371 *Orden PJC/522/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad.*

El Consejo de Seguridad Nacional, en su reunión de 24 de abril de 2025, ha aprobado un acuerdo por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad.

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

Madrid, 23 de mayo de 2025.–El Ministro de la Presidencia, Justicia y Relaciones con las Cortes, Félix Bolaños García.

ANEJO

Acuerdo por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad

EXPOSICIÓN

La Estrategia de Seguridad Nacional de 2021 (ESN21) ratifica la vulnerabilidad del ciberespacio como uno de los principales riesgos para la seguridad del país.

Hasta la fecha se han elaborado de forma concatenada dos Estrategias de segundo nivel en materia de ciberseguridad nacional, la primera en el año 2013 y la segunda, actualmente vigente, en 2019 (ENCS19). Los objetivos y líneas de acción de esta última han servido de guía para avanzar en la consecución de un ciberespacio común, global y confiable a nivel nacional y por ende a nivel europeo e internacional.

Esta positiva evolución sin embargo se ha visto acompañada en los últimos años de una expansión sin precedentes del panorama de amenazas. Por un lado, los ciberincidentes han crecido en frecuencia, sofisticación y persistencia, en especial aquellos llevados a cabo por actores hostiles estatales y no estatales, así como los dirigidos contra activos críticos del país: Administraciones públicas, infraestructuras críticas y operadores de servicios esenciales. De modo similar, la ciberdelincuencia, que es un factor clave para la ciberseguridad, en muchas ocasiones íntimamente ligado a la amenaza de actores hostiles, ha mantenido un notable incremento a pesar de los esfuerzos ya contemplados en la ENCS19. Por otro lado, existen nuevos desafíos tecnológicos que afrontar como son: el exponencial desarrollo de la inteligencia artificial que, en sus distintas funcionalidades, puede considerarse como amenaza o fortaleza en lo que respecta a la ciberseguridad, o los avances en la computación cuántica, susceptibles de poner en riesgo los actuales algoritmos de cifrado.

La nueva Estrategia Nacional de Ciberseguridad (ENCS) debe alinearse con las pautas establecidas por la UE, tanto en la Estrategia europea de ciberseguridad 2020, como con las distintas políticas y recomendaciones emitidas en ámbitos específicos como, por ejemplo: la Política de Ciberdefensa de la UE de 2022, el 5G, la certificación, la protección de cables submarinos o el «Pacto cuántico».

Así mismo, conviene referir el marco legal de referencia que supone 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

cve: BOE-A-2025-10371
Verificable en https://www.boe.es

la Unión, conocida como Directiva NIS2, cuyo articulado concreta buena parte de los elementos que la Estrategia Nacional de Ciberseguridad de los Estados miembros debe contener, incluyendo: políticas concretas para luchar contra el auge de los ciberataques de tipo ramsonware, para el fomento de la ciberprotección activa o aquellas dirigidas a la protección específica de los servicios públicos básicos digitalizados.

La Directiva NIS2 se encuentra en proceso de transposición al ordenamiento jurídico nacional a través del ante proyecto de ley en tramitación: de la coordinación y gobernanza en ciberseguridad. Este anteproyecto prevé la constitución de un Centro Nacional de Ciberseguridad para avanzar en la coordinación y gobernanza de la ciberseguridad nacional, entre cuyas funciones está previsto contribuya positivamente al impulso y desarrollo de la futura Estrategia.

La nueva Estrategia se alineará con el resto de la normativa general y en especial con aquella con implicaciones en ciberseguridad, tanto a nivel nacional, como la Ley de Ciberseguridad 5G y la que aprueba el Esquema Nacional de seguridad de las redes y servicios 5G, como europeo, concretamente con la Ley de Ciberresiliencia y la Ley de Cibersolidaridad.

En este sentido, aunque la legislación europea no aborda materias relativas a Defensa Nacional, por ser competencia de los Estados, la UE no renuncia a una estrategia común en este ámbito. En consecuencia, la Estrategia Europea de Ciberseguridad de 2020 incluye medidas orientadas al impulso de las capacidades de Ciberdefensa militar, entre ellas la consolidación del ciberespacio como dominio de las operaciones militares y el avance en mecanismos europeos de cooperación militar y defensa colectiva en el Ciberespacio. Medidas estas que se alinean con la necesidad, expresada en la Estrategia de Seguridad Nacional de 2021, de responder a los riesgos derivados de la consolidación del ciberespacio como dominio estratégico y como espacio de competición entre Estados, que obliga a incorporar nuevas tecnologías y formas de confrontación, para asegurar una capacidad de enfrentamiento actualizada y moderna. La necesidad de impulsar dichas líneas de colaboración se mantiene en la Política de Ciberdefensa de la Unión Europea de 2022, ante la posibilidad de que se den crisis de ciberseguridad con una importante dimensión exterior o de política común de seguridad y defensa.

Asimismo, la Estrategia impulsará las actividades de investigación y desarrollo encaminadas a facilitar el uso de tecnologías innovadoras, cumpliendo con el Derecho de la Unión en materia de protección de datos.

Finalmente, será también coherente con las líneas de trabajo, recomendaciones y conclusiones de otros organismos europeos e internacionales como son: La Agencia Europea de ciberseguridad ENISA, el Centro Europeo de Competencia en Ciberseguridad, la OSCE o la Unión Internacional de Telecomunicaciones (UIT).

ACUERDO

Único.

Se aprueba la elaboración de una nueva Estrategia Nacional de Ciberseguridad conforme al procedimiento que figura como anexo a este acuerdo.

ANEXO

Procedimiento para la elaboración de la nueva Estrategia Nacional de Ciberseguridad

1) Responsable de su elaboración:

El Consejo de Seguridad Nacional será responsable de la elaboración de la Estrategia Nacional de Ciberseguridad a través de su Comité especializado, el Consejo Nacional de Ciberseguridad.

cve: BOE-A-2025-10371
Verificable en https://www.boe.es

2) Mecanismo de elaboración:

Bajo la dependencia del Consejo de Seguridad Nacional, el Consejo Nacional de Ciberseguridad acordará la constitución de un Grupo de trabajo técnico para la elaboración de la Estrategia Nacional de Ciberseguridad.

1. Podrán formar parte del Grupo de trabajo técnico representantes de todos los departamentos ministeriales u organismos de la Administración, previa propuesta y aprobación del Consejo Nacional de Ciberseguridad.
2. Las Comunidades y las Ciudades Autónomas participarán en el proceso a través de la Conferencia Sectorial para Asuntos de la Seguridad Nacional.
3. Se podrán recabar aportaciones de aquellos expertos procedentes de la sociedad civil, el sector privado y el académico que, por su conocimiento y formación científico-técnica en la materia, contribuyan a la mejora de los contenidos de la Estrategia.

3) Mandato:

Elaborar un borrador de Estrategia Nacional de Ciberseguridad con arreglo a las fases y las directrices que a continuación se determinan.

4) Fases del proceso de elaboración:

1. El Grupo de trabajo técnico será el encargado de elaborar los distintos borradores de la Estrategia.
2. El Departamento de Seguridad Nacional, una vez elaborado un borrador, podrá recabar las aportaciones de expertos independientes procedentes de la sociedad civil, el sector privado y el académico.
3. El borrador final de la Estrategia será enviado a la Conferencia Sectorial para Asuntos de la Seguridad Nacional para conocimiento y posibles propuestas de las Comunidades y Ciudades Autónomas.
4. Una vez elaborado el borrador final, El Grupo de trabajo técnico presentará al Consejo Nacional de Ciberseguridad el borrador definitivo de la Estrategia Nacional de Ciberseguridad.
5. Una vez acordado el texto definitivo por el Consejo Nacional de Ciberseguridad, a través de la persona que ejerza su Presidencia, se elevará como propuesta de Estrategia Nacional de Ciberseguridad al Consejo de Seguridad Nacional, para su aprobación.

5) Directrices de elaboración:

1. Incluir un análisis del contexto actual en cuanto a las amenazas para la ciberseguridad nacional, tal y como se contempla en las Estrategias e informes anuales de Seguridad Nacional.
2. Presentar un enfoque amplio y transversal que se alinee con los intereses nacionales y europeos que se deben proteger, identificar los principales riesgos, y definir los objetivos estratégicos y los recursos necesarios para alcanzarlos, así como las líneas de acción necesarias para la reducción de los riesgos identificados.
3. Estar en consonancia con la normativa, Estrategias, Políticas, planes y recomendaciones existentes a nivel nacional y de la Unión Europea.
4. La elaboración de la Estrategia Nacional de Ciberseguridad deberá realizarse con el consenso más amplio posible.
5. En el proceso de elaboración se podrán tomar en consideración los trabajos realizados por la sociedad civil en el marco de iniciativas de cooperación público-privada como el Foro Nacional de Ciberseguridad, así como las investigaciones académicas existentes en los diferentes ámbitos de acción.
6. La Estrategia estará acompañada de una divulgación adecuada a la sociedad en su conjunto.

cve: BOE-A-2025-10371
Verificable en https://www.boe.es

6) Tramitación del acuerdo:

El contenido de esta acuerdo será tramitado por el Departamento de Seguridad Nacional en calidad de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional.

cve: BOE-A-2025-10371
Verificable en https://www.boe.es