Consejo de la Unión Europea

Bruselas, 3 de abril de 2025
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	2 de abril de 2025
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2025) 148 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES ProtectEU: una Estrategia Europea para la Seguridad Interior

Adjunto se remite a las delegaciones el documento COM(2025) 148 final.
Adj.: COM(2025) 148 final

COMISIÓN
EUROPEA

Estrasburgo, 1.4.2025
COM(2025) 148 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

ProtectEU: una Estrategia Europea para la Seguridad Interior

1. ProtectEU: una Estrategia Europea para la Seguridad Interior

La seguridad sienta los cimientos sobre los que se levantan todas nuestras libertades. La democracia, el Estado de Derecho, los derechos fundamentales, el bienestar de los europeos, la competitividad y la prosperidad: todo ello depende de nuestra capacidad para ofrecer unas garantías básicas de seguridad. En esta nueva era en la que vivimos ahora, caracterizada por las amenazas a la seguridad, la capacidad de los Estados miembros de la UE para garantizar la seguridad de sus ciudadanos depende, más que nunca, de la aplicación de un **enfoque unificado y europeo a la protección de nuestra seguridad interior**. Frente a un panorama geopolítico en constante evolución, Europa debe seguir cumpliendo su perdurable promesa de paz.

Ya se han dado los primeros pasos hacia la construcción de un aparato de seguridad europeo. A lo largo de la última década, hemos equipado a la Unión con mejores mecanismos colectivos de actuación en los ámbitos de la cooperación policial y judicial, la seguridad de las fronteras, la lucha contra la delincuencia grave y organizada y contra el terrorismo y el extremismo violentos, y la protección de las infraestructuras críticas, tanto físicas como digitales, de la UE. La cabal aplicación de la legislación adoptada y las políticas desarrolladas hasta ahora sigue siendo un factor esencial.

La naturaleza de las amenazas actuales y el vínculo intrínseco entre la seguridad interior y la seguridad exterior de la UE nos exigen ir más lejos.

El panorama que pintan las amenazas es sombrío. Los límites entre las **amenazas híbridas** y las hostilidades abiertas son difusos. Rusia ha estado librando una campaña híbrida tanto en entornos virtuales como reales contra la UE y sus socios con el fin de perturbar y socavar la cohesión social y los procesos democráticos y poner a prueba la solidaridad de la UE con Ucrania. Los Estados extranjeros hostiles y los agentes que ellos mismos patrocinan tratan de infiltrarse en nuestras infraestructuras críticas y nuestras cadenas de suministro para provocar disrupciones, robar datos sensibles y posicionarse de forma que puedan ocasionar, en el futuro, los mayores trastornos posibles. Utilizan la delincuencia como servicio y a los delincuentes como agentes vicarios. Por otra parte, nuestra dependencia respecto de terceros países en las cadenas de suministro nos hace más vulnerables a las campañas híbridas de Estados hostiles.

Están proliferando en Europa **redes de delincuencia organizada** que prosperan en el entorno virtual, se propagan desde allí a nuestra economía y afectan a nuestras sociedades, como pone de manifiesto el informe de Evaluación de la amenaza de la delincuencia grave y organizada de la Unión Europea (SOCTA) recientemente presentado por Europol[1]. Una vez que la delincuencia se asienta en alguna comunidad o en algún sector económico, su erradicación se convierte en una ardua batalla: una tercera parte de las redes delictivas más peligrosas están activas desde hace más de diez años. Las criptomonedas y los sistemas financieros paralelos las ayudan a blanquear y ocultar los beneficios de sus delitos.

La **amenaza terrorista sigue cerniéndose sobre Europa** Las crisis regionales que se producen fuera de la UE crean un «efecto dominó», insuflando a los agentes terroristas de todo el espectro ideológico una nueva motivación para captar adeptos, movilizar a sus agentes o ampliar sus capacidades. Estos agentes orientan específicamente su actividad de radicalización y captación hacia los sectores más vulnerables de nuestras sociedades y, en particular, hacia determinados jóvenes. Inspiran atentados por parte de agentes solitarios y generan oleadas de extremismo antisistema cuyo objetivo es perturbar el ordenamiento jurídico democrático.

Los rápidos **avances de la tecnología** nos ofrecen instrumentos esenciales con los que perfeccionar nuestro aparato de seguridad. No obstante, los ciberataques y la manipulación de

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

la información por parte de agentes extranjeros son cada vez más frecuentes y explotan nuevas tecnologías como la inteligencia artificial. Los niños, los jóvenes y las personas mayores corren un especial riesgo en el entorno virtual y la propagación del odio en línea es una amenaza para la libertad de expresión y la cohesión social.

Nuestras vidas se han vuelto menos seguras, fenómeno que cada vez sienten con mayor intensidad los europeos, cuya **percepción de la seguridad y la protección en la UE** se ha erosionado hasta el punto de que, al ser encuestados sobre el futuro, el 64 % de ellos manifiestan una tendencia a estar preocupados por la seguridad de la UE[2]. Las empresas también están cada vez más inquietas; la información errónea y la desinformación, la delincuencia y las actividades ilícitas y el ciberespionaje figuran entre los diez mayores riesgos destacados en el Informe de Riesgos Globales del Foro Económico Mundial de 2025[3].

Los europeos deben **poder vivir tranquilos y estar sin miedo**, ya sea en las calles, en sus hogares, en lugares públicos, en el metro o en internet. La protección de las personas, especialmente las más vulnerables a los ataques —que tienden a afectar desproporcionadamente a los niños, las mujeres y las minorías, incluidas las comunidades judía y musulmana— radica en el centro de la labor de la UE en materia de seguridad. Se trata de una empresa esencial para construir unas sociedades resilientes y cohesionadas.

La Comisión está elaborando una **Estrategia Europea para la Seguridad Interior** que permitirá repeler más eficazmente las amenazas en los próximos años. Mediante un conjunto de instrumentos jurídicos más precisos, una cooperación más estrecha y un intercambio de información más amplio, aumentaremos nuestra resiliencia y nuestra capacidad colectiva para anticipar, prevenir y detectar las amenazas para la seguridad y responder eficazmente a ellas. La aplicación de un enfoque unificado a la seguridad interior puede ayudar a los Estados miembros a encauzar provechosamente el poder de la tecnología para reforzar la seguridad —en lugar de debilitarla—, promoviendo al mismo tiempo la existencia de un espacio digital seguro para todos. Además, tal enfoque sustenta una respuesta común de los Estados miembros a las mutaciones políticas y económicas mundiales que afectan a la seguridad interior de la Unión.

La Estrategia se guía por **tres principios** y alberga en su núcleo el respeto del Estado de Derecho y los derechos fundamentales.

En primer lugar, fija como ambición un cambio de cultura en materia de seguridad. Necesitamos un **enfoque que implique a toda la sociedad** y en el que participen todos los ciudadanos y partes interesadas, incluida la sociedad civil, los centros de investigación, el entorno académico y las entidades privadas. Las acciones que se enmarcan en la Estrategia adoptan un enfoque integrado y multilateral siempre que es posible.

En segundo lugar, **las consideraciones de seguridad deben integrarse e incorporarse en toda la legislación, todas las políticas y todos los programas de la UE**, incluida la acción exterior de la UE. La legislación, las políticas y los programas deberán prepararse, revisarse y aplicarse teniendo siempre presente la dimensión de seguridad, asegurando que se atienden las consideraciones de seguridad necesarias para promover un enfoque coherente y global de esta.

Por último, una Europa segura, protegida y resiliente requiere una **considerable inversión por parte de la UE, sus Estados miembros y el sector privado**. Las prioridades y acciones establecidas en la presente Estrategia requieren unos recursos humanos y financieros suficientes para garantizar su ejecución. Según se expone en la Comunicación sobre la ruta hacia el

[2] Eurobarómetro Flash FL550: Retos y prioridades para la UE.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, p.17.

próximo marco financiero plurianual[4], Europa tendrá que aumentar el gasto público en seguridad y promover la investigación y la inversión en la materia, reforzando con ello su autonomía estratégica.

Esta Estrategia complementa la **Estrategia de Preparación de la Unión**[5], en la que se establece un enfoque integrado —que contempla todos los riesgos— de la preparación ante conflictos, catástrofes provocadas por el ser humano y catástrofes naturales y crisis, y el **Libro Blanco sobre el futuro de la defensa europea**[6], que propugna el desarrollo y la adquisición de capacidades de defensa en toda la UE para disuadir a los adversarios extranjeros. La Comisión propondrá también un **Escudo Europeo de la Democracia** para reforzar la resiliencia democrática en la UE. Juntas, estas iniciativas configuran la visión que corresponde a una UE segura, protegida y resiliente.

Una nueva gobernanza europea de la seguridad interior

La Comisión colaborará estrechamente con los Estados miembros y las agencias de la UE para perfeccionar el enfoque de la UE en materia de seguridad interior desde el punto de vista tanto estratégico como operativo.

Con tal fin:

- **se determinarán sistemáticamente las implicaciones de las iniciativas de la Comisión —tanto las de nuevo cuño como las revisiones— para la seguridad y la preparación, desde el inicio y a lo largo de todo el proceso de negociación;**
- **se convocarán reuniones periódicas del Grupo de Proyecto de la Comisión sobre Seguridad Interior Europea, sustentadas por una colaboración intersectorial estratégica en toda la Comisión**
- **se realizarán presentaciones de los análisis de amenazas relacionadas con la seguridad interior, en apoyo del trabajo de la Escuela de Seguridad**
- **se mantendrán debates con los Estados miembros, en el seno del Consejo, sobre la evolución de los retos en materia de seguridad interior, sobre la base del análisis de amenazas y los debates sobre las políticas prioritarias**
- **se presentarán informes periódicos al Parlamento Europeo y al Consejo para hacer un seguimiento de las iniciativas clave en materia de seguridad y apoyar su aplicación sistemática**

2. Conciencia situacional y análisis de las amenazas integrados

Dotaremos a la UE de nuevos métodos para poner en común y combinar la información y facilitaremos un análisis periódico de las amenazas para la seguridad interior de la UE, contribuyendo con esas medidas a una evaluación integral de los riesgos y amenazas.

La seguridad comienza con una **anticipación efectiva**. La UE debe apoyarse en una conciencia situacional y unos análisis de amenazas exhaustivos, actualizados y suficientemente autónomos. La inteligencia ejecutable, cuya mejora a través de la Capacidad Única de Análisis de Inteligencia (SIAC) como punto de acceso único para la inteligencia de los Estados miembros se recomienda encarecidamente a estos, es un factor vital para evaluar y neutralizar

[4] COM (2025) 46 final.
[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.

las amenazas y, en última instancia, fundamentar la adopción de políticas y actos legislativos[7]. Tenemos que utilizar los **análisis basados en la inteligencia** y las **evaluaciones de las amenazas** a escala de la UE de una manera más eficaz y colaborativa.

A partir de las distintas evaluaciones de riesgos y amenazas realizadas al nivel de la UE y para sectores específicos[8], la Comisión elaborará **análisis periódicos de las amenazas para la seguridad interior de la UE** a fin de detectar los principales retos en materia de seguridad y de fundamentar las prioridades estratégicas. Esta actividad contribuirá a desarrollar una política de seguridad interior ágil y reactiva que responda eficazmente a unas amenazas en constante evolución, ofrezca una mejor protección a las personas y las empresas frente a los ataques y permita realizar intervenciones específicas en tiempo oportuno. Estos análisis de las amenazas para la seguridad interior de la UE se integrarán también en **la evaluación general de riesgos y amenazas a escala de la UE (intersectorial y que abarque todos los peligros)** desarrollada por la Comisión y el Alto Representante, según se establece en la Estrategia de Preparación de la Unión.

El tratamiento de los datos en condiciones de seguridad y confianza es un factor esencial para el intercambio de información, que requiere unas infraestructuras fiables y seguras. Las instituciones, órganos y organismos de la UE deben garantizar su capacidad de utilizar **canales de comunicación seguros** para el intercambio de información sensible y clasificada, entre sí y con los Estados miembros. Las inversiones en **sistemas seguros interoperables** y tecnologías fiables reforzarán la autonomía de la UE y afianzarán su capacidad de gestionar crisis y asegurar la resiliencia operativa. Dado este contexto, la Comisión insta a los colegisladores a que concluyan las negociaciones relativas a la **propuesta de Reglamento sobre la seguridad de la información en las instituciones, órganos y organismos de la Unión**, en particular con el fin de garantizar un marco común para el tratamiento de la información sensible no clasificada y la información clasificada[9].

Para garantizar su seguridad operativa y su conciencia situacional propias, la Comisión revisará su marco de gobernanza de la seguridad institucional y creará un **Centro Integrado de Operaciones de Seguridad (ISOC)** con el que proteger a las personas, los activos físicos y las operaciones en todos los centros de la Comisión. Además, la Comisión fortalecerá sus capacidades operativas y analíticas para detectar y mitigar las amenazas híbridas.

En consonancia con la Estrategia de Preparación de la Unión, las consideraciones relativas a la preparación y a la seguridad se incluirán e integrarán en la legislación, las políticas y los programas de la UE. Al preparar nuevos actos legislativos, políticas o programas —o al revisar los existentes— desde la perspectiva de la preparación y la seguridad, la Comisión determinará sistemáticamente las posibles repercusiones sobre ambos aspectos de la opción estratégica seleccionada. Estas medidas se complementarán con formaciones periódicas destinadas a los responsables de la elaboración de las políticas de la Comisión.

En apoyo de los Estados miembros, la Comisión tratará con el Consejo acerca de la evolución de los retos para la seguridad interior y las prioridades de actuación esenciales y le mantendrá

[7] Más seguros juntos: fortalecimiento de la respuesta y la preparación civil y militar de Europa, p. 23.

[8] Entre las evaluaciones de amenazas por sectores que contribuirán a fundamentar este análisis se incluyen la Evaluación de la amenaza de la delincuencia grave y organizada de la UE (SOCTA), el Informe sobre la situación y las tendencias del terrorismo en Europa (TE-SAT), el Informe conjunto de evaluación de la ciberseguridad (JCAR) y las futuras evaluaciones de las amenazas, los riesgos y los métodos del blanqueo de capitales y la financiación del terrorismo que deberán llevar a cabo la Comisión y la Autoridad de Lucha contra el Blanqueo de Capitales.

[9] COM(2022) 119 final.

al corriente de la aplicación de la Estrategia. Además, mantendrá informados sobre todas las acciones pertinentes e implicados en ellas al Parlamento Europeo y a las partes interesadas.

Medidas clave

La Comisión:

- **elaborará y presentará análisis periódicos de amenazas en relación con los retos para la seguridad interior de la UE**

Se insta a los Estados miembros a que:

- **mejoren la puesta en común de inteligencia con la SIAC y aseguren un mejor intercambio de información con los órganos y organismos de la UE**

Se invita al Parlamento Europeo y al Consejo a que:

- **concluyan las negociaciones relativas a la propuesta de Reglamento sobre la seguridad de la información en las instituciones, órganos y organismos de la Unión**

3. Refuerzo de las capacidades de seguridad de la UE

Desarrollaremos nuevas herramientas para las fuerzas y cuerpos de seguridad, como la renovación de Europol, y mejoraremos los medios para coordinar y garantizar el intercambio seguro de datos y el acceso lícito a estos.

Si aspira a neutralizar con eficacia unas amenazas que se hallan en constante evolución, la UE debe robustecer sus capacidades de seguridad y fomentar la innovación. Como principales agentes contra las amenazas a la seguridad interior, las autoridades policiales y judiciales necesitan disponer de las herramientas y las capacidades operativas adecuadas para actuar con rapidez y eficacia. Es importante que, para llevar a cabo diligentemente su labor de prevención, detección, investigación y enjuiciamiento, estas autoridades puedan comunicarse y coordinarse de un país a otro y de un departamento a otro.

Órganos y organismos de la UE para la seguridad interior

Los órganos y organismos de la UE en los ámbitos de la justicia, los asuntos de interior y la ciberseguridad desempeñan un papel clave en la estructura de seguridad de la UE, papel que sigue creciendo a medida que se amplían sus responsabilidades.

Hoy, veinticinco años después de su creación, **Europol** es un organismo más necesario que nunca para el marco de seguridad de la UE. Permite realizar complejas investigaciones transfronterizas, facilita el intercambio de información, desarrolla innovadoras herramientas para la actividad policial y proporciona conocimientos especializados avanzados a las fuerzas y cuerpos de seguridad. Sin embargo, diversos factores impiden que Europol alcance todo su potencial de apoyo a las actividades investigativas y operativas de lucha contra la delincuencia transfronteriza: desde un insuficiente nivel de recursos hasta el hecho de que su mandato actual no cubre las nuevas amenazas a la seguridad, como el sabotaje, las amenazas híbridas o la manipulación de la información. Esa es la razón que lleva a la Comisión a proponer una **ambiciosa renovación del mandato de Europol** para convertir este organismo en una agencia policial verdaderamente operativa que preste un apoyo más provechoso a los Estados miembros. El objetivo es desarrollar los conocimientos tecnológicos y la capacidad de Europol para asistir a las fuerzas y cuerpos de seguridad nacionales, mejorar su coordinación con otros órganos y organismos y con los Estados miembros, reforzar las asociaciones estratégicas con los países socios y el sector privado y asegurar una mayor supervisión de Europol.

Además, la Comisión se afanará por seguir **mejorando la eficacia y la complementariedad de los órganos y organismos de la UE responsables de la seguridad interior y por reforzar la cooperación fluida** entre ellos.

El mandato de **Eurojust** se analizará y fortalecerá con el fin de lograr una cooperación judicial más eficaz, potenciando la complementariedad y la cooperación con Europol. Para ello es preciso, entre otras cosas, aumentar la eficiencia de Eurojust, así como su capacidad para prestar apoyo y presentar análisis de forma proactiva a las autoridades judiciales de los Estados miembros. Además, dada la competencia exclusiva de la **Fiscalía Europea** para investigar y enjuiciar los delitos que afectan a los intereses financieros de la Unión, la Comisión estudiará la mejor manera de ampliar la capacidad de este organismo para proteger los fondos de la Unión; será necesario con tal fin reforzar la cooperación entre la Fiscalía Europea y Europol.

Un **intercambio de información eficaz y seguro entre las agencias** es crucial para la cooperación. Europol y Frontex necesitan dotarse de un sistema rápido de intercambio de información (entre otros motivos, con fines operativos), atendiendo a lo expuesto en la Declaración conjunta de enero de 2024[10]. **eu-LISA** desempeña un papel central a la hora de garantizar el almacenamiento seguro y la disponibilidad de datos para una mejor coordinación y un intercambio de información más eficiente entre las agencias. La **Agencia de los Derechos Fundamentales de la Unión Europea** aporta conocimientos especializados sobre la protección de los derechos fundamentales en el desarrollo y la aplicación de las políticas de seguridad.

La **Autoridad de Lucha contra el Blanqueo de Capitales (ALBC) de la UE** ha sido facultada para cotejar la información, siguiendo el criterio de coincidencia o no coincidencia (*hit/no hit)*, con la información facilitada por Europol, la Fiscalía Europea, Eurojust y la Oficina de Lucha contra el Fraude de la UE, a fin de llevar a cabo análisis conjuntos de casos transfronterizos.

ENISA desempeña un papel esencial en la aplicación de la legislación europea en materia de ciberseguridad. En su revisión del **Reglamento sobre la Ciberseguridad**, la Comisión estudiará el mandato de esta agencia y propondrá su modernización a fin de aumentar el valor añadido que aporta a escala de la UE.

La cooperación entre las autoridades aduaneras y otras autoridades policiales se ampliará con la propuesta de creación de la **Autoridad Aduanera de la UE** y del **Centro Aduanero de Datos de la UE** en el marco del paquete de reformas aduaneras de la UE. La información procedente de este futuro Centro y los correspondientes datos facilitados por Europol, Eurojust, la Fiscalía Europea, la OLAF, la ALBC y Frontex en el contexto de sus respectivas competencias mejorarán los análisis conjuntos y contribuirán al aumento de la coherencia de las actividades operativas, especialmente las llevadas a cabo en las fronteras exteriores. La Comisión anima a los colegisladores a que ultimen sin dilación las negociaciones sobre la reforma aduanera de la UE, objetivo para el que seguirá prestándoles asistencia.

Los resultados de la revisión en curso de la **arquitectura de la UE de lucha contra el fraude** contribuirán también al aumento de la complementariedad entre la Fiscalía Europea, la OLAF, Europol, Eurojust, la ALBC y la Autoridad Aduanera de la UE propuesta. Este enfoque holístico, centrado en un mejor uso de los medios tanto penales como administrativos, la interoperabilidad de los sistemas informáticos y la mejora de la cooperación sería beneficioso para la seguridad interior.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

Comunicación crítica

En la actualidad, la mayor parte de los **sistemas de comunicación crítica**[11] funcionan de forma aislada a nivel nacional. Esto significa, a menudo, que el personal de primera intervención no puede comunicarse con sus homólogos cuando cruza las fronteras de otros Estados miembros. En algunos Estados miembros, existen además limitaciones a las comunicaciones entre los distintos tipos de equipos de primera intervención (por ejemplo, la policía y las ambulancias). Los estándares de la mayoría de los sistemas no cumplen los requisitos actuales en términos de funcionalidad y resiliencia, lo que restringe considerablemente la capacidad de reacción de dichos equipos, especialmente a través de las fronteras.

Para mejorar la capacidad de reacción de la UE ante las crisis, la Comisión propondrá un acto legislativo por el que se cree un **Sistema Europeo de Comunicación Crítica (SEUCC)** que conecte los sistemas de comunicación crítica de próxima generación de los Estados miembros. La intención es que el SEUCC se base en tres pilares estratégicos: movilidad operativa, fuerte resiliencia y autonomía estratégica. La iniciativa SEUCC fijará unos requisitos armonizados y contribuirá a modernizar los sistemas de comunicación crítica de los Estados miembros, permitiéndoles funcionar sin interrupción. Además, ampliará la cobertura de la red gracias al futuro sistema multiorbital IRIS^{2} [12], Proyectos financiados por la UE desarrollarán las capacidades técnicas del SEUCC, para lo que se recurrirá principalmente a proveedores de tecnología europeos a fin de fomentar la autonomía estratégica de la UE en este sector sensible.

Acceso lícito a los datos

Las fuerzas y cuerpos de seguridad y las autoridades judiciales deben poder realizar su labor de investigación y actuar contra la delincuencia. Hoy en día, casi todas las formas de delincuencia grave y organizada dejan una huella digital[13]. Aproximadamente el 85 % de las investigaciones penales dependen ahora de la capacidad de las autoridades policiales y judiciales para acceder a información digital[14].

El **Grupo de Alto Nivel sobre el acceso a los datos para una aplicación eficaz de la ley** destacó en su informe de conclusiones[15] que, a lo largo de la última década, tanto las fuerzas y cuerpos de seguridad como la administración de justicia habían ido perdiendo terreno en favor de los delincuentes, los cuales se sirven de herramientas y productos procedentes de otros países y de proveedores que han puesto en marcha medidas que les privan de los medios necesarios para tramitar adecuadamente las solicitudes de cooperación judicial en casos penales individuales. Por lo tanto, la cooperación sistemática entre las autoridades policiales y judiciales y ciertos particulares, como los proveedores de servicios, es esencial para las futuras medidas dirigidas a desbaratar la actividad de las redes delictivas y los individuos más peligrosos en la Unión y fuera de ella.

Habida cuenta de que la digitalización se está generalizando y proporciona una fuente cada vez mayor de herramientas nuevas a los delincuentes, resulta esencial disponer de un marco regulador del acceso a los datos que responda a la necesidad de hacer cumplir nuestras leyes a la vez que protegemos nuestros valores. Al mismo tiempo, garantizar que los sistemas digitales sigan siendo seguros frente a todo acceso no autorizado es igualmente vital para preservar la

[11] Es decir, las redes utilizadas por las fuerzas y cuerpos de seguridad, los guardias de fronteras, las autoridades aduaneras, la protección civil, los bomberos, los servicios médicos de urgencia y otros intervinientes esenciales para la seguridad y la protección públicas.
[12] Infraestructura para la Resiliencia, la Interconectividad y la Seguridad por Satélite de la UE
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[14] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52019PC0070.
[15] Informe de conclusiones del Grupo de Alto Nivel sobre el acceso a los datos para una aplicación eficaz de la ley - 15.11.2024, 4802e306-c364-4154-835b-e986a9a49281_en.

ciberseguridad y ofrecer protección contra las amenazas emergentes para la seguridad. Estos marcos reguladores del acceso a la información deben también respetar los derechos fundamentales y garantizar, entre otros extremos, que la privacidad y los datos personales estén adecuadamente protegidos.

En los últimos años, la UE ha adoptado medidas con el fin tanto de **luchar contra la delincuencia en línea como de facilitar el acceso a las pruebas digitales de todo tipo de delitos**, para lo que ha aprobado un conjunto de normas sobre pruebas electrónicas que se aplicarán plenamente a partir de agosto de 2026[16]. Estas normas se complementarán con los instrumentos internacionales de intercambio de información y pruebas. La Comisión propondrá próximamente la firma y celebración de la nueva **Convención de las Naciones Unidas contra la Ciberdelincuencia**.

Siguiendo las recomendaciones del Grupo de Alto Nivel[17], la Comisión presentará en el primer semestre de 2025 una **hoja de ruta en la que expondrá las medidas jurídicas y prácticas** que propone adoptar para **garantizar un acceso lícito y efectivo a los datos**. Al navegar por esta hoja de ruta, la Comisión dará prioridad a la evaluación del impacto de las **normas de conservación de datos** al nivel de la UE y a la preparación de una **hoja de ruta tecnológica sobre cifrado** con el fin de buscar y estudiar soluciones tecnológicas que permitan a las autoridades policiales acceder a datos cifrados de manera lícita, sin perjuicio de la ciberseguridad ni de los derechos fundamentales.

Cooperación operativa

La Comisión trabajará junto con los Estados miembros, las agencias y organismos de la UE y los países socios para reforzar la cooperación operativa, elemento esencial para un enfoque más eficaz de la lucha contra la delincuencia organizada y el terrorismo transnacionales.

Como principal marco de la UE en el que se inscribe la acción conjunta contra la delincuencia grave y organizada, **la plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT)** ha logrado sustanciales resultados operativos. El próximo ciclo de la EMPACT, 2026-2029, brinda la oportunidad de reforzar todavía más este marco. Para desarticular la actividad de las redes delictivas y los individuos que suponen una mayor amenaza, la Unión debe organizar y centrar sus esfuerzos en torno a las prioridades más acuciantes, reforzando los compromisos de los Estados miembros y garantizando un uso eficaz de los recursos.

A tal fin, la Comisión trabajará con las Presidencias del Consejo y con los Estados miembros para **maximizar el potencial de la EMPACT y abordar las prioridades clave para el próximo ciclo, 2026-2029**. Las necesidades comunes a todos estos ámbitos prioritarios son las siguientes: información estratégica sobre las redes delictivas más peligrosas, investigaciones y grupos de trabajo operativos conjuntos y una respuesta judicial firme que incorpore el enfoque consistente en «seguir el rastro del dinero». Además, la Unión debe hacer frente a las actividades de captación e infiltración con fines delictivos y reforzar las actividades de cooperación y formación interinstitucionales e internacionales en materia de control del cumplimiento de la ley.

La Comisión apoyará también otras formas de **cooperación policial transfronteriza operativa entre los Estados miembros y los países asociados a Schengen**. Al estar libre de controles en

[16] Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales (DO L 191 de 28.7.2023).
[17] Conclusiones del Consejo sobre el acceso a los datos para una aplicación eficaz de la ley (12 de diciembre de 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/es/pdf.

las fronteras interiores, el espacio Schengen requiere una estrecha cooperación y el intercambio de información entre las autoridades policiales de los Estados miembros para garantizar un alto nivel de seguridad interior. En la actualidad, los agentes de las fuerzas y cuerpos de seguridad siguen enfrentándose a dificultades a la hora de desarrollar su labor de vigilancia o de llevar a cabo intervenciones urgentes que requieren el cruce de fronteras[18]; la lucha contra las amenazas híbridas también exige una mayor cooperación transfronteriza. Es preciso crear un **Grupo de alto nivel sobre el futuro de la cooperación policial operativa** con el fin de desarrollar una visión estratégica común.

El intercambio eficiente de datos entre autoridades policiales también es esencial para una cooperación transfronteriza eficaz. Una vez establecida, la **arquitectura de interoperabilidad** proporcionará a las autoridades policiales y a Europol un acceso efectivo a información crucial. Al mismo tiempo, la UE y sus Estados miembros deben dar prioridad al intercambio bilateral y multilateral de información a través de la aplicación jurídica y técnica del **Reglamento Prüm II**[19], en cooperación con eu-LISA y Europol. Esto posibilitará el intercambio automatizado y seguro de impresiones dactilares, perfiles de ADN, datos de matriculación de vehículos, imágenes faciales y antecedentes policiales a través de enrutadores de la UE. A nivel nacional, los Estados miembros deben aplicar la **Directiva relativa al intercambio de información**[20], mejorando los canales de intercambio de información para establecer un flujo transfronterizo de información sin interrupciones y garantizar, al mismo tiempo, su integración en los sistemas existentes a escala de la Unión, como SIENA[21].

La eficacia de la cooperación transfronteriza depende también del fomento de una **cultura policial común en la UE**. La formación conjunta, los centros de excelencia y los programas de movilidad son esenciales para alcanzar este objetivo. La Comisión estudiará la mejor forma de que la UE apoye la formación de las autoridades de los Estados miembros, recurriendo a la **CEPOL** como agencia de la UE para la formación policial.

Aumento de la seguridad de las fronteras

El aumento de la resiliencia y la seguridad de las fronteras exteriores es un factor crucial para neutralizar las amenazas híbridas, como la instrumentalización de la migración, para evitar que los agentes y las mercancías de riesgo entren en la UE y para luchar eficazmente contra la delincuencia transfronteriza y el terrorismo. **Está previsto modernizar el Sistema de Información de Schengen (SIS)** en 2026, de forma que los Estados miembros puedan introducir descripciones de nacionales de terceros países implicados en actividades terroristas —como los combatientes terroristas extranjeros— y en otros delitos graves, tomando como base los datos facilitados por terceros países a Europol.

La mejora de la **interoperabilidad** de los sistemas de información a gran escala de la UE proporcionará a los Estados miembros información esencial sobre los nacionales de terceros países que crucen o tengan la intención de cruzar las fronteras exteriores, lo que ayudará a las

[18] Como se indica en la evaluación realizada por la Comisión de los efectos dados por los Estados miembros a la Recomendación (UE) 2022/915 del Consejo, de 9 de junio de 2022, relativa a la cooperación policial operativa (5909/25).

[19] Reglamento (UE) 2024/982 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, relativo a la búsqueda y al intercambio automatizados de datos para la cooperación policial, y por el que se modifican las Decisiones 2008/615/JAI y 2008/616/JAI del Consejo y los Reglamentos (UE) 2018/1726, (UE) 2019/817 y (UE) 2019/818 del Parlamento Europeo y del Consejo (Reglamento Prüm II) (DO L 2024/982 de 5.4.2024).

[20] Directiva (UE) 2023/977 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, relativa al intercambio de información entre los servicios de seguridad y de aduanas de los Estados miembros, por la que se deroga la Decisión Marco 2006/960/JAI del Consejo (DO L 134 de 22.5.2023, p. 1).

[21] Aplicación de la Red de Intercambio Seguro de Información.

autoridades a determinar si cumplen las condiciones que permiten autorizar su entrada en el territorio de los Estados miembros[22]. La Comisión mantendrá su estrecha colaboración con los Estados miembros y eu-LISA para la ágil aplicación de estos sistemas, en particular el **Sistema de Entradas y Salidas (SES), el Sistema Europeo de Autorización de Viajes (SEIAV) y el Sistema de Información de Visados (VIS) revisado**, a fin de garantizar su buen funcionamiento y los beneficios que aportan en materia de seguridad.

Para seguir fortaleciendo la seguridad de las fronteras y consolidando la cooperación de la UE frente a unas amenazas en constante evolución, **la Comisión propondrá el refuerzo de Frontex**. La Guardia Europea de Fronteras y Costas debería triplicar sus efectivos con el tiempo hasta alcanzar los 30 000. Es preciso equipar a esta Agencia con tecnología avanzada de vigilancia y conciencia situacional que le permita obtener, entre otros datos, la inteligencia pertinente para la gestión europea integrada de las fronteras y el acceso a servicios fiables de la UE de observación de la Tierra con fines de control fronterizo, que se implantarán de aquí a 2027. Estas medidas deberían potenciar más aún la capacidad de detectar, prevenir y combatir la delincuencia transfronteriza en las fronteras exteriores, así como reforzar la asistencia brindada por Frontex a los Estados miembros para la ejecución de los retornos, en particular cuando se trate de nacionales de terceros países que planteen algún riesgo para la seguridad.

El fraude documental y de identidad facilita el tráfico ilícito de migrantes, la trata de seres humanos, los movimientos clandestinos con fines delictivos y el tráfico de mercancías ilícitas. Una vez entre en funcionamiento, el **detector de identidades múltiples (DIM)**[23] mejorará la capacidad de las autoridades nacionales para identificar a las personas que estén utilizando identidades múltiples y así luchar contra la usurpación de identidad. La Comisión explorará vías para mejorar la seguridad de los documentos de viaje y residencia expedidos a ciudadanos de la UE y nacionales de terceros países. Además, estudiará la forma en que las carteras europeas de identidad digital, que se introducirán antes de que termine 2026 con arreglo al marco europeo de identidad digital, pueden contribuir a mejorar la seguridad de los documentos de viaje y la comprobación de la identidad. Estas medidas complementarán las propuestas sobre credenciales de viaje digitales y sobre la aplicación de viaje digital de la UE[24].

La **información sobre viajes** es crucial para que las autoridades detecten e investiguen los movimientos de los delincuentes, los terroristas y otros individuos que planteen amenazas para la seguridad. Si bien existe ya un marco de la UE para la información sobre los viajes aéreos comerciales[25], el tratamiento con fines policiales de los datos correspondientes a los otros modos de transporte está recogido en normas fragmentadas. Ello permite, por lo tanto, a los delincuentes y terroristas utilizar esos otros modos de transporte de forma que sus actividades ilegales pasen desapercibidas. La Comisión trabajará junto con los Estados miembros y el sector del transporte para **reforzar el marco de información sobre viajes**, examinando la posibilidad de implantar un régimen de la Unión que exija a los operadores de vuelos privados recoger y notificar los datos de los pasajeros, evaluando las normas de tratamiento de los registros de

[22] Concretamente, el Sistema de Entradas y Salidas (SES) permitirá a los Estados miembros identificar a los nacionales de terceros países en las fronteras exteriores del espacio Schengen y registrar sus entradas y salidas, posibilitando así la inmediata detección de quienes hayan sobrepasado el período de estancia autorizada. Antes de la llegada de cualquier nacional de un tercer país a las fronteras exteriores, el Sistema Europeo de Información y Autorización de Viajes (SEIAV) y el Sistema de Información de Visados (VIS) permitirán a los Estados miembros evaluar previamente si la presencia de esa persona en el territorio de la UE supondría algún riesgo para la seguridad.

[23] EL DIM es uno de los componentes de la interoperabilidad introducidos por el Reglamento (UE) 2019/818 y el Reglamento 2019/817.

[24] https://ec.europa.eu/commission/presscorner/detail/es/ip_24_5047.

[25] Marcos que regulan los registros de nombres de los pasajeros (PNR, por sus siglas en inglés) y la información anticipada sobre los pasajeros (API, por sus siglas en inglés) establecidos, respectivamente, por la Directiva (UE) 2016/681 («Directiva PNR») y los Reglamentos (UE) 2025/12 y (UE) 2025/13 («Reglamentos API»).

nombres de los pasajeros y estudiando formas de racionalizar el tratamiento de la información sobre viajes marítimos. Por lo que respecta al transporte por carretera, la Comisión analizará la posible ampliación del uso de los sistemas de **reconocimiento automático de matrículas (RAM)** y aumentará las posibilidades de sinergias de estos sistemas con el SIS.

Prospectiva, innovación y enfoque basado en las capacidades

La Comisión desarrollará un **enfoque prospectivo global de la seguridad interior a escala de la UE**, basándose en las mejores prácticas destacadas a nivel nacional, que sustentará la elaboración de políticas y orientará las inversiones en los programas de investigación e innovación en materia de seguridad pertinentes financiados por la UE.

La investigación y la innovación desempeñan un papel crucial en la seguridad interior por su capacidad de crear soluciones para neutralizar las amenazas emergentes, incluidas las derivadas del uso indebido de la tecnología[26]. La UE debe seguir invirtiendo, a través de la financiación de la investigación y la innovación en materia de seguridad[27], en el desarrollo de herramientas y soluciones innovadoras para hacer frente a las amenazas a la seguridad, sin menoscabo alguno de las normas y los derechos fundamentales de la UE. La Comisión debe apoyar la transición desde la fase de investigación a la de implantación para asegurar la adopción efectiva de esas capacidades modernas, otorgando prioridad a las **tecnologías modernas** como la IA. Este enfoque debe incluir actividades de formación para mejorar el uso de los sistemas de IA y otras capacidades técnicas por parte de las autoridades policiales y judiciales. Además, cuando así proceda, debe aprovecharse el potencial de doble uso de las tecnologías en ambas direcciones (del uso civil al uso de defensa y viceversa)[28].

El **Centro de Innovación de la UE para la Seguridad Interior**[29], una red de laboratorios de innovación que ofrece lo último en materia de innovación y soluciones eficaces para apoyar la labor de los agentes responsables de la seguridad interior en la UE y los Estados miembros, contribuirá a integrar la investigación en la práctica y las políticas. Para aumentar la eficacia de Europol es preciso reforzar su repositorio de herramientas, lo que permitirá a esta agencia localizar, desarrollar, adquirir conjuntamente y aplicar tecnologías avanzadas de forma operativa. Además, la Comisión creará, en el seno de su Centro Común de Investigación, un **Campus de Investigación e Innovación en materia de Seguridad** que reunirá a investigadores con el objetivo de acortar el ciclo que va desde la fase de obtención de los resultados de la investigación hasta las fases de innovación, desarrollo y aplicación fructífera, reduciendo al mismo tiempo los costes de desarrollo, ensayo y validación.

Nuestro **Espacio Europeo de Investigación** es, por su propia naturaleza, colaborativo y, por tanto, permeable a las injerencias extranjeras y la desinformación. A raíz de la adopción de la Recomendación del Consejo sobre la seguridad de la investigación[30], la Comisión y los Estados miembros han empezado a tomar medidas para capacitar a los agentes pertinentes, por ejemplo, la creación de un Centro de Asesoramiento sobre Seguridad de la Investigación.

---

[26] Véase el informe del Centro Común de Investigación de la Comisión sobre los «Nuevos riesgos y oportunidades para la seguridad interna de la UE derivados de las nuevas tecnologías» (*Emerging risks and opportunities for EU internal security stemming from new technologies*, documento disponible únicamente en inglés), https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] Estudio sobre el refuerzo de la investigación y la innovación en materia de seguridad financiadas por la UE: 20 años de investigación e innovación sobre seguridad civil financiadas por la UE, 2025 (*Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025*, documento disponible únicamente en inglés), https://data.europa.eu/doi/10.2837/0004501.

[28] Según lo indicado en el informe Niinistö.

[29] Centro de Innovación de la UE para la Seguridad Interior | Europol.

[30] DO C, C/2024/3510, 30.5.2024.

Medidas clave

La Comisión adoptará:

- **una propuesta legislativa para transformar a Europol en una agencia policial verdaderamente operativa en 2026**
- **una propuesta legislativa para reforzar Eurojust en 2026**
- **una propuesta legislativa para reforzar el papel y las tareas de Frontex en 2026**
- **una propuesta legislativa para establecer un sistema europeo de comunicación crítica en 2026**

La Comisión:

- **presentará en 2025 una hoja de ruta para lograr que las fuerzas y cuerpos de seguridad adquieran un acceso lícito y efectivo a los datos**
- **preparará en 2025 una evaluación de impacto con el fin de actualizar las normas sobre conservación de datos a escala de la UE, según proceda**
- **presentará en 2026 una hoja de ruta tecnológica sobre cifrado para buscar y analizar soluciones tecnológicas que permitan el acceso lícito a los datos por parte de las autoridades policiales**
- **trabajará en la creación de un Grupo de Alto Nivel para reforzar la cooperación policial operativa**
- **creará un Campus de Investigación e Innovación en materia de Seguridad, en el seno de su Centro Común de Investigación, en 2026**

La Comisión, en cooperación con los Estados miembros y las agencias pertinentes de la UE:

- **reforzará la arquitectura de la EMPACT**
- **trabajará para la rápida implantación de la arquitectura de interoperabilidad y la aplicación del Reglamento Prüm II**
- **reforzará el marco de información sobre viajes**

Se insta a los Estados miembros a que:

- **transpongan y den plena aplicación a la Directiva relativa al intercambio de información**

4. Resiliencia frente a las amenazas híbridas y otros actos hostiles

Aumentaremos la resiliencia frente a las amenazas híbridas reforzando la protección de las infraestructuras críticas, aumentando la ciberseguridad, la seguridad de los intercambiadores de transporte y los puertos y luchando contra las amenazas en línea.

Hemos asistido a un aumento tanto de la frecuencia como del grado de sofisticación de los actos hostiles que socavan la seguridad de la UE, y a una ampliación del arsenal empleado por los agentes malintencionados. Se han recrudecido las campañas híbridas dirigidas a la UE, sus Estados miembros y sus socios mediante actos de sabotaje contra infraestructuras críticas, incendios provocados, ciberataques, interferencias en los procesos electorales, injerencias y manipulación de información —incluidas actividades de desinformación— por parte de agentes extranjeros e instrumentalización de la migración. Debido a su papel político y operativo y a la naturaleza de la información que manejan, las instituciones, órganos y organismos de la Unión (en lo sucesivo, «las entidades de la Unión») no están exentos de este tipo de ataques.

La UE debe **aumentar su resiliencia**, utilizar con eficacia las herramientas de que dispone actualmente y desarrollar nuevas formas de hacer frente, tanto ahora como en el futuro, a estas amenazas en constante evolución por parte de agentes estatales y no estatales.

Infraestructuras críticas

Las amenazas a las **infraestructuras críticas** —incluidas las amenazas de carácter híbrido, como el sabotaje y la actividad cibernética malintencionada— son causa de honda preocupación, especialmente cuando afectan a infraestructuras que conectan a los Estados miembros, ya se trate de interconectores energéticos o de cables de comunicación transfronterizos, y a modos de transporte. Desde que empezó la guerra de agresión de Rusia contra Ucrania, han aumentado los actos de sabotaje contra infraestructuras críticas, en particular en 2024, y han perjudicado a numerosos Estados miembros. La cooperación entre las fuerzas del orden, los servicios de seguridad y ciberseguridad, los cuerpos militares y de protección civil y los operadores privados es esencial para anticipar, detectar, prevenir y responder eficazmente a tales actos.

Es imperativo reducir las fragilidades y reforzar la resiliencia de las entidades críticas para garantizar la prestación ininterrumpida de servicios esenciales que resultan vitales para la economía y la sociedad. La transposición en los plazos fijados y la correcta aplicación por todos los Estados miembros de la **Directiva relativa a la resiliencia de las entidades críticas (REC)** [31]**y la Directiva destinada a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2)**[32] son, por lo tanto, cruciales para esos fines.

Para asegurar que se avanza con rapidez, la Comisión asistirá a los Estados miembros en la tarea de determinar las entidades críticas[33] y en el intercambio de buenas prácticas sobre estrategias nacionales y evaluaciones de riesgos en lo que respecta a los servicios esenciales, en cooperación con el **Grupo de Resiliencia de las Entidades Críticas y el Grupo de Cooperación SRI**. De producirse perturbaciones en infraestructuras críticas con importantes repercusiones transfronterizas, las respuestas al nivel de la UE se coordinarán con arreglo al **Plan Director de la UE de Infraestructuras Críticas.** La Comisión anima al Consejo a que adopte, sin más demora, el **Plan Director de Ciberseguridad de la UE**, que reforzará todavía más la coordinación en el contexto de la gestión de crisis, facilitando una colaboración más estrecha en materia de resiliencia física y digital entre las autoridades competentes. Tras el éxito de las pruebas de resistencia del sector energético en 2023, la Comisión promoverá la realización de **pruebas de resistencia voluntarias** en otros sectores clave para la seguridad interior. Además, elaborará un **panorama general, a escala de la Unión, de los riesgos transfronterizos e intersectoriales** para los servicios esenciales, con el fin de sustentar las evaluaciones de riesgos de los Estados miembros y de sentar las bases para una evaluación de riesgos exhaustiva al nivel de la UE. Conforme a lo expuesto en la Estrategia de Preparación de la Unión, la Comisión colaborará con los Estados miembros en la detección de otros sectores y servicios no cubiertos por la legislación actual y respecto de los que podría ser necesario actuar.

[31] Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

[32] 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 (Directiva SRI 2).

[33] Los sectores contemplados por la Directiva son la energía, el transporte, la banca, las infraestructuras de los mercados financieros, la salud, el agua potable, las aguas residuales, la infraestructura digital, la administración pública, el espacio y la producción, transformación y distribución de alimentos.

El **Grupo de Trabajo UE-OTAN sobre la resiliencia de las infraestructuras críticas** ha propiciado una excelente cooperación a la hora de poner en común las mejores prácticas y mejorar la resiliencia en los sectores de la energía, el transporte, las infraestructuras digitales y el espacio. Esta labor proseguirá en el marco del **diálogo estructurado UE-OTAN sobre resiliencia**. El **conjunto de instrumentos de la UE contra las amenazas híbridas** ofrece a los Estados miembros y a nuestros socios un sólido apoyo para la preparación y la lucha contra estas amenazas. Los **equipos de respuesta rápida contra amenazas híbridas**[34] proporcionan asistencia individualizada a corto plazo a los Estados miembros, las misiones de la UE y otros socios que así la soliciten. Además, la Comisión impulsará la cooperación de la UE en la lucha contra el sabotaje a través de actividades de expertos[35] que incluirán un **programa de trabajo conjunto específico** para que los expertos racionalicen el intercambio de información y hagan un catálogo de contramedidas.

Los incidentes que afectan a los **cables submarinos** en Europa ponen de relieve la necesidad de adoptar medidas más estrictas y ofrecer respuestas más claras. Como se indica en el **Plan de Acción de la UE sobre la seguridad de los cables**[36], la Comisión, junto con el Alto Representante, colaborará con los Estados miembros, las agencias de la UE y otros socios, como la OTAN, para prevenir y detectar las amenazas a los cables submarinos, responder a ellas y disuadir a sus posibles autores. A fin de construir una visión integrada de la situación de estas amenazas, la Comisión trabajará junto con los Estados miembros para desarrollar e implantar, con carácter voluntario, un mecanismo integrado de vigilancia de los cables submarinos por cuencas marítimas, empezando por un centro regional nórdico/báltico.

Ciberseguridad

La naturaleza persistente de la **ciberactividad malintencionada**, que a menudo no es sino un elemento dentro de una gama más amplia de amenazas multidimensionales e híbridas, requiere una atención y una acción continuas a escala europea. En los últimos años, la Unión ha adoptado un conjunto de actos legislativos en materia de ciberseguridad que refuerzan la ciberresiliencia de las entidades contempladas en la Directiva SRI 2 que operan en sectores críticos de la UE[37] —así como la de las entidades de la Unión—, aumentan la seguridad de los productos digitales (Reglamento de Ciberresiliencia) y establecen un marco de apoyo para la preparación y la respuesta a incidentes (Reglamento de Cibersolidaridad). En enero de 2025, la Comisión adoptó el **Plan de Acción europeo sobre la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria**[38] con el fin de mejorar en ese sector la detección de amenazas, la preparación ante las crisis y la respuesta a estas. Su plena aplicación es un factor esencial. Al mismo tiempo, para hacer frente a nuevas amenazas y sucesos hasta ahora inéditos, debemos intensificar nuestra actividad, en particular en los ámbitos del intercambio de información, la seguridad de la cadena de suministro, los programas de secuestro de archivos y los ciberataques, así como la soberanía tecnológica.

---

[34] Brújula Estratégica de la UE para la Seguridad y la Defensa 2022, p. 22.

[35] Los asesores en materia de seguridad preventiva de la UE, la Red de Unidades de Desactivación de Municiones Explosivas (EEODN, por sus siglas en inglés), la Red ATLAS, la Red de Seguridad de Alto Riesgo de la UE (EU-HRSN, por sus siglas en inglés), el Grupo consultivo sobre seguridad QBRN y el Grupo de Resiliencia de las Entidades Críticas (CERG, por sus siglas en inglés).

[36] JOIN(2025) 9 final.

[37] Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión (DO L, 2023/2841, 18.12.2023).

[38] https://digital-strategy.ec.europa.eu/es/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

Por otra parte, la aplicación de estas iniciativas exige colmar el actual déficit de capacidades en materia de ciberseguridad, que equivale a 299 000 personas. La Comisión trabajará junto con los Estados miembros en el marco de la Unión de las Competencias[39] para aumentar la mano de obra dedicada a la ciberseguridad, para lo que recurrirá, en particular, a la nueva Academia de Cibercapacidades. El Plan Estratégico para la Enseñanza de las CTIM (ciencias, tecnologías, ingenierías y matemáticas)[40] contribuye a ampliar la reserva de profesionales de talento y a mejorar la respuesta de Europa a las necesidades en materia de ciberseguridad del mercado laboral.

En paralelo al aumento de su resiliencia, la UE seguirá haciendo pleno uso del marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas (**el conjunto de instrumentos de ciberdiplomacia**) a fin de prevenir las ciberamenazas procedentes de agentes estatales y no estatales, responder a ellas y disuadir a sus posibles autores.

Seguridad de las cadenas de suministro de TIC

El **conjunto de instrumentos para la seguridad de las redes 5G** proporciona la estructura adecuada para la protección de las redes 5G, pero su aplicación por parte de los Estados miembros es actualmente insuficiente. Persisten riesgos inaceptables para la seguridad, en particular en lo que respecta a la sustitución de los proveedores de alto riesgo. La aplicación de un enfoque armonizado a la seguridad de la cadena de suministro de TIC puede poner remedio a la actual fragmentación del mercado interior causada por los diferentes planteamientos nacionales, evitar dependencias decisivas y rebajar el riesgo que plantean determinados proveedores (los llamados «de alto riesgo») de nuestras cadenas de suministro de TIC, afianzando así nuestras infraestructuras críticas.

En consonancia con este enfoque, la Comisión aprovechará la próxima **revisión del Reglamento de Ciberseguridad** para acometer un examen más general de la seguridad y la resiliencia de las cadenas de suministro de TIC y su infraestructura. Además, la Comisión propondrá una mejora del **marco europeo de certificación de la ciberseguridad** para garantizar que los futuros regímenes de certificación puedan adoptarse en tiempo oportuno y responder a las necesidades estratégicas.

Basándose en las evaluaciones sectoriales ya realizadas o en curso[41], la Comisión desarrollará, junto con los Estados miembros, una **planificación estratégica de las evaluaciones coordinadas de los riesgos de ciberseguridad**.

Los servicios en la nube y las telecomunicaciones se han convertido en un elemento básico de las cadenas de suministro para las infraestructuras críticas, las empresas y las autoridades públicas. La Comisión adoptará medidas para animar a las entidades críticas a que opten por **servicios en la nube y de telecomunicaciones que ofrezcan un nivel adecuado de ciberseguridad**, teniendo en cuenta no solo los riesgos técnicos, sino también los riesgos y dependencias estratégicos.

Programas de secuestro de archivos y ciberataques

Los **programas de secuestro de archivos** siguen siendo uno de los grandes y persistentes retos para la ciberseguridad en la UE y en el resto del mundo; un informe indica que su coste anual

[39] COM(2025) 90 final.
[40] COM(2025) 89 final.
[41] Por ejemplo, las relativas a las redes 5G, las telecomunicaciones, la electricidad, las energías renovables y los vehículos conectados.

total habrá superado 250 000 millones EUR en 2031[42]. Tanto la **Directiva SRI 2** como el **Reglamento de Ciberresiliencia** mejorarán considerablemente la postura de seguridad de las distintas entidades, lo que encarecerá los ataques para las redes que se sirven de los programas de secuestro. Además, la Comisión colaborará estrechamente con los Estados miembros para asegurar que los programas de secuestro —en particular cuando se trate de amenazas persistentes avanzadas— y los pagos de rescates se denuncien con más frecuencia a la policía, facilitando con ello las investigaciones.

A fin de prevenir y detener los ciberataques, la UE debe fortalecer el intercambio de información entre las autoridades policiales y judiciales, las autoridades y organismos responsables de la ciberseguridad y las entidades privadas, bajo los auspicios de Europol y la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Europol y Eurojust deben proseguir su actividad, perseverando en los logros obtenidos en la desarticulación de operaciones con programas de secuestro de archivos, en apoyo de la cooperación policial. Para ello, las fuerzas y cuerpos de seguridad han de maximizar el uso de los mecanismos de cooperación, como el **modelo internacional de respuesta a los programas de secuestro de archivos, de Europol**, y la **Iniciativa internacional de lucha contra los programas de secuestro de archivos (CRI)**[43], y ENISA y Europol deben cooperar para ampliar el repositorio de herramientas de descifrado de las distintas familias de programas de secuestro[44].

Soberanía tecnológica

Habida cuenta de que la ciberseguridad y la soberanía tecnológica están estrechamente interrelacionadas, las dependencias tecnológicas deben afrontarse de forma prioritaria. La Unión debe **liderar el desarrollo y la implantación de nuevas tecnologías**; para ello, la Comisión se esforzará por **impulsar las capacidades en tecnologías estratégicas** como la IA, la conectividad cuántica y avanzada, la nube, el borde y la internet de las cosas[45] a través de sus próximas iniciativas como el Plan de Acción «Continente de IA», la Estrategia cuántica y otros programas[46]. La Comisión seguirá fomentando la aplicación en tiempo oportuno de los últimos **protocolos de internet** acordados internacionalmente, factor esencial para el mantenimiento de una internet escalable y eficiente con un mayor nivel de ciberseguridad. Es preciso adoptar nuevas medidas, como el uso de tecnologías de detección cuántica, y explorar el desarrollo de la capacidad de seguimiento por radiofrecuencia para afrontar los **retos referentes al espectro radioeléctrico**, como los relacionados con la suplantación de las señales de GNSS, las interferencias y los riesgos y dependencias de la cadena de suministro.

La implantación de soluciones de **criptografía postcuántica** (PQC, por sus siglas en inglés) será crucial para salvaguardar las comunicaciones sensibles y los datos en reposo y para proteger las identidades digitales en la nueva era cuántica. Basándose en la Recomendación de 2024 sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Disponible a través del proyecto *No More Ransom* («Ni un secuestro más»), https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_es#step-scope.
[46] Por ejemplo, la Empresa Común de Informática de Alto Rendimiento Europeahttps://eurohpc-ju.europa.eu/index_en o el «Buque insignia cuántico» Página de inicio del «Buque insignia cuántico» |, las redes 3C [COM(2024) 81 final] y el Plan de Acción de la UE sobre la seguridad de los cables [JOIN(2025) 9 final].

criptografía postcuántica[47], la Comisión está trabajando con los Estados miembros para impulsar dicha transición. Con tal fin, los Estados miembros deben localizar los casos de alto riesgo en las entidades críticas y garantizar para ellos un cifrado cuántico seguro lo antes posible y, a más tardar, antes de que finalice 2030. La Comisión también está trabajando con los Estados miembros y la Agencia Espacial Europea (AEE) para desarrollar e implantar la **infraestructura europea de comunicación cuántica (EuroQCI)**[48], basada en la distribución cuántica de clave (QKD, por sus siglas en inglés), como parte de **IRIS²**, el Programa de Conectividad Segura de la UE. En última instancia, ambas iniciativas permitirán a las entidades transmitir datos y almacenar información de forma segura.

Las **tecnologías cuánticas** también desempeñarán un papel clave en las aplicaciones de seguridad: como parte de la Estrategia cuántica, se elaborará una **hoja de ruta para la detección cuántica en las aplicaciones de seguridad**. Siguiendo esa misma línea, la Comisión está trabajando para conseguir que sus sistemas internos críticos para la seguridad, como sus sistemas informáticos clasificados, sean resistentes frente a la computación cuántica.

Un marco de ciberseguridad propicio a las empresas

La revisión del Reglamento de Ciberseguridad que se llevará a cabo próximamente constituye una buena oportunidad para **simplificar la legislación de la UE en materia de ciberseguridad**, en consonancia con lo indicado en la Brújula para la Competitividad. La Comisión colaborará estrechamente con los Estados miembros para garantizar una aplicación rápida, coherente y favorable a las empresas del marco horizontal de ciberseguridad establecido en la Directiva SRI 2, el Reglamento de Ciberresiliencia y el Reglamento de Cibersolidaridad, promoviendo la simplicidad y la coherencia y evitando la fragmentación o la duplicación de las normas en materia de ciberseguridad entre la legislación nacional y la de la UE.

Para permitir un acceso seguro a los servicios en línea y robustecer la seguridad digital en toda la UE, el **Marco Europeo de Identidad Digital** ofrecerá a todos los ciudadanos y residentes de la UE unas carteras de identidad digital fiables antes del final de 2026. La **cartera europea para empresas**, que se introducirá en un futuro próximo, facilitará unas interacciones transfronterizas seguras entre las empresas y las Administraciones públicas. Ambos sistemas son requisitos previos para un funcionamiento seguro y más eficiente de un mercado único apoyado en datos, merced a herramientas como la pasarela digital única, la facturación electrónica, la contratación pública electrónica y el pasaporte digital de productos.

Seguridad en línea

Algunas de las amenazas híbridas más graves que ponen en peligro la seguridad de los europeos y en cuyo punto de mira se halla la esfera democrática de la UE se producen en línea. Esas amenazas incluyen actividades ilegales y contenidos ilícitos en línea, tácticas de manipulación de la información, como su amplificación artificial, propagación de información engañosa y otras actividades de manipulación de la información e injerencia por parte de agentes extranjeros.

La rigurosa aplicación del **Reglamento de Servicios Digitales (RDS)** es fundamental para garantizar un entorno en línea seguro y accesible, con agentes responsables, que sea también resiliente frente a las amenazas híbridas. El RDS obliga a los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño a llevar a cabo evaluaciones de riesgos y a implantar medidas de mitigación de los riesgos sistémicos derivados del diseño, el funcionamiento o la utilización de sus servicios. Estos riesgos pueden

[47] Recomendación sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica | Configurar el futuro digital de Europa.
[48] https://digital-strategy.ec.europa.eu/es/policies/european-quantum-communication-infrastructure-euroqci.

incluir efectos negativos para el discurso cívico y los procesos electorales, así como para la seguridad pública, como la injerencia —por ejemplo, en los procesos electorales—, de agentes estatales extranjeros malintencionados, con graves consecuencias. Es importante velar por que las autoridades competentes de los Estados miembros reciban formación en cuanto al uso de instrumentos jurídicos para eliminar rápidamente los contenidos ilícitos en línea, en particular en lo que respecta a la ciberviolencia de género. El RDS contempla un mecanismo de respuesta a las crisis que puede activarse cuando circunstancias extraordinarias den lugar a una amenaza grave para la seguridad pública o la salud pública en la Unión o en partes significativas de esta. Como complemento de este mecanismo, la Comisión y las autoridades nacionales competentes que han sido designadas coordinadores de servicios digitales han desarrollado también un **marco** voluntario **de respuesta a incidentes en aplicación del RSD**. Los coordinadores de servicios digitales también han adoptado medidas para contribuir a proteger la integridad de las elecciones, por ejemplo organizando mesas redondas y pruebas de resistencia relativas a las elecciones[49]. El RSD, junto con el Reglamento sobre la publicidad política[50], constituye una de las diversas líneas de actuación para la salvaguardia de la democracia y la integridad de los procesos democráticos, que son vulnerables a los ataques de agentes hostiles perpetrados, entre otros medios, con herramientas digitales y a través de las redes sociales.

La aplicación del conjunto de instrumentos contra la **manipulación de información y la injerencia por parte de agentes extranjeros** es otro importante componente que ofrece una ayuda fundamental a escala de la UE. El fomento de la alfabetización digital y mediática y el pensamiento crítico también son factores esenciales para estos esfuerzos[51].

Freno a la instrumentalización de la migración

Con la ayuda y el respaldo decisivos de Bielorrusia, Rusia ha utilizado deliberadamente la migración como arma, facilitando ilegalmente los flujos migratorios hacia las fronteras exteriores de la UE con el objetivo de desestabilizar nuestras sociedades y socavar la unidad de la Unión Europea. Ello no solo pone en peligro la seguridad y la soberanía nacionales de los Estados miembros, sino también la protección y la integridad del espacio Schengen y la seguridad de la Unión en su conjunto. En sus Conclusiones de octubre de 2024, el Consejo Europeo subrayaba que no puede permitirse que ni Rusia, ni Bielorrusia, ni ningún otro país, pisoteen nuestros valores, incluido el derecho de asilo, ni menoscaben nuestras democracias.

Como se indica en la Comunicación de la Comisión de 2024 sobre la instrumentalización de la migración, para ofrecer una respuesta eficaz a esta amenaza, la Unión ha desplegado para con los países de origen y de tránsito —además de ofrecerles un fuerte apoyo político— esfuerzos financieros, operativos y diplomáticos[52]. Esta respuesta implica utilizar el nuevo marco establecido por el Consejo para sancionar a las personas y organizaciones que participen en acciones y políticas como la instrumentalización de la migración por parte de Rusia, imponiéndoles la inmovilización de activos y la prohibición de viajar[53]. La UE seguirá utilizando este marco cuando sea necesario y apoyará a los Estados miembros en la lucha contra esta amenaza.

[49] Conjunto de herramientas del RSD para procesos electorales destinados a los coordinadores de servicios digitales, 2025 https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política, (DO L, 2024/900, 20.3.2024).
[51] Plan de Acción de Educación Digital (2021-2027). Espacio Europeo de Educación.
[52] COM(2024) 570 final.
[53] Reglamento (UE) 2024/2642 del Consejo, de 8 de octubre de 2024, por el que se adoptan medidas restrictivas habida cuenta de las actividades desestabilizadoras de Rusia, ST/8744/2024/INIT (DO L, 2024/2642, 9.10.2024).

Seguridad del transporte

Los puertos marítimos, los aeropuertos y las infraestructuras terrestres son puntos cruciales de entrada y de salida. Desempeñan un papel vital en la economía y la sociedad de la UE y son esenciales para la movilidad militar. Sin embargo, estos intercambiadores y medios de transporte son también objetivos primordiales de las amenazas externas y la actividad delictiva. Los incidentes recientemente registrados, como los casos de vulneración de la seguridad de la carga aérea y los ataques a la infraestructura ferroviaria ponen de relieve la gravedad de estos riesgos. Los **operadores de transporte** pueden ser tanto objetivos como instrumentos para los agentes malintencionados. Las herramientas jurídicas existentes de la UE han mejorado la seguridad de la aviación[54], pero el elevado nivel de amenaza que pesa sobre la aviación civil requiere medios que permitan prever incidentes y consultar rápidamente a los Estados miembros afectados. La Comisión colaborará con los Estados miembros para modificar los actos legislativos de aplicación vigentes en el ámbito de la seguridad de la aviación para poder compartir información clasificada sobre **sucesos relacionados con la seguridad aérea**. Además, estudiará la posibilidad de introducir **medidas regulatorias** para hacer frente a nuevas amenazas, como los **incidentes relacionados con el transporte aéreo de mercancías**, y para reforzar las normas de seguridad aérea. Estas medidas implicarán también el refuerzo de la **legislación sobre seguridad aérea (AVSEC)** para permitir la aplicación de medidas de respuesta inmediata, manteniendo al mismo tiempo la zona de seguridad única en los aeropuertos de la UE.

Al desarrollar la próxima **estrategia portuaria de la UE**, basada en la **Alianza Europea de Puertos**, la Comisión estudiará las formas de seguir reforzando la legislación en materia de seguridad marítima para hacer frente con eficacia a las amenazas emergentes, proteger los puertos y aumentar la seguridad de la cadena de suministro de la UE. Con tal fin, la Comisión velará por la rigurosa aplicación de esta normativa y trabajará para la armonización de las prácticas nacionales y el refuerzo de la comprobación de los antecedentes en los puertos. La Comisión colaborará con los Estados miembros y el sector privado en la ampliación de los protocolos de seguridad establecidos para la carga aérea a fin de garantizar la seguridad de las cadenas de transporte marítimo.

La Autoridad Aduanera de la UE propuesta analizará y evaluará los riesgos a partir de la **información aduanera** relativa a las mercancías que entran en la UE, salen de ella y transitan por su territorio para ayudar a los Estados miembros a prevenir la explotación de las cadenas de suministro internacionales por parte de agentes malintencionados. De conformidad con la Estrategia de Seguridad Marítima de la UE[55], el **pacto europeo de los océanos** desempeñará un papel clave a la hora de intensificar la seguridad en las cuencas marítimas de toda la UE y fuera de ella, fomentando en particular el aumento de las operaciones y los ejercicios marítimos polivalentes.

Resiliencia de las cadenas de suministro

Europa debe procurar estar menos sujeta a las tecnologías de terceros países, so pena de exponerse a dependencias y riesgos para la seguridad. En efecto, la Comisión se propone reducir las dependencias respecto de proveedores extranjeros únicos, mitigar el riesgo que plantean algunos proveedores de alto riesgo en las cadenas de abastecimiento y afianzar las infraestructuras críticas y la capacidad industrial en suelo de la UE, según se especifica en la

[54] Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil (DO L 97 de 9.4.2008, p. 72).
[55] JOIN(2023) 8 final.

Brújula para la Competitividad[56] y en el **Pacto por una Industria Limpia**[57]**.** La Comisión promoverá una **política industrial para la seguridad interior**, colaborando con las industrias de la UE en ámbitos clave (por ejemplo, intercambiadores de transporte o infraestructuras críticas) para producir soluciones de seguridad como equipos de detección, tecnologías biométricas y drones, incorporando las características de seguridad desde el diseño. Al **revisar las normas de contratación pública de la UE**, la Comisión analizará si las consideraciones de seguridad de la Directiva sobre contratación pública en materia de defensa y seguridad de 2009[58] son suficientes para satisfacer las necesidades de resiliencia tanto de las fuerzas y cuerpos de seguridad como de las entidades críticas.

La Comisión asistirá a los Estados miembros en su actividad de **control de la inversión extranjera directa (IED)** y la adquisición de equipos para los centros logísticos, garantizando que las infraestructuras y la tecnología críticas sigan siendo seguras.

Una vez entre en aplicación, el **Reglamento de Emergencia y Resiliencia del Mercado Interior** ayudará a la UE a gestionar las crisis que causen perturbaciones en las cadenas de suministro críticas y en la libre circulación de bienes, servicios y personas. Este Reglamento permitirá una rápida coordinación en caso de crisis y la identificación de los bienes y servicios pertinentes en esas situaciones y proporcionará un conjunto de herramientas para garantizar la disponibilidad de estos. Además, en estrecha cooperación con los Estados miembros, la Comisión propondrá la creación de un **mecanismo interinstitucional de alerta sobre la seguridad de la cadena de transporte y la cadena de suministro** para garantizar el intercambio seguro y oportuno de la información pertinente y necesaria para anticipar y contrarrestar las amenazas.

Por otra parte, con la aplicación del Reglamento de Materias Primas Fundamentales y el Reglamento sobre la Industria de Cero Emisiones Netas, la extensión del uso de los criterios de sostenibilidad, resiliencia y preferencia europea en la contratación pública de la UE fomentará el desarrollo de mercados líderes. El refuerzo de los vínculos comerciales, a través por ejemplo de las asociaciones sobre materias primas y las asociaciones de comercio e inversión limpios, contribuirá a diversificar las cadenas de suministro.

Resiliencia y preparación ante amenazas químicas, biológicas, radiológicas y nucleares

La guerra de agresión rusa contra Ucrania ha incrementado el riesgo de **amenazas químicas, biológicas, radiológicas y nucleares (QBRN)**. Para hacer frente a la adquisición y la instrumentalización potenciales de materiales QBRN, la Comisión apoyará a los Estados miembros y a los países socios mediante formación y ejercicios específicos. Además, la Comisión impulsará las capacidades de preparación y respuesta QBRN, estableciendo un orden de prioridad de las amenazas y financiando la innovación para el desarrollo de contramedidas y capacidades rescEU y el almacenamiento de contramedidas médicas en el marco de un nuevo **Plan de Acción de Preparación y Respuesta QBRN**. Además, la **Estrategia de la UE sobre contramedidas médicas** apoyará la creación de contramedidas médicas, desde la fase de investigación hasta las de fabricación y distribución, con el fin de proteger a la UE de las pandemias y las amenazas QBRN.

[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Directiva 2009/81/CE del Parlamento Europeo y del Consejo sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE (DO L 216 de 20.8.2009).

La experiencia de la pandemia de COVID-19 ha llevado a la UE a reforzar el marco de seguridad sanitaria[59]. La Comisión está designando laboratorios de referencia de la UE en materia de salud pública para reforzar tanto la vigilancia a escala nacional y de la UE como las capacidades de detección rápida. En 2025 se publicará un Plan de la Unión sobre preparación, prevención y respuesta en materia de seguridad sanitaria.

Medidas clave

La Comisión:

- **examinará y revisará el Reglamento sobre la Ciberseguridad en 2025**
- **desarrollará medidas para garantizar un uso ciberseguro de los servicios de computación en la nube**
- **propondrá una estrategia portuaria de la UE en 2025**
- **revisará las normas de contratación pública de la UE en materia de defensa y seguridad en 2026**
- **presentará un nuevo Plan de Acción de Preparación y Respuesta QBRN en 2026**

La Comisión, en cooperación con los Estados miembros:

- **desarrollará e implantará la infraestructura europea de comunicación cuántica (EuroQCI)**
- **garantizará la aplicación efectiva del Reglamento de Servicios Digitales**
- **trabajará para neutralizar la instrumentalización de la migración**
- **establecerá un sistema de notificación de sucesos relativos a la seguridad de la aviación**
- **trabajará en el establecimiento de un mecanismo interinstitucional de alerta sobre la seguridad de la cadena de transporte y la cadena de suministro**

Se insta al Consejo a que:

- **adopte la Recomendación del Consejo sobre el Plan Director de Ciberseguridad de la UE**

Se insta a los Estados miembros a que:

- **transpongan y den plena aplicación a las Directivas REC y SRI 2**

5. Estrechamiento del cerco en torno a la delincuencia grave y organizada

Contribuiremos a erradicar la delincuencia organizada proponiendo normas más estrictas —también en lo que respecta a las investigaciones— para hacer frente a las redes de delincuencia organizada y conseguir que los jóvenes de la UE sean menos vulnerables a la captación con fines delictivos e intensificaremos las medidas para impedir el acceso a instrumentos y activos delictivos.

La delincuencia organizada está explotando un entorno que se halla en constante evolución y proliferando exponencialmente. Se aprovecha de las tecnologías avanzadas, actúa en múltiples países y mantiene sólidas conexiones más allá de las fronteras de la UE. La complejidad y el carácter transnacional de estas amenazas hacen que la coordinación y el apoyo a escala de la UE sean vitales.

[59] En particular mediante el Reglamento (UE) 2022/2371 sobre las amenazas transfronterizas graves para la salud.

Prevención de la delincuencia

La captación de jóvenes para la delincuencia organizada constituye una fuente de preocupación cada vez mayor en la UE. La lucha contra la delincuencia organizada exige abordar sus **causas profundas**, impartiendo educación y ofreciendo alternativas a la delincuencia mediante un enfoque que implique al conjunto de la sociedad. La Comisión favorecerá la integración de las consideraciones de seguridad en las políticas educativas, sociales, de empleo y regionales de la UE. La UE promoverá unas **políticas de prevención de la delincuencia basadas en datos**[60] y adaptadas a los contextos locales.

Para proteger a los destinatarios de los servicios en línea —y, en particular, a los menores— de los abusos sexuales, la trata de personas y la captación en línea con fines delictivos o de extremismo violento, entre otras actividades nocivas, las medidas recogidas en el **Reglamento de servicios digitales** exigen a los proveedores de las plataformas en línea a las que puedan acceder los menores que gestionen los riesgos y actúen contra los contenidos ilícitos, incluida la incitación al odio. La Comisión tiene previsto publicar unas **directrices para la protección de los menores** que ayudarán a los proveedores de plataformas en línea a garantizar a dicho colectivo de usuarios un elevado nivel de privacidad, seguridad y protección en línea. Esas directrices contendrán una serie de recomendaciones dirigidas a todos los servicios digitales que operen en la Unión para aumentar la protección de los menores en línea. En 2025, la Comisión tiene también prevista una solución de la UE para **la comprobación de la edad sin vulnerar la privacidad** que colmará una laguna existente antes de la implantación de la cartera europea de identidad digital a finales de 2026. La Comisión presentará también un plan de acción contra el ciberacoso.

Además, la Comisión seguirá apoyando el diálogo multilateral voluntario con las plataformas en línea y otros agentes pertinentes, a través, en particular, del Foro de la UE sobre Internet, así como la adopción de códigos de conducta específicos en el marco del Reglamento de Servicios Digitales, como el Código de Conducta de 2025 para la Lucha contra la Incitación Ilegal al Odio en Internet. El objetivo es hacer una labor de sensibilización, ofrecer una respuesta común a las amenazas actuales y emergentes y generar y compartir buenas prácticas en cuanto a las medidas de mitigación.

El impacto local de la delincuencia organizada pone de manifiesto la necesidad de adoptar soluciones a escala regional para reducir el atractivo de las actividades ilegales y la vulnerabilidad de quienes pueden ser captados para cometerlas. La Agenda de la UE para las Ciudades abordará los retos en materia de seguridad en el medio urbano, tomando como base la iniciativa Ciudades de la UE contra la Radicalización. La Comisión ofrecerá a los Estados miembros su apoyo para la mejora de la seguridad urbana y regional a través del Fondo Europeo de Desarrollo Regional.

Unas capacidades y unos fundamentos educativos más sólidos pueden sustentar unas sociedades resilientes y cohesionadas. A través de la **Unión de las Competencias** y del **Plan de Acción sobre Integración e Inclusión**, la Unión se esforzará por lograr que las personas sean más resilientes frente a la información errónea y la desinformación, la radicalización y la captación con fines delictivos.

Proteger a los menores de todas las formas de violencia, incluidos los delitos y la violencia física o mental, tanto en línea como fuera de línea, es un objetivo fundamental de la UE. Para atender las necesidades específicas de los grupos especialmente vulnerables, como los menores, cada vez más expuestos a la captación y la radicalización, la seducción y el abuso sexual, el ciberacoso, la desinformación y otras amenazas, la UE desarrollará un **Plan de acción para la**

[60] https://www.eucpn.org/.

protección de los menores frente a la delincuencia en los entornos virtual y real. Este plan fijará un enfoque coherente y coordinado basado en los marcos y herramientas disponibles, incluidos el futuro Centro de la UE para prevenir y combatir el abuso sexual de menores y otros organismos y agencias de la UE, y propondrá soluciones para colmar las posibles lagunas.

Desmantelamiento de las redes delictivas y de la actividad de sus facilitadores

Es preciso intensificar la lucha contra las redes delictivas de alto riesgo, sus cabecillas y sus facilitadores. Aunque recientemente se han cosechado importantes éxitos[61], el carácter obsoleto de las normas y las dispares definiciones de lo que se consideran redes delictivas entorpecen una respuesta eficaz de la justicia penal y la cooperación transfronteriza. La Comisión revisará la legislación obsoleta en esta materia y propondrá una renovación del **marco jurídico contra la delincuencia organizada** para reforzar dicha respuesta.

La acción administrativa puede complementar la acción policial y judicial para obtener resultados más rápidos, como han demostrado la Fiscalía Europea y la Oficina Europea de Lucha contra el Fraude (OLAF) en su actividad de lucha contra el **fraude transfronterizo y los delitos contra los intereses financieros de la UE**. Quienes perciben subvenciones con tácticas fraudulentas se concentran en sectores como las energías renovables, los programas de investigación y la agricultura[62]. La Comisión estudiará formas de coordinar el uso de los instrumentos penales y administrativos, mejorando la cooperación con Europol, Eurojust y la Fiscalía Europea. Además, seguirá propugnando una aplicación más general del **enfoque administrativo** que capacite a las autoridades locales y otras autoridades administrativas para desarticular los movimientos de infiltración con fines delictivos[63].

La UE está trabajando para reforzar su marco jurídico de lucha contra la **corrupción**[64]. El Parlamento Europeo y el Consejo deberían concluir rápidamente las negociaciones sobre el marco actualizado de lucha contra la corrupción propuesto por la Comisión. La Comisión presentará una Estrategia de la UE de Lucha contra la Corrupción para fomentar la integridad y reforzar la coordinación entre todas las autoridades y partes interesadas pertinentes en este ámbito.

Las armas de fuego son un factor esencial para la escalada de actos violentos perpetrados por grupos de delincuencia organizada. La Comisión propondrá normas penales comunes sobre el tráfico ilícito de armas de fuego. El nuevo **Plan de Acción de la UE sobre el Tráfico de Armas de Fuego** se centrará en resguardar el mercado lícito de estas armas y poner freno a las actividades delictivas a partir de una mejor información estratégica y del refuerzo de la cooperación internacional, prestando una especial atención a Ucrania y los Balcanes Occidentales.

Es preciso adoptar medidas respecto de los artículos pirotécnicos comercializados ilegalmente —que se utilizan para la comisión de delitos— con fines preventivos y para mejorar su trazabilidad. La Comisión está evaluando actualmente la Directiva sobre **artículos pirotécnicos** y estudiará también la posibilidad de imponer **sanciones penales al tráfico** de dichos artículos.

[61] Incluidos los recientes casos de la EMPACT.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.
[64] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la corrupción, por la que se sustituyen la Decisión Marco 2003/568/JAI del Consejo y el Convenio relativo a la lucha contra los actos de corrupción en los que estén implicados funcionarios de las Comunidades Europeas o de los Estados miembros de la Unión Europea, y por la que se modifica la Directiva (UE) 2017/1371 del Parlamento Europeo y del Consejo, COM(2023) 234 final, Bruselas, 3.5.2023.

Seguir el rastro del dinero

Seguir el rastro del dinero es una táctica esencial para luchar contra la delincuencia organizada y el terrorismo, pero sigue siendo una tarea muy ardua. Los vínculos entre la delincuencia organizada y los flujos de dinero requieren esfuerzos intensos y combinados para interrumpir el acceso de las redes delictivas a las fuentes de financiación y proteger mejor a las personas, las empresas y los presupuestos públicos.

La UE ha intensificado su actividad en este ámbito mediante las nuevas normas contra el blanqueo de capitales, como la creación de la **Autoridad de Lucha contra el Blanqueo de Capitales (ALBC)** de la UE[65]. La colaboración entre la ALBC, la OLAF, la Fiscalía Europea, Eurojust y Europol es esencial para la eficacia de las investigaciones financieras. La Comisión apoyará la creación de **asociaciones**, tanto las que faciliten la cooperación entre agencias como las que impliquen al sector privado.

La incautación de activos y el decomiso de las ganancias de origen delictivo son fundamentales para desarmar los móviles económicos de la delincuencia organizada. Los Estados miembros deben transponer sin demora y aplicar en toda su extensión las normas más estrictas recientemente adoptadas en materia de **recuperación y decomiso de activos**[66]. La lucha contra los sistemas financieros paralelos que eluden el marco de la UE contra el blanqueo de capitales, entre los que se incluyen los sistemas basados en criptoactivos, requiere también acciones innovadoras, la puesta en común de las mejores prácticas entre los Estados miembros y un mayor apoyo por parte de Europol y Eurojust. La Comisión explorará la viabilidad de un nuevo sistema a escala de la UE para rastrear los beneficios derivados de la delincuencia organizada y la financiación del terrorismo, fomentando también la mayor abundancia y puntualidad de los flujos de información desde las **Unidades de Inteligencia Financiera** hasta las fuerzas y cuerpos de seguridad. La Comisión estudiará la manera de cerrar los resquicios legales, apoyará a los Estados miembros en el desarrollo de capacidades y seguirá trabajando para reforzar la cooperación con los terceros países a través de los cuales los delincuentes llevan a cabo, de forma dolosa, operaciones bancarias sumergidas.

Lucha contra la delincuencia grave

Además del desmantelamiento de las redes delictivas, la lucha contra los delitos graves requiere otras intervenciones específicas. Para reforzar nuestra capacidad de lucha contra el **fraude en línea**, que está acarreando un grave perjuicio financiero[67], la Comisión fomentará medidas preventivas y acciones policiales más eficaces, y colaborará con los Estados miembros y las partes interesadas para apoyar y proteger a las víctimas, ayudándolas, en particular, a recuperar sus fondos. Estos esfuerzos se formalizarán en un **Plan de acción contra el fraude en línea**.

Tomando como punto de partida la Estrategia de la UE 2020-2025 para luchar contra el **abuso sexual de menores**[68], la Comisión ayudará a los colegisladores a ultimar las dos propuestas legislativas[69] dirigidas a prevenir y combatir el abuso sexual de menores en línea y a aumentar la eficacia de la intervención policial contra el abuso y la explotación sexual de menores. Si bien están vigentes normas provisionales hasta abril de 2026, es esencial fijar un marco jurídico permanente, por lo que la Comisión anima a los colegisladores a entablar negociaciones sobre la propuesta de Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual de los menores. Se invita también a los colegisladores a que avancen hacia las

[65] https://www.amla.europa.eu/index_es.
[66] Directiva (UE) 2024/1260 del Parlamento Europeo y del Consejo, de 24 de abril de 2024, sobre recuperación y decomiso de activos (DO L, 2024/1260, 2.5.2024).
[67] Global Anti-Scam Report 2024.
[68] COM(2020) 607 final
[69] COM (2022) 209 final y COM (2024) 60 final.

negociaciones sobre la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores, que establecerá normas mínimas en lo que respecta a la tipificación de las infracciones y las sanciones penales en casos de explotación sexual de los menores.

La mitad de las redes delictivas más peligrosas de la UE están implicadas en el **tráfico** violento **de drogas**. Aunque la UE ha recrudecido en los últimos tiempos su lucha contra este delito[70], en particular gracias a la ampliación del mandato de la Agencia de la UE sobre Drogas, es preciso adoptar nuevas medidas. La Comisión trabajará en estrecha cooperación con los Estados miembros para proponer una nueva **Estrategia de la UE sobre drogas**. También revisará el **marco jurídico aplicable a los precursores de drogas** y propondrá un **Plan de acción de la UE contra el tráfico de drogas**, cuyas rutas y modelos de negocio aspira a desarticular. La **asociación público-privada de la Alianza Europea de Puertos**, dedicada al refuerzo de la protección portuaria, se ampliará para incluir puertos más pequeños e interiores y garantizar el cumplimiento de las normas de seguridad marítima. Reconocedora de las graves repercusiones locales del tráfico de drogas, la Comisión seguirá apoyando una política equilibrada, basada en datos contrastados y multidisciplinaria de la que forme parte la preparación para el surgimiento de flujos repentinos de drogas, especialmente opioides sintéticos.

Para luchar contra la explotación de las personas, la UE ha adoptado nuevas normas[71] e introducirá una **Estrategia renovada de lucha contra la trata de seres humanos** (2026-2030) que abarque todas las fases —desde la prevención hasta el procesamiento— y se centre en el apoyo a las víctimas, a escala tanto de la UE como internacional.

En la lucha contra el **tráfico ilícito de migrantes** —también en línea—, la Comisión encabezará los esfuerzos con nuestros socios principales a través de la nueva Alianza Mundial contra el Tráfico Ilícito de Migrantes, en cooperación con Europol, Eurojust y Frontex. Las propuestas de la Comisión sobre la lucha contra este tráfico ilícito[72] deben adoptarse y aplicarse sin demora. Además, tras la adopción del **conjunto de instrumentos aplicable a los transportistas**[73], la Comisión ha intensificado sus contactos con las autoridades y operadores extranjeros, y seguirá colaborando con el sector de la aviación y las organizaciones de aviación civil[74] en la labor de sensibilización sobre el tráfico ilícito de migrantes por vía aérea[75].

Los **delitos medioambientales** suponen una amenaza para el medio ambiente, la salud pública y, a largo plazo, las economías. La Comisión asistirá a los Estados miembros en la aplicación de la Directiva sobre delitos contra el medio ambiente[76] y reforzará las redes operativas y las acciones en este ámbito[77]. El riguroso control del cumplimiento de las normas es esencial. Además, el Convenio del Consejo de Europa sobre la protección del medio ambiente mediante

[70] COM(2023) 641 final.
[71] Directiva (UE) 2024/1712, de 13 de junio de 2024, por la que se modifica la Directiva 2011/36/UE relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas (DO L, 2024/1712, 24.6.2024).
[72] COM(2023) 755 final y COM(2023) 754 final.
[73] Conjunto de instrumentos para abordar el uso de medios de transporte comerciales para facilitar la migración irregular a la UE.
[74] Incluida la Organización de Aviación Civil Internacional (OACI).
[75] La Comisión promoverá asimismo la finalización del Reglamento relativo a las medidas contra los operadores de transporte que participen en la trata de personas o el tráfico ilícito de migrantes, o los faciliten, COM(2021) 753 final.
[76] Directiva (UE) 2024/1203 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, relativa a la protección del medio ambiente mediante el Derecho Penal (DO L 2024/1203/CE, 30.4.2024).
[77] Red europea para la aplicación y el cumplimiento de la legislación en materia de medio ambiente (IMPEL), Red Europea de Fiscales para el Medio Ambiente (ENPE), EnviCrimeNet y Foro de Jueces de la UE para el Medio Ambiente (EUFJE).

el Derecho penal[78], recientemente adoptado, contribuirá a garantizar la adopción de medidas contundentes y homogéneas para luchar contra la delincuencia medioambiental, tanto en Europa como fuera de ella.

Respuesta de la justicia penal

La delincuencia y el terrorismo pueden afectarnos a todos, motivo por el que es primordial defender y salvaguardar los derechos de las **víctimas** para mitigar los daños y aumentar la seguridad general y la confianza en las autoridades. Tomando como base la Directiva sobre los derechos de las víctimas, la Comisión introducirá una nueva **Estrategia de la UE sobre los Derechos de las Víctimas**.

Los sistemas de justicia penal de la UE necesitan herramientas eficaces para hacer frente a las amenazas emergentes. Para desarrollarlas, la Comisión ha creado un **Foro de alto nivel sobre el futuro de la justicia penal de la UE** que reúne a los Estados miembros, el Parlamento Europeo, las agencias y organismos de la UE y otras partes interesadas. Su objetivo es debatir sobre las maneras de garantizar que nuestros sistemas de justicia penal sigan siendo eficaces, justos y resilientes en un contexto de retos en constante evolución, reforzando al mismo tiempo la cooperación judicial y aumentando la confianza mutua, a través, entre otros medios, de la digitalización[79].

Medidas clave

La Comisión:

- **presentará una propuesta legislativa para modernizar las normas aplicables a la delincuencia organizada en 2026**
- **presentará una propuesta legislativa para revisar el marco jurídico sobre precursores de drogas en 2025**
- **presentará una propuesta de normas penales comunes sobre el tráfico ilícito de armas de fuego en 2025**
- **evaluará la necesidad de revisar las Directivas sobre productos pirotécnicos y explosivos civiles**
- **estudiará la necesidad de seguir reforzando la orden europea de investigación y la orden de detención europea**
- **presentará una nueva estrategia de la UE contra la trata de seres humanos en 2026**
- **presentará una nueva estrategia de la UE sobre los derechos de las víctimas en 2026**
- **presentará un Plan de acción de la UE para la protección de los menores frente a la delincuencia antes del final de 2027;**
- **presentará un Plan de acción de la UE contra el tráfico de drogas en 2025**
- **presentará un Plan de acción de la UE contra el tráfico de armas de fuego en 2026**
- **ampliará a partir de 2025, en fases sucesivas, la Alianza Europea de Puertos**
- **adoptará directrices relativas al Reglamento de Servicios Digitales en lo que respecta a la protección de los menores en 2026**
- **presentará un plan de acción de la UE contra el ciberacoso en 2026**

Se insta a los Estados miembros a que:

[78] Comité de expertos sobre protección del medio ambiente a través del Derecho Penal (PC-ENV) — Comité Europeo para los Problemas Criminales.

[79] En particular, a través del establecimiento del sistema de comunicación para la justicia digital mediante el intercambio electrónico de datos (e-CODEX) y del Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (ECRIS-TCN).

- **transpongan plenamente y apliquen en toda su extensión las nuevas normas en materia de recuperación y decomiso de activos antes de que termine 2026**
- **apliquen el enfoque administrativo a la lucha contra la infiltración delictiva**
- **establezcan asociaciones público-privadas contra el blanqueo de capitales**
- **transpongan y den plena aplicación a la Directiva para prevenir y luchar contra la violencia dirigida contra las mujeres y la violencia doméstica**

Se insta al Parlamento Europeo y al Consejo a que:

- **avancen hacia las negociaciones sobre el Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual de menores y la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores**
- **concluyan las negociaciones sobre la Directiva relativa a la lucha contra la corrupción**

6. Lucha contra el terrorismo y el extremismo violento

Introduciremos un programa integral de lucha contra el terrorismo para prevenir la radicalización, proteger los espacios en línea y públicos, agilizar los canales de financiación y responder a los atentados cuando se produzcan.

El nivel de amenaza terrorista en la UE sigue siendo elevado. Está estrechamente relacionado con los efectos indirectos de los acontecimientos geopolíticos, las nuevas tecnologías y los nuevos medios de financiación del terrorismo. Hemos de garantizar que la UE esté adecuadamente equipada para anticipar las amenazas, prevenir la radicalización (tanto en línea como fuera de línea), proteger a los ciudadanos y los espacios públicos de los atentados y responder eficazmente a estos cuando se produzcan. En 2025 se presentará una nueva **Agenda de la UE para prevenir y combatir el terrorismo y el extremismo violento** en la que se expondrá la acción futura de la UE. Conforme a esa nueva Agenda, la UE y los Balcanes Occidentales firmarán el nuevo **Plan de Acción Conjunto** para prevenir y combatir el terrorismo y el extremismo violento en 2025.

Prevención de la radicalización y protección de las personas en el entorno digital

Al igual que la lucha contra la delincuencia organizada, la lucha contra el terrorismo y el extremismo violento empieza por **abordar sus causas profundas**. El **Centro de conocimientos de la UE en materia de prevención de la radicalización** intensificará su apoyo a los profesionales y los responsables de las políticas mediante un nuevo y **completo conjunto de herramientas de prevención** que facilite la detección temprana del fenómeno y las intervenciones centradas en las personas vulnerables, en particular los menores. A menudo, la radicalización se produce en las cárceles, situación para la que la Comisión formulará nuevas recomendaciones que ayuden a los Estados miembros a afrontarla.

Los terroristas y extremistas violentos utilizan plataformas en línea para difundir contenidos terroristas y nocivos, recabar fondos y captar adeptos. La radicalización en línea de los usuarios vulnerables, en particular los menores, está alcanzando un ritmo alarmante. El **Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea** ha sido fundamental al

permitir la rápida retirada del material más abyecto y peligroso[80]. La Comisión, que está evaluando actualmente su funcionamiento, estudiará la mejor manera de reforzar este marco.

El **Protocolo de Crisis de la UE** para una respuesta conjunta y rápida de las fuerzas y cuerpos de seguridad y la industria tecnológica en caso de atentados terroristas se modificará para garantizar la escalabilidad y la flexibilidad a la hora de reaccionar frente a la expansión de la dimensión digital de los ataques terroristas. El Foro de la UE sobre Internet seguirá siendo la principal vía de cooperación voluntaria con la industria tecnológica para luchar contra los contenidos terroristas y nocivos en línea. Además, la Comisión está participando en iniciativas internacionales como la Fundación Christchurch Call y el Foro Mundial de Internet para la Lucha contra el Terrorismo (GIFCT, por sus siglas en inglés).

Lucha contra la financiación del terrorismo

Los terroristas financian sus actividades con campañas de financiación participativa, criptoactivos, neobancos o plataformas de pago en línea. Las fuerzas y cuerpos de seguridad deben ser capaces de detectar e investigar esos flujos financieros, para lo que requieren medios, herramientas y conocimientos especializados. La **red de investigadores financieros para la lucha contra el terrorismo** desempeña un papel fundamental. La Comisión estudiará la creación de un nuevo **sistema de rastreo a escala de la UE de la financiación del terrorismo** que cubra las transacciones dentro de la UE y las operaciones SEPA, las transferencias de criptoactivos y los pagos en línea y por cable, complementando el Acuerdo relativo al Programa de Seguimiento de la Financiación del Terrorismo (TFTP, por sus siglas en inglés) entre la UE y los EE.UU.

Es necesario **proteger** el presupuesto de la UE frente a todo **uso indebido dirigido a alentar posiciones radicales y extremistas** en los Estados miembros. El **Reglamento Financiero** revisado incluye ahora entre los motivos de exclusión de la financiación de la UE las condenas por «incitación a la discriminación, el odio o la violencia». La Comisión seguirá analizando la mejor manera de utilizar su conjunto de herramientas para la obtención de los mejores resultados, también en lo que se refiere a la selección de los posibles beneficiarios. La protección del presupuesto de la UE depende también de una estrecha cooperación y de un intenso intercambio de información con las autoridades nacionales, las agencias y los organismos de la UE.

Protección frente a los atentados

Junto a la inversión en la prevención de la radicalización, un importante componente de la protección de los ciudadanos es la restricción de los medios que permiten a terroristas y delincuentes perpetrar atentados y ataques. Es necesario actuar en relación tanto con los instrumentos que utilizan los terroristas como con la protección de los objetivos en riesgo de sufrir atentados.

Además de adoptar medidas relativas a las armas de fuego, la Comisión **revisará las normas** sobre **precursores de explosivos** para incluir en su ámbito de aplicación las sustancias químicas de alto riesgo. Los **espacios públicos** siguen siendo los objetivos más comunes de los atentados terroristas, especialmente los cometidos por «lobos solitarios». A fin de proteger a los ciudadanos frente a cualquier daño, se reforzará el **programa europeo de asesoramiento en materia de seguridad preventiva** de la UE para llevar a cabo evaluaciones de la vulnerabilidad de los espacios públicos, las infraestructuras críticas y los eventos de alto riesgo, a petición de los Estados miembros y con cargo al presupuesto de la UE destinado al Fondo de Seguridad

[80] A 31 de diciembre de 2024 se habían dictado 1 426 órdenes de retirada o de bloqueo del acceso a contenidos terroristas, la gran mayoría de los cuales eran contenidos terroristas yihadistas, pero también contenidos terroristas de derechas.

Interior. La UE procurará aumentar los fondos disponibles para la protección del espacio público. La Comisión presta asistencia a las autoridades de los Estados miembros y a los operadores privados mediante directrices y herramientas específicas, como el Centro de conocimientos sobre la protección de los espacios públicos[81], espacios para la mejora de cuya protección ya se han facilitado 70 millones EUR desde 2020.

La Comisión estudiará también la posibilidad de introducir requisitos para que las distintas organizaciones consideren o empleen medidas de seguridad en los lugares de acceso público, para lo que colaborará con las autoridades locales y los socios privados.

Dada la manifiesta vulnerabilidad de sus destinatarios, **la Estrategia de la UE de lucha contra el antisemitismo y apoyo a la vida judía (2021-2030)** seguirá guiando las acciones de la Comisión para proteger a la comunidad judía. Asimismo, la Comisión velará por la existencia de las herramientas adecuadas para secundar a los Estados miembros en la lucha contra **el odio antimusulmán**.

El uso de **drones** con fines de espionaje y comisión de atentados plantea un reto cada vez mayor para la seguridad. La Comisión desarrollará una **metodología armonizada de ensayo de los sistemas de defensa contra los drones**, creará un **centro de excelencia de defensa contra los drones** y evaluará la necesidad de armonizar las legislaciones y los procedimientos correspondientes de los Estados miembros[82].

Combatientes terroristas extranjeros

Para identificar a los combatientes terroristas extranjeros que regresan a la UE o que atraviesan sus fronteras exteriores, se necesitan datos sobre los individuos que suponen una amenaza terrorista. A tal fin, la Comisión, junto con Europol, reforzará su **cooperación con los terceros países clave para obtener datos biográficos y biométricos de las personas que puedan suponer una amenaza terrorista** —entre las que se encuentran los combatientes terroristas extranjeros—, datos que posteriormente podrán introducirse en el Sistema de Información de Schengen, sin perjuicio de los marcos jurídicos aplicables nacionales y de la UE. Es fundamental para ello que los Estados miembros hagan uso de todas las herramientas existentes, como la introducción de toda la información pertinente en el **SIS**, la mejora de los controles biométricos y la realización sistemática y obligatoria de controles a todas las personas en las fronteras exteriores de la UE[83]. Además, los **indicadores comunes de riesgo** desarrollados por Frontex seguirán ayudando a las autoridades de vigilancia de las fronteras de los Estados miembros a detectar y evaluar el riesgo de desplazamientos sospechosos de posibles combatientes terroristas extranjeros.

Además, para garantizar que los Estados miembros mantengan el acceso a las **pruebas** recogidas en el **campo de batalla** por el Equipo de Investigaciones de las Naciones Unidas para Promover la Rendición de Cuentas por los Crímenes del Dáesh/Estado Islámico (UNITAD, por sus siglas en inglés) con vistas al enjuiciamiento de combatientes terroristas extranjeros, la Comisión, junto con Eurojust, valorará la posibilidad de almacenar estas pruebas en la base de datos de pruebas de crímenes internacionales fundamentales de Eurojust. Además, el nuevo **Registro Judicial Antiterrorista** europeo seguirá facilitando a los órganos jurisdiccionales de los Estados miembros la rápida detección de conexiones transfronterizas en casos de terrorismo.

Medidas clave

[81] Centro de conocimientos sobre la protección de los espacios públicos.
[82] Como complemento de las medidas clave descritas en la Comunicación de 2023 sobre la lucha contra las posibles amenazas que plantean los clones, COM(2023) 659 final.
[83] En estricto cumplimiento del Código de fronteras Schengen y del Reglamento de triaje.

La Comisión:

- **adoptará una nueva Agenda de la UE para prevenir y combatir el terrorismo y el extremismo violento en 2025**
- **firmará con los Balcanes Occidentales un nuevo Plan de Acción Conjunto para prevenir y combatir el terrorismo y el extremismo violento en 2025**
- **desarrollará un nuevo conjunto completo de herramientas de prevención con el Centro de conocimientos de la UE**
- **evaluará la aplicación del Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea en 2026**
- **modificará el Protocolo de Crisis de la UE en 2025**
- **presentará una propuesta legislativa de revisión del Reglamento sobre la comercialización y la utilización de precursores de explosivos en 2026**
- **explorará la viabilidad de un nuevo sistema de rastreo de las fuentes de financiación del terrorismo a escala de la UE**

Se insta a los Estados miembros a que:

- **mejoren los controles biométricos y lleven a cabo controles obligatorios y sistemáticos en las fronteras exteriores de la UE**
- **hagan pleno uso del Registro Judicial Antiterrorista europeo**

7. La UE como gran potencia mundial en materia de seguridad

Para reforzar la seguridad de la UE, impulsaremos la cooperación operativa a través de asociaciones con regiones clave como nuestros socios de la ampliación y la vecindad, América Latina y la región mediterránea. Los intereses de seguridad de la UE se tendrán en cuenta en la cooperación internacional, para lo que se recurrirá en particular a las herramientas e instrumentos de la UE.

En los últimos años, han quedado patentes los vínculos intrínsecos entre la seguridad exterior y la seguridad interior de la UE. La guerra de agresión rusa contra Ucrania, el conflicto en Gaza, la situación en Siria y otros conflictos emergentes en todo el mundo han tenido graves efectos indirectos sobre la seguridad interior de la UE. Para contrarrestar las repercusiones de la inestabilidad mundial en su seguridad interior, **la UE debe defender activamente sus intereses en materia de seguridad** afrontando las amenazas externas, desarticulando las rutas de tráfico y salvaguardando los corredores de interés estratégico, como las rutas comerciales. Al mismo tiempo, la UE seguirá siendo un fuerte aliado de los países socios, junto a los que trabajará para mejorar la seguridad mundial y reforzar la resiliencia mutua frente a las amenazas.

En los últimos años, la UE ha dado importantes pasos para mejorar su cooperación en materia de seguridad. Ha establecido acuerdos operativos de cooperación policial y judicial, así como otros tipos de acuerdos con los países socios. Está persiguiendo activamente la celebración de nuevos acuerdos internacionales, de conformidad con las directrices de negociación del Consejo, y la ejecución de iniciativas de desarrollo de capacidades, facilitadas por las agencias y organismos de la UE. El instrumento Europa Global-IVDCI es también crucial para reforzar la seguridad con los países socios.

El **orden multilateral basado en normas** es una piedra angular que sustenta la seguridad mundial. Los diálogos sobre seguridad, incluidos los temáticos, son vitales para intensificar estos esfuerzos. La aplicación de la **Brújula Estratégica para la Seguridad y la Defensa**, así como los marcos de cooperación bilateral y multilateral, como los acuerdos de estabilización y asociación y los acuerdos de asociación, y las colaboraciones con organizaciones como las

Naciones Unidas y la OTAN, son cruciales para el desarrollo de soluciones de seguridad eficaces. La UE seguirá desempeñando su papel en los foros multilaterales[84] e intensificará su cooperación con las organizaciones y marcos internacionales y regionales pertinentes, como la OTAN, las Naciones Unidas, el Consejo de Europa, Interpol, el G7, la OSCE y la sociedad civil.

Cooperación regional

Mantener el apoyo inquebrantable de la UE a **Ucrania** es una prioridad y reforzar la seguridad y la resiliencia de los **países de la ampliación de la UE** es un imperativo político y geoestratégico. El apuntalamiento de la seguridad de la UE debe ir acompañado de una **integración acelerada de los países candidatos** en la **arquitectura de seguridad de la UE**, en paralelo a la consolidación de la cooperación regional. La Comisión utilizará la política de ampliación de la UE para sustentar las capacidades de los países candidatos y candidatos potenciales a la adhesión a la UE para responder a las amenazas, para ampliar la cooperación operativa y el intercambio de información y para garantizar la armonización con los principios, la legislación y las herramientas de la UE. El Instrumento de Ayuda Preadhesión (IAP III) y los Mecanismos para Ucrania, para Moldavia y para los Balcanes Occidentales son cruciales para el refuerzo de la seguridad tanto en los países candidatos como en los candidatos potenciales.

La UE proseguirá, además, el proceso de integración de los **socios de la vecindad** en la arquitectura de seguridad de la UE. A través del **Nuevo Pacto por el Mediterráneo** y del **Enfoque Estratégico para el Mar Negro**, que se presentará en breve, la Unión procurará seguir desarrollando la cooperación regional y las asociaciones estratégicas integrales bilaterales con una dimensión de seguridad, manteniendo para ello de forma periódica, según proceda, diálogos de alto nivel. Se reforzará la cooperación operativa con África del Norte, **Oriente Próximo y los países del Golfo**, especialmente en materia de lucha contra el terrorismo, el blanqueo de capitales y el tráfico de armas de fuego y contra la producción y el tráfico de drogas, en particular el captagón.

Con el fin de detener el auge de la actividad terrorista y delictiva y sus posibles efectos indirectos en el **África subsahariana, en particular en el Sahel, el Cuerno de África y África Occidental**, la UE reforzará su apoyo a la Unión Africana, a las comunidades económicas regionales y a los países de la región. En aplicación de la Estrategia de Seguridad Marítima de la UE[85], la UE reforzará la cooperación en el **golfo de Guinea, el mar Rojo y el océano Índico** para hacer frente al tráfico y la piratería, apoyando la cooperación en el seno de África y la cooperación regional, con la ayuda de las presencias marítimas coordinadas (PMC) de la UE y del Centro de Análisis y Operaciones Marítimas en Materia de Drogas (MAOC-N, por sus siglas en inglés).

La UE reforzará la cooperación operativa con **América Latina y el Caribe** para desarticular las redes delictivas de alto riesgo y enjuiciar a sus miembros y para interceptar las actividades ilícitas y las rutas de tráfico, impulsando para ello los marcos de cooperación como el Comité Latinoamericano de Seguridad Interior (CLASI) y el Mecanismo de Coordinación y Cooperación en materia de Drogas entre la Unión Europea y la Comunidad de Estados Latinoamericanos y Caribeños (UE-CELAC, por sus siglas en inglés). Entre las prioridades figurarán la resiliencia de los centros logísticos, las asociaciones y los enfoques de seguimiento del rastro del dinero. La UE seguirá apoyando el desarrollo de la Comunidad de Policías de América (AMERIPOL), de forma que este organismo se convierta en el equivalente regional

[84] Foro Mundial contra el Terrorismo, Coalición Mundial contra el Dáesh, Foro Mundial de Internet contra el Terrorismo (GIFCT, por sus siglas en inglés), Fundación Christchurch Call y Coalición Mundial para Hacer Frente a las Amenazas de las Drogas Sintéticas.
[85] JOIN(2023) 8 final.

de Europol, y reforzando la cooperación judicial entre los Estados miembros y la región. La UE colaborará también con **Asia Meridional y Central** en relación con los retos comunes en materia de seguridad relacionados con el terrorismo, el tráfico de mercancías ilícitas (incluidas las drogas), la trata de seres humanos y el tráfico ilícito de migrantes.

Además, la UE ofrecerá su apoyo a los marcos de cooperación regional en terceros países para seguir ayudándoles a detener el tráfico ilícito en origen, en aplicación del principio de responsabilidad compartida a lo largo de toda la cadena de suministro delictiva. Por otro lado, la UE pondrá de su parte para aumentar la seguridad de los centros logísticos en el extranjero, encargándose de la coordinación de las **inspecciones conjuntas en puertos de terceros países**.

Cooperación operativa

Global Gateway propiciará la ejecución de proyectos para infraestructuras sostenibles y de alta calidad en los sectores digital, climático y energético, del transporte, de la salud, de la educación y de la investigación. De ahora en adelante, la Comisión integrará las consideraciones de seguridad, siempre que proceda, en las futuras inversiones de Global Gateway, que incluirán iniciativas críticas para la autonomía estratégica de la UE y sus países socios, como los proyectos de infraestructura que incorporen evaluaciones de seguridad y medidas de mitigación de riesgos.

La Comisión trabajará para la celebración de nuevos **acuerdos entre la UE y terceros países**, en particular países latinoamericanos, **en materia de cooperación con Europol y Eurojust**.

Por otra parte, la participación proactiva de los países no pertenecientes a la UE en la **EMPACT** es uno de los medios más eficaces para reforzar la cooperación operativa. La UE seguirá impulsando la implicación en este marco de terceros países, en particular los países de los Balcanes Occidentales, la vecindad oriental, el África subsahariana, África del Norte, Oriente Próximo, América Latina y el Caribe. Otra herramienta para intensificar la cooperación con terceros países en la lucha contra la delincuencia son los grupos de trabajo operativos entre Estados miembros coordinados por Europol, en los que pueden participar terceros países. La Comisión pretende, además, concluir las negociaciones relativas al acuerdo internacional entre la **UE e Interpol**[86], garantizando con él un enfoque más homogéneo de las amenazas a la seguridad mundial y la lucha contra los delitos transnacionales.

La **Unión debe estar presente sobre el terreno, aplicando así el enfoque de «Equipo Europa»**. El personal especializado de la Unión y de los Estados miembros desempeña un papel fundamental a la hora de garantizar que la acción exterior de la Unión esté adecuadamente informada y coordinada y sea reactiva. Para elevar este enfoque a una dimensión superior, la Comisión, con el apoyo del Alto Representante para Asuntos Exteriores y Política de Seguridad, reforzará las **redes de enlace** y facilitará el despliegue de **funcionarios regionales de enlace de Europol y Eurojust**, en función de las necesidades operativas de los Estados miembros.

La UE procurará establecer una cooperación policial y judicial más estrecha y fomentará el intercambio de información en tiempo real y las operaciones conjuntas a través de **equipos conjuntos de investigación** en terceros países, con el apoyo de Europol y Eurojust. Además, ayudará a los Estados miembros a crear **centros de fusión conjuntos** que reúnan a expertos y autoridades policiales locales en terceros países estratégicos.

Herramientas de la Política Exterior y de Seguridad Común (PESC)

Las misiones de la Política Común de Seguridad y Defensa (PCSD) también se aprovecharán al máximo para detectar y afrontar mejor las amenazas externas a la seguridad

[86] Decisión (UE) 2021/1312 del Consejo, de 19 de julio de 2021, y Decisión (UE) 2021/1313 del Consejo, de 19 de julio de 2021.

interior de la UE, en consonancia con los mandatos que les haya conferido el Consejo. Para desarrollar las capacidades de terceros países, el Alto Representante para Asuntos Exteriores y Política de Seguridad y la Comisión apoyarán las acciones de la PCSD con instrumentos específicos de financiación y explorarán todas las vías de financiación adecuadas.

Las medidas restrictivas de la UE son un instrumento de la PESC que goza de un gran arraigo y se utiliza también en la lucha contra el terrorismo. A partir de las sugerencias del Alto Representante para Asuntos Exteriores y Política de Seguridad, de los Estados miembros o de la Comisión, el Consejo podría estudiar la forma de conseguir que las actuales medidas restrictivas autónomas de la UE (lista de terroristas de la UE) sean más eficaces, operativas y ágiles. Además, podría considerarse la posibilidad de aplicar nuevas medidas restrictivas contra las redes delictivas, en consonancia con los objetivos de la PESC.

Política de visados e intercambio de información

La política de visados de la UE es una herramienta clave para cooperar con terceros países y proteger nuestras fronteras a través del control de la entrada en la UE y el establecimiento de las condiciones para ello. La Comisión integrará plenamente las **consideraciones de seguridad en la política de visados de la UE** mediante la Estrategia de política de visados de la UE que se presentará próximamente. Por otra parte, trabajará junto con los colegisladores para adoptar la propuesta de revisión y racionalización del mecanismo de suspensión de visados, en particular en relación con los casos específicos de uso indebido del régimen de exención de visado[87]. Se alentará a los terceros países a que notifiquen información sobre las personas que puedan plantear amenazas para la seguridad con el fin de introducirla en los sistemas de información y las bases de datos de la UE.

A fin de lograr la coordinación de las políticas y los esfuerzos realizados en fases anteriores, facilitando con ello una cooperación más eficiente, rápida y fluida, la Comisión trabajará para establecer **mecanismos de flujo de datos** y explorará formas de **mejorar el intercambio de información** con fines policiales y de gestión de las fronteras con terceros países de confianza, sin desproteger los derechos fundamentales ni incumplir las normas de protección de datos.

Medidas clave

La Comisión:

- **celebrará acuerdos internacionales entre la UE y terceros países prioritarios en materia de cooperación con Europol y Eurojust**
- **fomentará la participación de los países socios en la EMPACT para luchar contra la delincuencia organizada y el terrorismo**
- **apoyará a las agencias y organismos de la UE en el establecimiento y el refuerzo de los acuerdos de trabajo con los países socios**
- **reflejará en mayor medida las consideraciones de seguridad en la política de visados de la UE a través de la próxima Estrategia de visados**
- **reforzará el intercambio de información con terceros países de confianza con fines policiales y de gestión de las fronteras**

La Comisión, en cooperación con el Alto Representante para Asuntos Exteriores:

- **hará pleno uso de las misiones civiles de la política común de seguridad y defensa (PCSD)**
- **coordinará las inspecciones conjuntas en puertos de terceros países de aquí a 2027**

[87] COM(2023) 642.

La Comisión, en cooperación con el Alto Representante para Asuntos Exteriores y los Estados miembros:

- **reforzará las redes de enlace y cooperación siguiendo un enfoque de «Equipo Europa»**
- **creará equipos operativos conjuntos y centros de fusión en terceros países a partir de 2025**

Se insta al Parlamento Europeo y al Consejo a que:

- **concluyan las negociaciones sobre la revisión del mecanismo de suspensión de visados**

8. Conclusión

En un mundo caracterizado por la incertidumbre, es preciso reforzar la capacidad de la Unión para anticipar las amenazas a la seguridad, prevenirlas y responder a ellas.

No basta con reaccionar ante las crisis únicamente cuando se producen. Tenemos que tomar una mayor conciencia de la situación, formándonos una visión completa de las amenazas a medida que estas van evolucionando. Y, además, tenemos que garantizar que nuestras herramientas y capacidades estén a la altura de esta tarea.

El conjunto integral de medidas que se detalla en la presente Estrategia contribuirá a crear una Unión más fuerte en el mundo: una Unión capaz de anticipar, planificar y cubrir sus propias necesidades de seguridad, capaz de responder eficazmente a las amenazas a su seguridad interior y de exigir responsabilidades a sus autores, y capaz de proteger a sus sociedades y democracias abiertas, libres y prósperas.

Es preciso operar un cambio de mentalidad en lo que se refiere a la seguridad interior. Trabajaremos para contribuir a fomentar una nueva cultura de la seguridad de la UE, en la que las consideraciones de seguridad se integren en la totalidad de nuestra legislación, nuestras políticas y nuestros programas, desde su concepción hasta su aplicación. Y en la que la colaboración entre los distintos ámbitos de actuación nos permita abrir nuevas vías.

No es tarea de una sola institución, un solo gobierno o un solo agente. Se trata del esfuerzo común de Europa.