Consejo de la Unión Europea

Bruselas, 18 de octubre de 2023
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	18 de octubre de 2023
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2023) 665 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO relativa al sexto informe de situación sobre la aplicación de la Estrategia de la UE para una Unión de la Seguridad

Adjunto se remite a las delegaciones el documento COM(2023) 665 final.

Adj.: COM(2023) 665 final

COMISIÓN
EUROPEA

Bruselas, 18.10.2023
COM(2023) 665 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

relativa al sexto informe de situación sobre la aplicación de la Estrategia de la UE para una Unión de la Seguridad

I. Introducción

Hace tres años, la Comisión adoptó la Estrategia para una Unión de la Seguridad para el período 2020-2025[1], en la que se definen las principales prioridades de la Unión en el ámbito de la seguridad. Desde entonces, hemos realizado importantes avances en los cuatro pilares de la Estrategia y hemos elaborado legislación emblemática en todos los ámbitos, desde la protección de las entidades críticas hasta la mejora de la ciberresiliencia. Sin embargo, el panorama de las amenazas para la seguridad en Europa y nuestros países vecinos sigue evolucionando. Los atentados terroristas perpetrados en una escuela en Francia y en las calles de Bruselas en los últimos días son un crudo recordatorio de la necesidad urgente de seguir adaptando y reforzando nuestra arquitectura de seguridad. El peligro que plantean los ciberataques sigue en aumento y se está intensificando debido a que los agentes malintencionados toman partido en los conflictos en curso. Las amenazas híbridas, como la desinformación, siguen multiplicándose. Europol ha señalado a la guerra de agresión de Rusia contra Ucrania como la causa de un considerable repunte de los ciberataques contra objetivos de la Unión, la mayoría motivados y coordinados por grupos de piratas informáticos prorrusos[2]. Esto se ha traducido en el bloqueo del acceso a internet y en la interrupción de servicios estratégicos como las redes energéticas[3].

La Estrategia para una Unión de la Seguridad se concibió con el fin de preparar a la Unión de manera que pueda resistir mejor ante un panorama de amenazas cambiantes. Nos hemos enfrentado a las crisis planteadas por la pandemia y la guerra, y los acontecimientos han puesto de manifiesto la importancia del enfoque adoptado en la Estrategia: nuestro empeño por cohesionar el ecosistema de seguridad de la Unión y derribar los muros entre las dimensiones cibernética y física de la seguridad, lo que implica combatir la delincuencia organizada y el terrorismo, así como la radicalización.

No obstante, una actitud vigilante exige que sigamos investigando qué nos falta en nuestros esfuerzos por mantener la seguridad de nuestros ciudadanos. La Estrategia se centra en ámbitos prioritarios en los que la Unión puede aportar valor añadido para ayudar a los Estados miembros a promover la seguridad de todas las personas que viven en Europa. Desde su adopción, se han abordado todas las medidas que recoge y se han incorporado otras nuevas para responder a los retos actuales en materia de seguridad.

La Comisión ha presentado treinta y seis iniciativas legislativas en total en el marco de la Estrategia para una Unión de la Seguridad. En más de la mitad de estas propuestas, las negociaciones interinstitucionales ya han concluido y han dado lugar a una nueva legislación sólida, tal como se describe en el cuadro que figura en el anexo. Sin embargo, el Parlamento Europeo y el Consejo siguen negociando varias iniciativas clave propuestas por la Comisión. Dado que la actual legislatura concluye con las elecciones europeas de junio de 2024, es necesario trabajar con celeridad para resolver estos expedientes pendientes, de modo que los ciudadanos puedan beneficiarse plenamente de la Unión de la Seguridad. Por lo tanto, este sexto

---

1 COM(2020) 605.

2 Ataques distribuidos de denegación de servicio (DDoS): véase el informe Spotlight de Europol titulado *Cyber-attacts: the apex of crime-as-a-service* [«Ciberataques: el culmen del delito como servicio», documento en inglés], de 13 de septiembre de 2023.

3 En el conflicto en Ucrania se han utilizado con frecuencia programas maliciosos del tipo *wiper* para destruir datos y sistemas, los cuales afectaron, por ejemplo, al acceso a internet de miles de abonados en la Unión, así como a una importante empresa energética alemana que perdió el acceso de seguimiento remoto a más de 5 800 turbinas eólicas. *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict* [«El papel de la dimensión cibernética en la guerra de Rusia contra Ucrania: su impacto y consecuencias para el futuro de los conflictos armados», documento en inglés], estudio del Parlamento Europeo, septiembre de 2023. PE 702.594.

informe de situación sobre la Unión de la Seguridad se centra en esbozar los expedientes legislativos y no legislativos fundamentales relativos a la Unión de la Seguridad adoptados por la Comisión y en cuya resolución y ejecución efectivas es preciso seguir trabajando.

En cuanto a la legislación de la Unión ya acordada, sus beneficios no se percibirán hasta que se ponga en práctica. Los esfuerzos deben centrarse en su transposición, ejecución y aplicación correctas y completas por parte de los Estados miembros. En 2023, la Comisión continuó garantizando el cumplimiento de la Estrategia de la UE para una Unión de la Seguridad, haciendo uso de sus competencias institucionales para incoar procedimientos de infracción cuando los Estados miembros no habían transpuesto la legislación de la Unión o lo habían hecho de forma incorrecta.

El presente informe también resume los ámbitos en los que la acción de los Estados miembros o de las agencias de la Unión es fundamental para la ejecución. Las agencias de la Unión desempeñan un papel primordial en el apoyo a la ejecución de las iniciativas de la Unión de la Seguridad, y sus responsabilidades han evolucionado en los últimos años. El informe esboza algunas de las principales tareas nuevas que se les han asignado para redoblar el apoyo a los Estados miembros en la ejecución de iniciativas clave en el marco de la Unión de la Seguridad.

Además, la situación geopolítica ha puesto de relieve la importancia de la seguridad exterior para nuestra seguridad interior. Un marco interno de la Unión más robusto en el ámbito de la seguridad está intrínsecamente ligado a unas asociaciones y una cooperación más sólidas con terceros países. La Unión debe seguir buscando activamente la manera de que el compromiso de la comunidad internacional pueda contribuir a garantizar la seguridad de los ciudadanos dentro de sus fronteras.

II. Un entorno de seguridad con garantías de futuro

Ciberseguridad y resiliencia de las infraestructuras críticas

En el marco de la Unión de la Seguridad, la Unión se ha comprometido a garantizar que todos los ciudadanos y empresas europeos estén bien protegidos, tanto en línea como fuera de línea, así como a promover un ciberespacio abierto, seguro y estable. Los incidentes de ciberseguridad, cuya magnitud, frecuencia y consecuencias van en aumento, constituyen una amenaza importante para el funcionamiento de las redes y los sistemas de información y para el mercado interior. La guerra de agresión de Rusia contra Ucrania ha exacerbado esta amenaza, y las tensiones geopolíticas actuales se ven agravadas por las intervenciones de múltiples agentes alineados con Estados, criminales y hacktivistas. El sabotaje de los gasoductos Nord Stream que tuvo lugar el pasado otoño, puso de relieve que los sectores esenciales como los de la energía, la infraestructura digital, el transporte y el espacio dependen de infraestructuras críticas resilientes. El reciente incidente relacionado con un gasoducto submarino y un cable de datos en Estonia y Finlandia ilustra la necesidad de un alto nivel de preparación para hacer frente a este tipo de situaciones. Aunque la causa de los daños sigue sin estar clara y prosiguen las investigaciones, el intercambio de información a distintos niveles entre los Estados miembros y la Comisión resulta alentador. Las alteraciones no tuvieron un efecto inmediato en la conectividad a internet ni en la seguridad del suministro de gas a escala europea o local, lo que da muestra de los progresos realizados y los esfuerzos redoblados de preparación de los últimos meses.

Por lo tanto, es esencial contar con un marco jurídico claro y sólido para garantizar la protección y la resiliencia de estas infraestructuras críticas. En este contexto, supuso un avance crucial la adopción paralela de la Directiva revisada relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (SRI 2)[4] y la Directiva relativa a la resiliencia de las entidades críticas (REC)[5], que entraron en vigor el 16 de enero de 2023. Ahora se insta a los Estados miembros a que transpongan estos actos legislativos fundamentales rápida e íntegramente, a más tardar el 17 de octubre de 2024, a fin de establecer un marco sólido de la Unión para proteger las infraestructuras críticas de la Unión contra las amenazas físicas y cibernéticas.

En julio de 2023, la Comisión estableció en un Reglamento Delegado de la Comisión servicios esenciales en los once sectores contemplados por la Directiva REC[6]. El siguiente paso consiste en que los Estados miembros lleven a cabo evaluaciones de riesgos de estos servicios. A raíz de la Recomendación del Consejo[7] de 8 de diciembre de 2022, se han intensificado los trabajos relativos a pruebas de resistencia en infraestructuras críticas, empezando por el sector de la energía, y al refuerzo de la cooperación con la OTAN y los principales países socios. Este trabajo se plasmó en un informe del Grupo de Trabajo UE-OTAN sobre la resiliencia de las infraestructuras críticas en junio de 2023, en el que se describen los retos actuales en materia de seguridad para las infraestructuras críticas en cuatro sectores estratégicos (energía, transporte, infraestructuras digitales y espacio) y se formulan recomendaciones para aumentar la resiliencia. Las recomendaciones, en particular sobre una mayor coordinación, intercambio de información y ejercicios, están siendo aplicadas por el personal de la Unión y la OTAN en el marco del diálogo estructurado sobre resiliencia.

Paralelamente, el 6 de septiembre de 2023, la Comisión adoptó una propuesta[8] de Recomendación del Consejo relativa a un plan rector sobre una respuesta coordinada a las perturbaciones importantes de infraestructuras críticas con una importancia transfronteriza significativa. El 4 de octubre de 2023 se organizó un ejercicio de debate basado en escenarios sobre dicho plan rector, con el fin de probar cómo se aplicaría en la práctica y fundamentar las negociaciones en curso sobre la propuesta en el Consejo.

A raíz de los llamamientos del Consejo[9], la Comisión, el Alto Representante y el Grupo de Cooperación SRI han llevado a cabo evaluaciones de riesgos y han formulado escenarios de riesgo desde la perspectiva de la ciberseguridad. Este trabajo se centra inicialmente en los sectores de las telecomunicaciones y la electricidad. La participación de todas las agencias y redes pertinentes, civiles y militares, permite por primera vez una evaluación exhaustiva e inclusiva a escala de la Unión. Además, complementará las evaluaciones coordinadas de riesgos para la seguridad de las cadenas de suministro críticas que se llevan a cabo en el marco de la Directiva SRI 2, así como las evaluaciones de riesgos y las pruebas de resistencia de las infraestructuras críticas en los sectores de la energía, las infraestructuras digitales, el transporte y el espacio. En aras de la coordinación y la coherencia, estas actividades deben basarse la una

---

4 Directiva (UE) 2022/2555, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2).

5 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.

6 C(2023) 4878.

7 Recomendación del Consejo de 8 de diciembre de 2022 sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas.

8 COM(2023) 526.

9 Conclusiones del Consejo, de 23 de mayo de 2022, sobre el desarrollo de la posición de la Unión Europea en materia de ciberseguridad
y llamamiento conjunto de Nevers, de 9 de marzo de 2022, para reforzar las capacidades de la UE en materia de ciberseguridad.

en la otra para poder establecer un enfoque normalizado y orientar el desarrollo de futuros ejercicios. El éxito de estas acciones dependerá ahora de la participación activa de los Estados miembros.

El funcionamiento de las economías y las sociedades depende cada vez más de los servicios y datos relacionados con el espacio, especialmente en el ámbito de la seguridad y la defensa. El espacio es un ámbito estratégico cada vez más disputado y su importancia para la seguridad ha aumentado especialmente tras la invasión rusa de Ucrania. La Estrategia Espacial de la UE para la Seguridad y la Defensa se adoptó en marzo de 2023 para reforzar nuestra posición estratégica y nuestra autonomía en el espacio. Como acción clave derivada de esta Estrategia, la Comisión Europea propondrá en 2024 una Ley Espacial de la UE que regule la protección, la sostenibilidad y la resiliencia y seguridad de las actividades espaciales en la Unión.

En cuanto a la dimensión exterior, unas infraestructuras seguras sustentan la resiliencia de la economía y las cadenas de suministro mundiales[10] y, por este motivo, la Estrategia «Pasarela Mundial» [Global Gateway] de la UE incorpora un importante componente de seguridad. Del mismo modo, dadas las interconexiones entre las infraestructuras de la Unión y de los países socios, es esencial una mayor cooperación internacional para reforzar la ciberresiliencia mundial y apoyar un ciberespacio libre, abierto, seguro y protegido.

Ley de Ciberresiliencia

Garantizar que los consumidores y las empresas puedan confiar en productos digitales seguros es de vital importancia para la ciberseguridad europea. La Comisión trató de abordar esta necesidad en su propuesta de Ley de Ciberresiliencia[11], adoptada el 15 de septiembre de 2022. Esta introduciría requisitos horizontales obligatorios de ciberseguridad para los productos con elementos digitales durante cinco años o todo su ciclo de vida (el periodo más breve de los dos). Crearía las condiciones para el diseño y el desarrollo de productos seguros con elementos digitales, garantizando que los productos de *hardware* y *software* se introduzcan en el mercado con el menor número posible de vulnerabilidades. Se trataría de un hito clave en la mejora del nivel de ciberseguridad en Europa en todos los ámbitos, y es probable que se convierta en un punto de referencia internacional, además de ofrecer claras ventajas para la industria de la ciberseguridad de la Unión en los mercados mundiales. El Parlamento Europeo y el Consejo adoptaron sus respectivas posiciones en julio de 2023 y se prevé que las negociaciones avancen a buen ritmo.

La certificación de la ciberseguridad también desempeña un papel esencial a la hora de aumentar la confianza en los productos y servicios de TIC, permitiendo a los consumidores, las empresas y las autoridades hacer elecciones con conocimiento de causa y con un nivel adecuado de ciberseguridad. Se está trabajando en la certificación de la ciberseguridad, y el esquema europeo de certificación de la ciberseguridad basado en criterios comunes se evalúa mediante procedimientos de comité. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) está preparando la propuesta de esquema europeo de certificación de la ciberseguridad para los servicios en la nube (EUCS), la cual estudia el Grupo Europeo de Certificación de la Ciberseguridad. El intenso trabajo con expertos de diversos sectores, consumidores y proveedores debe conducir a un enfoque jurídico y técnico sólido que ofrezca las garantías de seguridad necesarias en consonancia con el Derecho de la Unión, los compromisos internacionales y las obligaciones impuestas por la Organización Mundial del Comercio. Asimismo, ENISA está preparando el esquema candidato de la UE para las redes 5G y la cartera de identidad digital de la UE («cartera EUDI»). Los esfuerzos concertados de todos los Estados

[10] JOIN(2021) 30.
[11] COM(2022) 454.

miembros son esenciales para mejorar la seguridad general de los productos, servicios y procesos de TIC.

Reglamentos sobre seguridad de la información y ciberseguridad para instituciones, órganos y organismos de la Unión (IOUE)

Los Reglamentos propuestos conjuntamente en marzo de 2022 para regular la ciberseguridad y la seguridad de la información de las propias instituciones de la Unión han avanzado a distinto ritmo. El pasado mes de junio se alcanzó un acuerdo político en cuanto al Reglamento sobre ciberseguridad, el cual permite reforzar la posición en materia de ciberseguridad de todas las instituciones, órganos y organismos de la Unión y refleja la importancia que esta atribuye a la rápida implementación de la presente propuesta. Dada la situación, resulta especialmente preocupante que la propuesta paralela relativa a la seguridad de la información, esencial para completar un marco legislativo sólido para las IOUE, avance a un ritmo inesperadamente lento. Ambas propuestas deben adoptarse antes de las elecciones al Parlamento Europeo para que la Administración europea sea creíble y resiliente en el contexto geopolítico actual. Un conjunto mínimo de reglas y normas de seguridad de la información para todas las IOUE aportaría certezas a todas las partes implicadas y garantizaría una protección coherente frente a la evolución de las amenazas a la información de la Unión, tanto clasificada como no clasificada. En conjunto, estas nuevas normas proporcionarían una base estable para el intercambio seguro de información entre IOUE y con los Estados miembros, con prácticas y medidas normalizadas para proteger los flujos de información. Por consiguiente, responden a múltiples llamamientos del Consejo para aumentar la resiliencia de las IOUE y proteger mejor el proceso de toma de decisiones de la Unión frente a injerencias malintencionadas.

Ley de Cibersolidaridad

Sobre la base del sólido marco estratégico, político y legislativo ya existente, la propuesta de Ley de Cibersolidaridad[12], presentada el 18 de abril de 2023 por la Comisión, contribuirá a mejorar la detección de ciberamenazas, la resiliencia y la preparación a todos los niveles del ecosistema de la ciberseguridad de la Unión. Estos objetivos se ejecutarían a través de tres acciones principales:

(1) El despliegue de un ***Escudo Cibernético Europeo*** para crear y mejorar las capacidades comunes de detección y conocimiento de la situación. Estará integrado por todos los centros de operaciones de seguridad nacionales («COS nacionales») y transfronterizos («COS transfronterizos»).
(2) La creación de un ***Mecanismo de Ciberemergencia*** para ayudar a los Estados miembros a prepararse ante incidentes de ciberseguridad significativos y a gran escala, así como a responder y recuperarse inmediatamente de ellos. El apoyo a la respuesta a incidentes incluiría la reserva de ciberseguridad de la UE, que también estaría a disposición de las IOUE y de los terceros países asociados al programa Europa Digital, siempre que su Acuerdo de Asociación al Programa Europa Digital así lo prevea.
(3) El establecimiento de un ***Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad*** para examinar y evaluar incidentes significativos o a gran escala. ENISA coordinará y preparará los informes de revisión posteriores a los incidentes.

[12] COM(2023) 209.

Se han iniciado las negociaciones en el Consejo y en el Parlamento Europeo. La conclusión de las negociaciones antes de que finalice el actual mandato del Parlamento Europeo daría un gran impulso a los esfuerzos por proteger a los ciudadanos y a las empresas de toda la Unión.

La Academia de Cibercapacidades de la UE

Mientras las ciberamenazas aumentan, la Unión necesita urgentemente profesionales con las capacidades y competencias necesarias para prevenir, detectar, disuadir y defender a la Unión frente a los ciberataques. Sus necesidades de trabajadores en el campo de la ciberseguridad se estiman actualmente en 883 000 profesionales, mientras que en 2022 las vacantes sin cubrir oscilaron entre 260 000 y 500 000. Debe alentarse a todos los sectores de la sociedad a que contribuyan a colmar esta laguna, pero, en particular en 2022, solo el 20 % de las personas tituladas en ciberseguridad y el 19 % de las personas especialistas en tecnologías de la información y las comunicaciones eran mujeres. Como parte del Año Europeo de las Competencias 2023, la Comisión adoptó el 18 de abril de 2023[13] una iniciativa acogida con satisfacción por los Estados miembros[14] para crear una Academia de Cibercapacidades a fin de colmar la brecha de talento en materia de ciberseguridad. La Academia de Cibercapacidades reunirá las iniciativas existentes en materia de capacidades de ciberseguridad y mejorará la coordinación. La Comisión anima a los Estados miembros, a las autoridades regionales y locales y a las entidades públicas europeas a adoptar estrategias o iniciativas específicas en materia de capacidades de ciberseguridad, o bien a integrar las capacidades de ciberseguridad en las estrategias o iniciativas pertinentes con un ámbito de aplicación más amplio (ciberseguridad, capacidades digitales, empleo, etc.). La participación de las partes interesadas del sector privado también será esencial para reducir el déficit de capacidades en materia de ciberseguridad y la consiguiente escasez de mano de obra en Europa.

Los drones

El uso malintencionado de drones constituye otra amenaza creciente para los espacios públicos y las infraestructuras críticas. Los incidentes relacionados con drones se han vuelto más frecuentes, tanto dentro de la Unión como fuera de sus fronteras, y las soluciones de defensa contra los drones son una herramienta clave para las autoridades policiales y otras autoridades públicas de la Unión, así como para los operadores de infraestructuras críticas. Al mismo tiempo, el uso legítimo de drones contribuye de manera considerable a la consecución de la doble transición ecológica y digital[15]. Tal como se anunció en la Estrategia 2.0 para los Drones, adoptada en noviembre de 2022, la Comisión adopta hoy una Comunicación sobre cómo contrarrestar las amenazas potenciales que plantean los drones, respaldada por dos manuales con orientaciones prácticas sobre aspectos técnicos clave[16]. La iniciativa tiene por objeto aportar un marco político global y armonizado, con un entendimiento común de las normas vigentes para combatir las posibles amenazas planteadas por los drones y adaptarse en la medida necesaria a la rápida evolución tecnológica. Se invita a los Estados miembros y a los operadores privados pertinentes a que colaboren estrechamente con la Comisión para garantizar su plena aplicación.

Seguridad marítima y aérea

[13] COM(2023) 207.
[14] Conclusiones del Consejo, de 22 de mayo de 2023, sobre la política de ciberdefensa de la UE.
[15] COM(2022) 652.
[16] COM(2023) 659.

Las actividades ilícitas, como la piratería, el robo a mano armada en el mar, el tráfico ilícito de migrantes y la trata de seres humanos, armas y drogas, así como el terrorismo, siguen siendo retos para la seguridad marítima, agravados por la evolución de amenazas como los ataques híbridos y los ciberataques. El 10 de marzo de 2023, la Comisión y el Alto Representante adoptaron una Comunicación conjunta por la que se actualiza la Estrategia de Seguridad Marítima de la UE[17], que ahora debe aplicarse en consonancia con el Plan de Acción actualizado.

En el ámbito de la seguridad aérea, el 2 de febrero de 2023 la Comisión adoptó un documento de trabajo de los servicios de la Comisión titulado *Working towards an enhanced and more resilient aviation security policy*[18] [«Trabajar por una política de seguridad aérea mejorada y más resiliente», documento en inglés], que contiene un ambicioso programa para 1) modernizar la arquitectura reglamentaria de la seguridad aérea 2) fomentar el desarrollo y la adopción de soluciones más innovadoras; y 3) actualizar la base de referencia en materia de seguridad aérea para que los aeropuertos de la Unión puedan beneficiarse plenamente de las tecnologías nuevas y punteras para hacer frente a las amenazas más prioritarias. Deben ejecutarse catorce acciones emblemáticas en un plazo de dos años.

La Comisión insta al Parlamento Europeo y al Consejo a que concluyan urgentemente las negociaciones, en cualquier caso antes de que finalice el mandato del actual Parlamento Europeo, sobre los siguientes expedientes:

- La propuesta de Ley de Ciberresiliencia;
- La propuesta de Ley de Cibersolidaridad;
- La propuesta de Reglamento sobre seguridad de la información para las IOUE.

La Comisión insta a los Estados miembros a:

- proseguir la transposición de la Directiva relativa a la resiliencia de las entidades críticas con carácter prioritario, así como las pruebas de resistencia de las infraestructuras críticas en el sector de la energía;
- adoptar la Recomendación del Consejo sobre un Plan director para coordinar la respuesta a escala de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa;
- transponer plena y urgentemente la Directiva SRI 2 para impulsar la ciberseguridad de las entidades esenciales e importantes;
- participar activamente en la realización de evaluaciones de riesgos de ciberseguridad y en la elaboración de escenarios de riesgo de infraestructuras y cadenas de suministro críticas;
- dar seguimiento a la labor de la Academia de Cibercapacidades con un fuerte compromiso a escala europea y estrategias o iniciativas nacionales específicas en materia de capacidades de ciberseguridad, con la participación de las principales partes interesadas, en particular las autoridades regionales y locales;
- colaborar con los operadores privados pertinentes y la Comisión para garantizar la aplicación de todas las acciones enumeradas en la Comunicación sobre la lucha contra las amenazas potenciales causadas por drones;
- aplicar el Plan de Acción de la Estrategia de Seguridad Marítima de la UE e informar periódicamente sobre los logros alcanzados;

[17] JOIN(2023) 8.
[18] SWD(2023) 37.

- aplicar las catorce acciones emblemáticas identificadas para mejorar la seguridad aérea.

III. Hacer frente a las amenazas cambiantes

Las nuevas tensiones geopolíticas han aportado pruebas contundentes de que el reto de la seguridad para la Unión no solo está aumentando, sino que es cada vez más volátil y se ha acentuado debido al carácter híbrido de muchas amenazas. La seguridad también debe responder a los cambios en la sociedad y la tecnología. La pandemia de COVID-19 proporcionó nuevas oportunidades a los ciberdelincuentes; se produjo, en particular, una mayor amenaza de material de abusos sexuales a menores en línea. Los delincuentes y los agentes malintencionados siempre están dispuestos a aprovechar los avances tecnológicos. Ante estas amenazas, a menudo complejas y multidimensionales, es necesaria una acción firme y coherente de la Unión.

Reglamento sobre la lucha contra el abuso sexual de menores en línea

La Evaluación sobre la amenaza de la delincuencia organizada en Internet de Europol reveló que, en 2022, la explotación y los abusos sexuales de menores habían aumentado aún más en términos de frecuencia y gravedad, y los delincuentes habían seguido aprovechando las posibilidades técnicas para ocultar sus acciones e identidades[19]. El sistema actual, basado en la detección voluntaria y la denuncia por parte de las empresas, ha demostrado ser insuficiente para proteger a los menores. Un Reglamento provisional permite la detección y notificación voluntarias por parte de las empresas, siempre que ello sea lícito en virtud del Reglamento general de protección de datos (RGPD). Este Reglamento expira en agosto de 2024. En mayo de 2022, la Comisión propuso un Reglamento[20] para abordar el uso indebido de los servicios en línea con fines de abuso sexual de menores. El marco propuesto hace especial hincapié en la prevención. Las empresas estarían obligadas a evaluar el riesgo de abuso sexual de menores a través de sus sistemas y a adoptar medidas preventivas. Como medida de último recurso y en caso de riesgo significativo únicamente, los órganos jurisdiccionales nacionales o las autoridades administrativas independientes podrían emitir órdenes de detección específicas a los proveedores de servicios. Un nuevo Centro de la UE independiente facilitaría los esfuerzos de los proveedores de servicios que actúan como centro de conocimientos especializados, proporcionando información fiable sobre el material identificado, recibiendo y analizando denuncias de abusos sexuales de menores en línea procedentes de proveedores para detectar denuncias erróneas y prestando apoyo a las víctimas. Es esencial que las nuevas normas se adopten y ejecuten lo antes posible para proteger a los menores de nuevos abusos, evitar que el material vuelva a aparecer en línea y llevar a los delincuentes ante la justicia. Se están entablando negociaciones en el Consejo y en el Parlamento con el objetivo de llegar a un acuerdo sobre el expediente antes de que finalice el mandato del Parlamento.

Directiva sobre la lucha contra la violencia contra las mujeres y la violencia doméstica

La ciberviolencia contra las mujeres, también en el contexto de la violencia doméstica, se ha convertido en una nueva forma de este tipo de violencia, que se propaga y traspasa las fronteras

[19] Europol (2023), *Internet Organised Crime Threat Assessment (IOCTA) 2023* [«Evaluación de la amenaza de la delincuencia organizada en Internet (IOCTA) 2023», documento en inglés].

[20] COM(2022) 209.

de los Estados miembros a través de internet. En marzo de 2022, la Comisión propuso una Directiva para abordar la violencia contra las mujeres y la violencia doméstica, la cual recogía normas específicas sobre ciberviolencia y medidas para colmar las lagunas en materia de protección, acceso a la justicia y prevención. La rápida adopción y ejecución de esta Directiva proporcionaría a los Estados miembros herramientas adicionales para luchar contra esta forma de delincuencia. Los colegisladores entablaron negociaciones interinstitucionales en julio de 2023, y se han propuesto concluir las negociaciones antes de que finalice el actual mandato del Parlamento Europeo.

Ciberseguridad de las redes 5G

La seguridad de las redes 5G es una prioridad de primer orden para la Comisión, además de un componente esencial de su Estrategia para una Unión de la Seguridad. Las redes 5G son una infraestructura central que sienta las bases para una amplia gama de servicios esenciales para el funcionamiento del mercado interior y para funciones sociales y económicas vitales. El 15 de junio de 2023, las autoridades de los Estados miembros de la Unión representadas en el Grupo de Cooperación SRI publicaron, con el apoyo de la Comisión y ENISA, un segundo informe de situación sobre la aplicación del conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G. Según el informe, veinticuatro Estados miembros han adoptado o preparan medidas legislativas que otorgan a las autoridades nacionales competencias para llevar a cabo una evaluación de los proveedores y emitir restricciones, y diez Estados miembros han impuesto ya tales restricciones. Sin embargo, para evitar vulnerabilidades para la Unión en su conjunto, es necesario adoptar nuevas medidas que podrían afectar gravemente a la seguridad de los usuarios particulares y las empresas de toda la Unión, así como de sus infraestructuras críticas. Todos los Estados miembros deben aplicar el conjunto de instrumentos sin demora. Ese mismo día, la Comisión adoptó una Comunicación sobre la aplicación del conjunto de instrumentos por parte de los Estados miembros y sobre las comunicaciones corporativas de la propia Comisión y las actividades de financiación de la Unión. En ella se puso de manifiesto la gran preocupación por los riesgos para la seguridad de la Unión que plantean los proveedores de equipos de comunicación de redes móviles Huawei y ZTE. En este contexto, la Comisión está tomando medidas para evitar la exposición de sus comunicaciones corporativas a redes móviles cuyos proveedores sean Huawei y ZTE. En las contrataciones se excluirán nuevos servicios de conectividad que dependan de equipos de dichos proveedores y la Comisión colaborará con los Estados miembros y los operadores de telecomunicaciones para garantizar que dichos proveedores se eliminen progresivamente de los servicios de conectividad existentes en los centros de la Comisión. La Comisión también está estudiando cómo reflejar esta decisión en los programas e instrumentos de financiación de la Unión pertinentes, respetando plenamente el Derecho de la Unión.

Acceso a los datos para una aplicación efectiva de la ley

En la era digital actual, casi todos los delitos tienen un componente digital. También se están utilizando con fines delictivos tecnologías y herramientas que en algunos casos son imprescindibles para satisfacer las necesidades de ciberseguridad, protección de datos y privacidad de nuestra sociedad. Esto hace cada vez más difícil mantener una aplicación efectiva de la ley en toda la Unión para salvaguardar la seguridad pública y prevenir, detectar, investigar y enjuiciar los delitos y, aunque se han realizado esfuerzos significativos a escala nacional y de la Unión a través de la legislación y de iniciativas de desarrollo de capacidades e innovación, persisten los retos jurídicos y técnicos. La Comisión, en asociación con la Presidencia del Consejo, ha creado un Grupo de Alto Nivel sobre el acceso a los datos para una aplicación efectiva de la ley con el fin de proporcionar una plataforma colaborativa para un amplio abanico de partes interesadas y expertos, al objeto de explorar los retos a los que se enfrentan los

profesionales encargados de la aplicación de la ley penal (como el cifrado, la retención de datos, las redes 5G y la normalización). La Comisión espera que el Grupo de Alto Nivel formule recomendaciones equilibradas, sólidas y alcanzables antes de junio de 2024, que reflejen la complejidad de estas cuestiones, también desde la perspectiva de la ciberseguridad y la protección de datos. Por lo tanto, se anima a los Estados miembros y a los expertos participantes a que se impliquen activamente en este proceso y trabajen en pos de soluciones efectivas, legales y comúnmente aceptadas.

Amenazas híbridas

En un contexto geopolítico en el que las amenazas híbridas son cada vez más complejas y sofisticadas, la Brújula Estratégica para la Seguridad y la Defensa[21] de la UE (Brújula Estratégica) proporcionó una evaluación conjunta de las amenazas y los retos a los que se enfrenta la Unión, así como un plan de acción estratégico. El aumento de los comportamientos malintencionados en el ciberespacio por parte de Estados y agentes no estatales, entre otros en el marco de la guerra contra Ucrania, ha dejado aún más patente que el ciberespacio es un ámbito de la política exterior y de seguridad. Los posibles riesgos de acciones malintencionadas y de desinformación exigen una vigilancia especial en los períodos electorales, también en la fase previa a las elecciones europeas de 2024.

Teniendo en cuenta el alto riesgo de efectos indirectos, la Unión ha seguido desarrollando actividades de creación de capacidades cibernéticas y fomentando asociaciones con terceros países, en particular a través de diálogos específicos en materia cibernética, para contribuir activamente a su resiliencia general. Se han desarrollado, revisado y reforzado una serie de herramientas a fin de mejorar la capacidad de la Unión para abordar de forma efectiva las amenazas híbridas, tal como se describe en el séptimo informe de situación sobre las amenazas híbridas, publicado el 14 de septiembre de 2023[22]. Algunas de ellas son:

- el conjunto de instrumentos de la UE contra las amenazas híbridas, para garantizar un marco para una respuesta coordinada y bien fundamentada a las amenazas y campañas híbridas;
- los trabajos en curso encaminados a crear equipos de la Unión de respuesta rápida contra amenazas híbridas para prestar apoyo personalizado a corto plazo a los Estados miembros, los países socios y las misiones y operaciones de la política común de seguridad y defensa (PCSD);
- el Protocolo operativo revisado de la UE para la lucha contra las amenazas híbridas («EU Playbook»)[23], que describe los procesos y estructuras de la Unión para hacer frente a las amenazas y campañas híbridas;
- las directrices de ejecución revisadas del marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas[24] («conjunto de instrumentos de ciberdiplomacia») que permite el desarrollo de estrategias sostenidas, adaptadas, coherentes y coordinadas contra los agentes de ciberamenazas persistentes;
- el conjunto de instrumentos contra la manipulación de información y la injerencia por parte de agentes extranjeros, a fin de reforzar las herramientas existentes de la Unión para prevenir, disuadir y responder a la misma;
- la política de ciberdefensa de la UE[25], para impulsar las capacidades de ciberdefensa de la Unión, mejorar el conocimiento de la situación y coordinar todo el espectro de

[21] Documento del Consejo 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 de 8 de junio de 2023.
[25] JOIN(2022) 49.

opciones defensivas disponibles, con el fin de reforzar la resiliencia, responder a los ciberataques y garantizar la solidaridad y la asistencia mutua.

Por consiguiente, se alienta a los Estados miembros a que prosigan y mejoren su cooperación en este ámbito, garantizando la aplicación efectiva de los instrumentos mencionados, en particular mediante ejercicios periódicos, y alcanzando un acuerdo sobre el concepto de equipos de respuesta rápida contra amenazas híbridas, que proporcionará orientación para la adopción de nuevos pasos hacia la creación de los equipos.

La inteligencia artificial en el contexto de la aplicación de la ley

La inteligencia artificial (IA) se ha convertido rápidamente en un elemento común de la vida cotidiana. Los efectos del uso de la IA en la ciberdelincuencia y la ciberseguridad aún no se conocen plenamente, pero sin duda plantearán nuevos retos. Si bien la IA puede aportar beneficios cuando se utiliza de manera segura y controlada, puede resultar peligrosa en manos de agentes malintencionados, ya que podría ayudar a los delincuentes a ocultar su identidad en delitos como el terrorismo y el abuso sexual de menores. Por lo tanto, es fundamental que las autoridades se mantengan al día de su evolución para prevenir los abusos y actuar ante usos indebidos[26]. Las negociaciones sobre la propuesta de Ley de Inteligencia Artificial tienen por objeto abordar estas cuestiones y han entrado en una fase crucial en la que los colegisladores debaten cuestiones técnicas y políticas que determinarán las interacciones con esta tecnología en los próximos años. Será esencial hallar soluciones equilibradas, especialmente en lo que respecta a las aplicaciones de alto riesgo, también en el ámbito policial.

La Comisión insta al Parlamento Europeo y al Consejo a que concluyan las negociaciones interinstitucionales, con carácter urgente y en cualquier caso antes de que finalice el mandato del actual Parlamento, sobre los siguientes expedientes pendientes:

- Propuesta de Reglamento sobre la lucha contra el abuso sexual de menores en línea;
- Propuesta de Directiva sobre la lucha contra la violencia contra las mujeres y la violencia doméstica;
- Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial).

La Comisión insta a los Estados miembros a:

- lograr la plena ejecución sin demora del conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G;
- apoyar la labor del Grupo de Alto Nivel sobre el acceso a los datos para una aplicación efectiva de la ley, con vistas a formular recomendaciones claras, sólidas y factibles para abordar de manera proporcionada los retos actuales y previstos;
- adoptar medidas, en cooperación con el Alto Representante, para garantizar la aplicación efectiva del conjunto de instrumentos de la UE contra las amenazas híbridas, el conjunto de instrumentos de ciberdiplomacia revisado y el conjunto de instrumentos contra la manipulación de la información y la injerencia por parte de agentes extranjeros, en particular mediante ejercicios periódicos y teniendo en cuenta las dinámicas mundiales;

[26] Véase, por ejemplo, el informe de Europol publicado el 17 de abril de 2023: *ChatGPT - The impact of Large Language Models on Law Enforcement* [«ChatGPT: el impacto de los grandes modelos lingüísticos en la aplicación de la ley», documento en inglés].

- alcanzar un acuerdo sobre el concepto de equipos de respuesta rápida contra amenazas híbridas.

IV. Protección de los europeos frente al terrorismo y la delincuencia organizada

El riesgo de que acontecimientos internacionales o locales provoquen nuevos brotes de terrorismo está siempre presente. Al mismo tiempo, la delincuencia organizada y el tráfico de drogas se encuentran entre las amenazas más graves para la seguridad de la Unión. A fin de redoblar los esfuerzos conjuntos de la Unión para combatir estas amenazas, se ha emprendido una labor colectiva encaminada a la ejecución de la Estrategia de la UE contra la Delincuencia Organizada[27], la Estrategia de la UE en la lucha contra la trata de seres humanos[28], la Agenda y Plan de Acción de la UE en materia de Lucha contra la Droga[29] y la Agenda de lucha contra el terrorismo de la UE[30]. Sin embargo, para responder al preocupante deterioro de la situación en lo que respecta a la delincuencia organizada y el tráfico de drogas, es necesario intensificar el trabajo de los Estados miembros y de la Unión, a fin de reforzar nuestra respuesta colectiva a las redes delictivas y proteger mejor a las víctimas de la delincuencia. Al mismo tiempo que el presente informe, se publica una hoja de ruta de la UE para luchar contra el tráfico de drogas y la delincuencia organizada[31].

En el ámbito de la lucha contra el terrorismo, la Unión está reforzando también su conjunto de instrumentos exteriores[32], haciendo pleno uso de los diálogos políticos de alto nivel sobre la lucha contra el terrorismo y la red de expertos en lucha contra el terrorismo y seguridad de las delegaciones de la Unión, así como a través de su participación en foros multilaterales, en particular como copresidente del Foro Mundial contra el Terrorismo.

Narcotráfico

Con el nuevo mandato de la Agencia de la UE para las Drogas, que se aplicará a partir de julio de 2024, la Unión estará mejor preparada para abordar un complejo problema de seguridad y salud que afecta a millones de personas dentro y fuera de sus fronteras. Asimismo, la Comisión revisa[33] los Reglamentos sobre precursores de drogas[34] para abordar los principales retos identificados en la evaluación de 2020[35], la cual puso de relieve la necesidad de resolver la problemática de los precursores de diseño[36] para reducir el suministro de drogas ilegales.

Sin embargo, ante un aumento sin precedentes de las drogas ilícitas disponibles en Europa, debe intensificarse la lucha contra el tráfico de drogas, en cooperación con los socios internacionales. Es necesario que los Estados miembros y la Unión adopten medidas adicionales para

[27] COM(2021) 170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM(2023) 641.
[32] Tal como se pide en la Brújula Estratégica y en las Conclusiones del Consejo sobre «Abordar la dimensión exterior de una amenaza terrorista y extremista violenta en constante evolución», adoptadas en junio de 2022.
[33] Precursores de drogas: legislación de la UE (revisión de las normas) (europa.eu).
[34] Reglamento (CE) n.° 273/2004 del Parlamento Europeo y del Consejo sobre precursores de drogas y Reglamento (CE) n.° 111/2005 del Consejo por el que establecen normas para la vigilancia del comercio de precursores de drogas entre la Comunidad y terceros países.
[35] COM(2020) 768.
[36] Acción 23 del Plan de Acción de la UE en materia de Lucha contra la Droga, COM(2020) 606.

desmantelar las redes delictivas y proteger mejor a las víctimas de delitos. La Comisión presenta hoy una hoja de ruta de la UE para luchar contra el tráfico de drogas y la delincuencia organizada. Establece diecisiete acciones en cuatro ámbitos prioritarios: reforzar la resiliencia de los centros logísticos con una Alianza Europea de Puertos; desmantelar las redes delictivas; intensificar los esfuerzos de prevención, y reforzar la colaboración con los socios internacionales. Estas acciones se ejecutarán en 2024 y 2025.

Armas de fuego

El tráfico de armas de fuego alimenta la delincuencia organizada tanto dentro de la Unión como en su vecindad. Se calcula que existe una cantidad tan importante como 35 millones de armas de fuego ilícitas en poder de civiles en la UE; además, unas 630 000 armas de fuego están declaradas como robadas o perdidas en el Sistema de Información de Schengen. Debido a la expansión de la entrega rápida de paquetes y de nuevas tecnologías como la impresión 3D, el tráfico de armas de fuego está adoptando nuevas formas capaces de eludir los controles. La guerra de agresión de Rusia contra Ucrania también ha aumentado el riesgo de proliferación de armas de fuego. En octubre de 2022, la Comisión adoptó una propuesta para actualizar la legislación vigente en materia de importación, exportación y tránsito de armas de fuego de uso civil, a fin de colmar las lagunas existentes en las normas vigentes que pueden aumentar el número de armas de fuego introducidas de contrabando y desviadas hacia la Unión[37]. A medio plazo, estas nuevas normas contribuirán a reducir el riesgo de elusión de embargos en el caso de las exportaciones de armas de fuego de uso civil, así como a aumentar los controles de la importación de este tipo de armas de fuego procedentes de terceros países. Ambos colegisladores tienen que adoptar aún sus posiciones sobre este expediente con el objetivo de alcanzar un acuerdo al respecto antes de que finalice el mandato del Parlamento.

Trata de seres humanos

La trata de seres humanos es una forma especialmente grave de delincuencia organizada y constituye una grave violación de los derechos fundamentales. Las víctimas son objeto de trata dentro de la Unión principalmente con fines de explotación sexual y laboral, pero también de mendicidad y delincuencia forzadas, entre otros. En diciembre de 2022, la Comisión propuso modificar la Directiva relativa a la prevención y lucha contra la trata de seres humanos[38] para introducir normas actualizadas a fin de abordar las deficiencias del marco jurídico actual. En particular, una vez adoptada, la Directiva revisada añadiría el matrimonio forzado y la adopción ilegal a su ámbito de aplicación e introduciría una referencia explícita a la dimensión en línea de la trata de seres humanos. También incluiría un régimen obligatorio de sanciones para los autores y formalizaría el establecimiento de mecanismos nacionales de derivación a fin de mejorar la identificación temprana y la derivación transfronteriza para la asistencia y el apoyo a las víctimas. El uso consciente de los servicios prestados por las víctimas de la trata se tipificaría como delito y la recopilación anual de datos sobre la trata de seres humanos, que será publicada por Eurostat, pasaría a ser obligatoria. El Consejo adoptó su orientación general en junio de 2023, mientras que el Parlamento aún debe fijar su posición. Será necesario actuar con rapidez para llegar a un acuerdo antes de que finalice el mandato del Parlamento.

Delitos contra el medio ambiente

Los delitos contra el medio ambiente se han convertido en una amenaza mundial, y aumentan a un ritmo estimado de entre el 5 y el 7 % cada año. Los importantes beneficios que pueden generarse, las lagunas jurídicas entre los Estados miembros y el bajo riesgo de detección atraen

[37] COM(2022) 480.
[38] COM(2022) 732.

a la delincuencia organizada. Según Europol, existen indicios de que el producto de estas actividades se utiliza para financiar el terrorismo. En diciembre de 2021, la Comisión adoptó una propuesta para sustituir la Directiva de 2008 relativa a la protección del medio ambiente mediante el Derecho penal. Esta propuesta se centra en perfeccionar y actualizar las definiciones de las categorías de delitos contra el medio ambiente y en definir tipos y niveles de sanciones efectivos, disuasorios y proporcionados para las personas físicas y jurídicas. Entre los nuevos delitos figuran los relacionados con la deforestación ilegal, las infracciones de la legislación de la Unión en materia de sustancias químicas, la extracción ilegal de aguas superficiales o subterráneas y el reciclado ilegal de buques. La propuesta tiene por objeto reforzar significativamente la cadena de aplicación de la ley y la cooperación transfronteriza entre las autoridades de los Estados miembros y las agencias y organismos de la Unión. El Parlamento Europeo y el Consejo han adoptado sus respectivas posiciones sobre la propuesta y se encuentran en un proceso de negociación que se espera que concluya antes de final de año. Debe aplicarse un plan de acción revisado[39] contra el tráfico de especies silvestres para reforzar la prevención y el cumplimiento.

Recuperación y decomiso de activos

Privar a los delincuentes de sus ingresos ilícitos es fundamental para desarticular la delincuencia organizada. Por este motivo, además de la propuesta que proporciona a las autoridades policiales acceso a la información sobre cuentas bancarias en toda la Unión[40] (sobre la que se alcanzó un acuerdo político en junio de 2023), la Comisión presentó una propuesta sobre recuperación y decomiso de activos[41] en mayo de 2022, con el fin de reforzar las capacidades de seguimiento, identificación, embargo, decomiso y gestión de activos. Las disposiciones fundamentales de la propuesta se refieren a los requisitos para las investigaciones financieras y a las competencias e instrumentos adicionales de los organismos de recuperación de activos, así como a medidas de embargo y decomiso más eficaces para un conjunto ampliado de delitos. Una de las nuevas infracciones penales a las que se aplicarían estas medidas es la vulneración de las medidas restrictivas de la Unión. En diciembre de 2022, la Comisión adoptó una propuesta independiente para armonizar las definiciones penales y las sanciones por incumplimiento de las medidas restrictivas de la Unión. La aplicación y el cumplimiento efectivos de las medidas restrictivas de la Unión siguen siendo una prioridad absoluta para la Comisión, reforzada por la labor del Grupo de Trabajo «Inmovilización y Decomiso» creado por la Comisión en respuesta a la guerra de agresión de Rusia contra Ucrania. Para ambas propuestas, el Parlamento Europeo y el Consejo han adoptado sus posiciones con el fin de llegar a un acuerdo antes de finales de este año.

Paquete de medidas de lucha contra el blanqueo de capitales

El blanqueo de capitales está vinculado a prácticamente todas las actividades delictivas que generan ingresos delictivos en la Unión[42] y, por lo tanto, es un elemento clave para luchar contra la delincuencia en la Unión. En julio de 2021, la Comisión presentó propuestas ambiciosas para reforzar las medidas de la Unión encaminadas a prevenir el blanqueo de capitales y la financiación del terrorismo[43]. Se trata de cuatro propuestas legislativas para reforzar la

[39] COM(2022) 581.
[40] COM(2021) 429.
[41] COM(2022) 245.
[42] Europol, *Enterprising criminals – Europe's fight against the global networks of financial and economic crime* [«Abordar la delincuencia: la lucha de Europa contra las redes mundiales de delincuencia financiera y económica», documento en inglés], 2020.
[43] COM(2021) 420.

prevención y la detección de los intentos de los delincuentes de blanquear ingresos ilícitos o financiar actividades terroristas a través del sistema financiero. En mayo de 2023, los colegisladores adoptaron una de las cuatro iniciativas del paquete para garantizar la trazabilidad de las transferencias de criptoactivos[44]. El presente Reglamento será aplicable a partir del 30 de diciembre de 2024, fecha en la que todos los proveedores de servicios de criptoactivos tendrán que recopilar y conservar información sobre los originadores y los beneficiarios de las transferencias de criptoactivos. Las tres propuestas restantes tienen por objeto i) establecer una nueva autoridad de la Unión en materia de lucha contra el blanqueo de capitales para garantizar una supervisión coherente y de alta calidad en todo el mercado interior, en particular de las entidades transfronterizas de mayor riesgo, que apoye y coordine el trabajo de las Unidades de Inteligencia Financiera, ii) establecer normas armonizadas para el sector privado, incluida la introducción de un límite de 10 000 EUR a escala de la Unión para los grandes pagos en efectivo por servicios y bienes, y iii) reforzar las competencias y los instrumentos de cooperación de las autoridades competentes. Se espera que este paquete mejore significativamente la capacidad de la Unión para luchar contra el blanqueo de capitales y proteger a los ciudadanos de la Unión del terrorismo y la delincuencia organizada. Los colegisladores han entablado negociaciones sobre las tres propuestas restantes al objeto de alcanzar un acuerdo sobre este expediente antes de que finalice el mandato del Parlamento.

La Comisión insta al Parlamento Europeo y al Consejo a que concluyan las negociaciones interinstitucionales, con carácter urgente y en cualquier caso antes de que finalice el mandato del actual Parlamento, sobre los siguientes expedientes pendientes:

- Propuesta de Directiva sobre recuperación y decomiso de activos;
- Propuesta de Directiva para armonizar las definiciones de las infracciones y las sanciones penales por la vulneración de las medidas restrictivas de la Unión;
- Propuesta de Directiva relativa a la prevención y lucha contra la trata de seres humanos;
- Propuesta de Directiva relativa a una mejor protección del medio ambiente mediante el Derecho penal;
- Propuesta de paquete de medidas de lucha contra el blanqueo de capitales;
- Propuesta de actualización de la legislación vigente en materia de importación, exportación y tránsito de armas de fuego de uso civil.

La Comisión pide a los Estados miembros y a las agencias y organismos de la Unión que:

- Colaboren en la aplicación de las diecisiete acciones de la hoja de ruta de la UE para luchar contra el tráfico de drogas y la delincuencia organizada en 2023 y 2024.

V. Un ecosistema de seguridad europeo sólido

En los últimos años, las amenazas a la seguridad han adquirido un carácter cada vez más transfronterizo, lo que exige mayores sinergias y una cooperación más estrecha a todos los niveles. Desde la adopción de la Estrategia para una Unión de la Seguridad, se han adoptado iniciativas importantes para maximizar la cooperación transfronteriza, racionalizar y mejorar los instrumentos y procedimientos disponibles tanto en las fronteras exteriores como dentro del

[44] Reglamento (UE) 2023/1113, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849.

espacio Schengen y mejorar el intercambio de información entre las autoridades policiales y judiciales para combatir mejor la delincuencia organizada. En este contexto, la aplicación efectiva del marco de interoperabilidad para el intercambio de datos constituye un pilar importante para mejorar la seguridad y una respuesta europea eficaz a las amenazas transfronterizas, garantizando al mismo tiempo la libre circulación interna.

Mejora del intercambio de información dentro del espacio Schengen: Información anticipada sobre los pasajeros (API), registros de nombres de los pasajeros (PNR) y Prüm II

Las dos propuestas sobre API adoptadas por la Comisión en diciembre de 2022[45] mejorarían la seguridad interior de la Unión al proporcionar a las autoridades policiales de los Estados miembros herramientas adicionales para luchar contra la delincuencia grave y el terrorismo. En particular, la información anticipada sobre los pasajeros de los vuelos interiores de la Unión, unida a los PNR de los viajeros aéreos, permitiría a las autoridades policiales de los Estados miembros aumentar significativamente la eficiencia de sus investigaciones, al facilitar intervenciones más específicas. Es importante que las normas propuestas se adopten lo antes posible: esto no solo respaldaría la lucha contra la delincuencia organizada y el terrorismo, sino que también reduciría significativamente la necesidad de controles sistemáticos de todos los viajeros en caso de restablecimiento temporal de los controles en las fronteras interiores, facilitando el transporte aéreo y la libertad de circulación. El 6 de septiembre de 2023, la Comisión Europea recomendó al Consejo que autorizara las negociaciones con Suiza, Islandia y Noruega de acuerdos sobre la transferencia de datos PNR. La adopción de estas tres Recomendaciones promovería una política exterior de la Unión coherente y efectiva en materia de PNR.

Los intercambios amparados por el Reglamento Prüm son utilizados diariamente por la policía para luchar contra la delincuencia organizada, las drogas, el terrorismo, la explotación sexual y la trata de seres humanos. La propuesta de Reglamento relativo al intercambio automatizado de datos para la cooperación policial («Prüm II»)[46] revisa el marco vigente de Prüm con el fin de colmar las lagunas de información e impulsar la prevención, detección e investigación de infracciones penales en la Unión. Las normas revisadas sobre el intercambio automatizado de datos para la cooperación policial completan las propuestas de cooperación policial del presente mandato, así como la Recomendación del Consejo, ya adoptada, que refuerza la cooperación transfronteriza operativa y la Directiva relativa al intercambio de información entre las autoridades policiales. La rápida adopción y aplicación de estos instrumentos conexos mejoraría, facilitaría y aceleraría el intercambio de datos entre las autoridades policiales y ayudaría a identificar a los delincuentes.

Sistema de gestión de fronteras plenamente interoperable para un espacio Schengen seguro, fuerte, digital y unido

El buen funcionamiento del espacio Schengen sin fronteras interiores depende de la confianza mutua entre los Estados miembros. Esto, a su vez, se basa en controles eficientes, ya sea en las fronteras exteriores de la Unión o en forma de medidas alternativas en el territorio de los Estados miembros. La modificación propuesta por la Comisión al Código de fronteras Schengen[47] establece la manera en que los Estados miembros pueden hacer un mejor uso de las alternativas a los controles en las fronteras interiores, que pueden ofrecer un alto nivel de

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784.
[47] COM(2021) 891.

seguridad. Es importante que la modificación del Código de fronteras Schengen se adopte y aplique plenamente para garantizar un nivel de seguridad elevado y proporcionado dentro del espacio Schengen. Se sigue desarrollando una nueva arquitectura de los sistemas de información de la Unión para apoyar mejor el trabajo de las autoridades nacionales encaminado a garantizar la seguridad y la gestión de las fronteras. Comprende el Sistema de Información Schengen renovado, el Sistema Europeo de Información y Autorización de Viajes, el Sistema de Entradas y Salidas, la actualización del Sistema de Información de Visados y el marco de interoperabilidad para interconectar los sistemas con plena seguridad. Una vez completada, esta nueva arquitectura proporcionaría a las autoridades nacionales información sobre seguridad más completa y fiable. Todos los componentes del marco de interoperabilidad son esenciales, lo que significa que un retraso en un aspecto o en un Estado miembro daría lugar a un retraso en el despliegue en todos los Estados. Los retrasos en el desarrollo técnico del Sistema de Entradas y Salidas deben reducirse al mínimo, de modo que dicho sistema pueda empezar a funcionar lo antes posible y puedan establecerse todos los elementos clave del marco de interoperabilidad.

La propuesta de control[48] reforzaría la seguridad en el espacio Schengen al crear normas uniformes relativas a la identificación de los nacionales de terceros países que no cumplan las condiciones de entrada a que se refiere el Código de fronteras Schengen y someterlos a los controles sanitarios y de seguridad en las fronteras exteriores. El sistema Eurodac propuesto respaldaría estos objetivos indicando aquellos casos en que, tras el control, se estime que una persona pueda suponer una amenaza para la seguridad interior. Esto, a su vez, facilitaría la aplicación de la propuesta de Reglamento sobre la gestión del asilo y la migración. La Comisión anima a los colegisladores a concluir rápidamente las negociaciones sobre estos expedientes antes de que finalice la actual legislatura.

Lucha contra la corrupción

La corrupción es muy perjudicial para nuestras democracias, la economía y nuestra seguridad, ya que actúa como medio habilitador de la delincuencia organizada y las injerencias extranjeras hostiles. Prevenir y combatir con éxito la corrupción es esencial tanto para salvaguardar los valores de la Unión y la efectividad de sus políticas como para sustentar el Estado de Derecho y la confianza en quienes gobiernan y en las instituciones públicas. Tal como anunció la presidenta Von der Leyen en el discurso sobre el estado de la Unión de 2022, la Comisión adoptó el 3 de mayo de 2023 un paquete de medidas de lucha contra la corrupción[49]**.** La propuesta de Directiva de la Comisión relativa a la lucha contra la corrupción incluye normas reforzadas que tipifican los delitos de corrupción y armonizan las sanciones en toda la Unión. Asimismo, permite investigaciones y enjuiciamientos efectivos y presta especial atención a la prevención y a la creación de una cultura de integridad en la que no se tolera la corrupción. Los debates sobre esta propuesta han comenzado en el Parlamento Europeo y en el Consejo. Además, se invita a los Estados miembros a aplicar las recomendaciones derivadas del pilar de lucha contra la corrupción del Informe sobre el Estado de Derecho de 2023, adoptado el 5 de julio de 2023. Otra propuesta del Alto Representante, apoyada por la Comisión, crearía un régimen de sanciones de la política exterior y de seguridad común (PESC) específico para combatir los actos graves de corrupción en todo el mundo.

Refuerzo de los derechos de las víctimas

[48] COM(2020) 612.
[49] COM(2023) 234.

El 12 de julio de 2023, la Comisión propuso modificaciones de la Directiva sobre los derechos de las víctimas para reforzar el acceso de estas a la información, el apoyo y la protección, la participación en procesos penales y la indemnización. Uno de los objetivos generales de la revisión es contribuir a un alto nivel de seguridad creando un entorno más seguro para las víctimas a fin de fomentar la denuncia de delitos, reduciendo los temores a represalias.

La Comisión insta al Parlamento Europeo y al Consejo a que concluyan las negociaciones interinstitucionales, con carácter urgente y en cualquier caso antes de que finalice el mandato del actual Parlamento, sobre los siguientes expedientes pendientes:

- Propuesta sobre el Reglamento Prüm II;
- Propuestas sobre información anticipada sobre los pasajeros (API);
- Propuestas sobre la lucha contra la corrupción y, en particular, para establecer un régimen de sanciones específico en el marco de la política exterior y de seguridad común (PESC);
- Propuesta de modificación del Reglamento sobre el Código de fronteras Schengen;
- Propuesta de Directiva sobre los derechos de las víctimas;
- Propuesta de control.

La Comisión insta a los Estados miembros a:

- garantizar la entrada en vigor del Sistema de Entradas y Salidas a la mayor brevedad para completar la aplicación de la arquitectura de la Unión en materia de intercambio de información.

VI. Ejecución

Garantizar la seguridad de Europa en su conjunto es una responsabilidad común en la que todos los agentes deben cumplir con su cometido. Esto abarca desde la adopción de nuevas normas de la Unión sólidas, exhaustivas y prácticas por parte del Parlamento Europeo y los colegisladores hasta la transposición e implementación oportunas de dichas normas por parte de los Estados miembros, así como el trabajo operativo llevado a cabo sobre el terreno por una serie de autoridades, organizaciones y partes interesadas. Las agencias de la Unión en los ámbitos de la justicia, los asuntos de interior y la ciberseguridad también desempeñan un papel clave, que ha aumentado con la reciente ampliación de sus responsabilidades.

Mejora del control de los beneficiarios de financiación de la Unión

Al ejecutar el presupuesto de la Unión, la Comisión tiene la responsabilidad de garantizar que los beneficiarios de la financiación de la Unión respeten los valores de esta. Los mecanismos y sistemas de control que determinan quién puede beneficiarse de financiación de la Unión ya son de por sí sólidos, y la negociación en curso relativa a la refundición del Reglamento Financiero también pretende dotar a la Comisión de medios jurídicos más contundentes para actuar en caso necesario. Además, la Comisión está trabajando en formas de optimizar el control de los beneficiarios actuales y posibles beneficiarios futuros de financiación de la Unión, mejorando para ello las orientaciones sobre las obligaciones relativas al respeto de los valores de la Unión y las consecuencias de vulnerarlos. Ello permitirá aclarar las responsabilidades tanto de los beneficiarios como de los que llevan a cabo controles a escala de la Unión, y puede servir como referencia en el ámbito nacional. En caso de incumplimiento de las condiciones de financiación, la Comisión no duda ni dudará en poner fin a la cooperación con los beneficiarios del proyecto en cuestión y en recuperar los fondos en caso necesario. Es importante que los Estados miembros compartan de forma proactiva información con la Comisión cuando

adviertan posibles riesgos con respecto a las organizaciones que solicitan financiación de la Unión.

Infracciones

En el ámbito de la seguridad, la Comisión ha llevado a cabo numerosos procedimientos de infracción. Por ejemplo, en 2023 se incoó un gran número de procedimientos de infracción por incumplimiento de las obligaciones derivadas del Reglamento de 2021 sobre la lucha contra la difusión de contenidos terroristas en línea (dieciséis Estados miembros)[50], y a lo largo de los años 2022 y 2023, veinte Estados miembros recibieron cartas de emplazamiento adicionales debido a la ejecución incorrecta de la Directiva de 2011 relativa a la lucha contra el abuso sexual de los menores[51]. Un número significativo de procedimientos de infracción siguen abiertos por motivo de no conformidad de la legislación nacional con la Directiva de 2017 relativa a la lucha contra el terrorismo[52] y por la falta de transposición de normas que facilitan el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de determinados delitos[53]. Otros de los ámbitos en los que están en curso procedimientos de infracción son la legislación sobre armas de fuego; las normas sobre las sustancias psicoactivas utilizadas en las drogas; la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo; la lucha contra el blanqueo de capitales; el intercambio de antecedentes penales entre los Estados miembros de la Unión y la Directiva sobre los derechos de las víctimas. Los Estados miembros que aplican las iniciativas y acciones acordadas han recibido apoyo (técnico y financiero), y la Comisión sigue a disposición de los Estados miembros para trabajar en la optimización de la ejecución.

Seguimiento a través de las evaluaciones de Schengen y su nuevo sistema de gobernanza

El mecanismo de evaluación y seguimiento de Schengen ha seguido contribuyendo a la ejecución efectiva de las normas de Schengen destinadas a mejorar la seguridad en el espacio sin controles internos. En 2023, se llevaron a cabo las primeras evaluaciones en el marco del mecanismo reforzado de evaluación y seguimiento de Schengen, las cuales permitieron la identificación y subsanación oportunas de las vulnerabilidades estratégicas, que tienen un impacto transfronterizo en la seguridad y la protección en el seno de la Unión. Además, en 2023, la Comisión puso en marcha una evaluación temática de Schengen para examinar las prácticas de los Estados miembros que se enfrentan a retos similares en la lucha contra el tráfico de drogas en la Unión, en especial el de gran volumen. Estas evaluaciones introdujeron un enfoque reforzado y más exhaustivo de los elementos de seguridad de Schengen. Sobre la base de los resultados de las evaluaciones periódicas, temáticas y sin previo aviso de Schengen, el Consejo estableció en junio de 2023 las prioridades para el ciclo de Schengen 2023-2024. Establece ámbitos de interés en los que se deben redoblar los esfuerzos en pos de un espacio Schengen más seguro y más fuerte. Una aplicación eficaz y rápida de estas prioridades, unida a una mayor coordinación de las políticas del Consejo Schengen, reforzará aún más la lucha contra la delincuencia organizada y maximizará la cooperación operativa transfronteriza.

[50] Reglamento (UE) 2021/784 sobre la lucha contra la difusión de contenidos terroristas en línea.

[51] Directiva 2011/93/UE relativa a la lucha contra los abusos sexuales de los menores.

[52] Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo.

[53] Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo.

El papel de las agencias y los organismos de la Unión

La asociación es clave para la aplicación de las iniciativas de la Unión de la Seguridad, ya que para obtener resultados concretos se precisa la labor de las diferentes autoridades y organismos nacionales y europeos. Por ejemplo, la plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT) permite una cooperación multidisciplinar estructurada entre Estados miembros, con el apoyo de todas las instituciones, órganos y organismos de la Unión (como Europol, Frontex, Eurojust, CEPOL, OLAF, eu-LISA). Las operaciones llevadas a cabo por la plataforma EMPACT, en particular a través de grupos operativos específicos, coordinan los esfuerzos de los Estados miembros y de los socios operativos en la lucha contra las redes delictivas y la delincuencia grave. Solo en 2022, la plataforma EMPACT dio lugar a un total de 9 922 detenciones, más de 180 millones EUR en activos y efectivo incautados, 9 263 investigaciones iniciadas, 4 019 víctimas identificadas, más de 62 toneladas de drogas incautadas, 51 objetivos de alto valor identificados y 12 detenidos, así como operaciones en el contexto de la guerra de agresión contra Ucrania, en particular para hacer frente a la trata de seres humanos y las amenazas relacionadas con armas de fuego.

Frontex, la Agencia Europea de Seguridad Marítima (AESM) y la Agencia Europea de Control de la Pesca (AECP) siguen reforzando su cooperación en las funciones de guardacostas para ayudar a las autoridades nacionales a aumentar la seguridad y la protección en el mar. Estas agencias contribuirán en gran medida a la implementación de la Estrategia de Seguridad Marítima de la Unión.

Varias iniciativas de la Unión de la Seguridad han encomendado nuevas responsabilidades y tareas a las agencias pertinentes, a veces con efectos en los recursos humanos.

Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Por lo que se refiere a la preparación y la respuesta a incidentes para mejorar la ciberseguridad, la Comisión ha establecido una acción a corto plazo para apoyar a los Estados miembros, transfiriendo fondos del programa Europa Digital a la **Agencia de la Unión Europea para la Ciberseguridad (ENISA)** a los efectos de reforzar la preparación y las capacidades de respuesta a incidentes cibernéticos graves. La propuesta de Ley de Cibersolidaridad adoptada en abril de 2023 se basa en esta acción y, una vez adoptada por los colegisladores, puede encomendar a ENISA tareas adicionales, como el funcionamiento y la administración de la futura reserva de ciberseguridad de la Unión o la preparación de un informe de revisión de incidentes tras incidentes de ciberseguridad a gran escala. La propuesta de Ley de Ciberresiliencia encargaría a ENISA la tarea de recibir notificaciones de los fabricantes sobre vulnerabilidades en productos con elementos digitales e incidentes que afecten a la seguridad de dichos productos, y transmitírselas a los CSIRT pertinentes o a los puntos de contacto únicos oportunos de los Estados miembros. También se espera que ENISA elabore un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en los productos con elementos digitales y lo presente al Grupo de Cooperación SRI.

El Centro Europeo de Competencia en Ciberseguridad

El **Centro Europeo de Competencia en Ciberseguridad (ECCC)**, junto con la Red de Centros Nacionales de Coordinación (CNC), es el nuevo organismo de la Unión encargado de apoyar la innovación y la política industrial en materia de ciberseguridad. Este ecosistema reforzará las capacidades de la comunidad tecnológica de ciberseguridad, mantendrá la excelencia en la investigación y reforzará la competitividad de la industria de la Unión en este ámbito. El ECCC y los CNC tomarán decisiones de inversión estratégica y pondrán en común recursos de la Unión, de sus Estados miembros e, indirectamente, de la industria para mejorar y reforzar las capacidades tecnológicas y de ciberseguridad industrial. Por lo tanto, el ECCC tiene una función fundamental que desempeñar en la consecución de los ambiciosos objetivos de ciberseguridad de los programas Europa Digital y Horizonte Europa.

El ECCC ya ha contratado a más de la mitad de su personal y pronto contratará a su director/a ejecutivo/a. El trabajo ya en curso incluye la parte relativa a la ciberseguridad del programa DIGITAL y una nueva agenda estratégica[54] para el desarrollo y el despliegue de tecnología que establece acciones prioritarias para apoyar a las pymes en el desarrollo y el uso de tecnologías, servicios y procesos estratégicos de ciberseguridad; apoyar y aumentar la mano de obra profesional; y reforzar los conocimientos especializados en investigación, desarrollo e innovación en el ecosistema europeo de ciberseguridad en un sentido más amplio.

Europol

Con un nuevo mandato, **Europol** estará mejor preparada para apoyar a los Estados miembros en la lucha contra la delincuencia organizada. La lucha contra el tráfico de drogas es una prioridad clave, habida cuenta de su importancia e impacto negativo crecientes en la seguridad de los ciudadanos de la Unión. Tras la autorización del Consejo de la Unión Europea el 15 de mayo de 2023, la Comisión ha estado trabajando activamente en la celebración de acuerdos internacionales con Bolivia, Brasil, Ecuador, México y Perú sobre el intercambio de datos personales con Europol con el fin de prevenir y combatir la delincuencia grave y el terrorismo.

Eurojust

Con sus más de veinte años de experiencia prestando apoyo judicial a las autoridades nacionales para luchar contra una amplia variedad de delitos transfronterizos graves y complejos, **Eurojust** ha afianzado su posición en el espacio de libertad, seguridad y justicia de la Unión. Para reforzar la cooperación en todos los ámbitos, la Comisión está negociando acuerdos internacionales para facilitar la colaboración entre Eurojust y trece terceros países con el propósito de intercambiar datos personales para luchar contra la delincuencia organizada y el terrorismo[55]. Las negociaciones con Armenia y Líbano ya han concluido, están en curso con Argelia y Colombia y han comenzado con Bosnia y Herzegovina. La Comisión anima al Parlamento Europeo y al Consejo a celebrar acuerdos con estos países antes de que finalice la legislatura, a fin de reforzar la cooperación judicial transnacional y ampliar la lucha contra la delincuencia transfronteriza.

La Fiscalía Europea

Desde el inicio de sus actividades operativas en junio de 2021, la **Fiscalía Europea** ha demostrado ser una poderosa herramienta del conjunto de instrumentos de la Unión para investigar y enjuiciar los delitos que afectan al presupuesto de la Unión, incluidos aquellos relacionados con la participación en una organización delictiva que se enfocan como delitos contra el presupuesto de la Unión. La Comisión anima a los Estados miembros que aún no participan en la cooperación reforzada de la Fiscalía Europea a que lo hagan lo antes posible a

[54] https://cybersecurity-centre.europa.eu/strategic-agenda_en.

[55] Argelia, Argentina, Armenia, Bosnia y Herzegovina, Brasil, Colombia, Egipto, Israel, Jordania, Líbano, Marruecos, Túnez y Turquía.

fin de aprovechar todo el potencial que esta brinda en lo que respecta a la protección del dinero de los contribuyentes de la Unión.

EUDA

Con un nuevo mandato adoptado por los colegisladores en junio de 2023, el Observatorio Europeo de las Drogas y las Toxicomanías (OEDT) se convertirá en una agencia de pleno derecho —la **Agencia de la Unión Europea para las Drogas (EUDA)**— con funciones reforzadas. La Agencia podrá evaluar de manera más exhaustiva los nuevos retos en materia de salud y seguridad que plantean las drogas ilícitas, así como contribuir de manera más eficaz al trabajo de los Estados miembros y a escala internacional. La recogida, el análisis y la difusión de datos seguirán siendo la principal tarea de la Agencia, pero el mandato reforzado también le permitirá desarrollar capacidades generales de evaluación de amenazas para la salud y la seguridad con el fin de detectar amenazas emergentes como el consumo simultáneo de sustancias, reforzar su cooperación a través de puntos focales nacionales y establecer una red de laboratorios que le proporcionen información forense y toxicológica. Esto ayudará a la Agencia a emitir alertas cuando aparezcan en el mercado sustancias especialmente peligrosas y a aumentar la sensibilización.

La Comisión insta al Parlamento Europeo y al Consejo a que concluyan las negociaciones interinstitucionales, con carácter urgente y en cualquier caso antes de que finalice el mandato del actual Parlamento, sobre los siguientes expedientes pendientes:

- Propuesta de refundición del Reglamento Financiero.

La Comisión insta a los Estados miembros a:

- compartir de forma proactiva información con la Comisión cuando aprecien posibles riesgos con respecto a las organizaciones que solicitan financiación de la Unión;
- aplicar sin demora las prioridades del ciclo de Schengen 2023-2024 para lograr un espacio Schengen más seguro y más fuerte;
- abordar los procedimientos de infracción incoados contra ellos con el fin de garantizar la correcta transposición de la legislación en cuestión.

VII. Conclusión

Los últimos tres años se han caracterizado por un esfuerzo constante y decidido para dar vida a la ambición de crear una Unión de la Seguridad para la UE. Se han realizado grandes avances en todo el ámbito de la política de seguridad. En el momento actual, la realidad cambiante de las amenazas requiere esfuerzos continuos con una motivación renovada. Los trabajos sobre el marco legislativo deben concluirse a su debido tiempo, antes de que finalice la legislatura en la primavera de 2024. Los Estados miembros tienen la responsabilidad constante de transponer, ejecutar y aplicar nuevas leyes. La ejecución requiere esfuerzos concertados, también con el apoyo de las agencias de la Unión, y muy a menudo una cooperación cada vez más estrecha con nuestros socios internacionales.

Sin los esfuerzos colectivos y decididos de todas las partes interesadas no alcanzaremos los niveles de seguridad y protección de la Unión que esperan los ciudadanos y, en las

circunstancias actuales, debería ser prioritario que todos los actores desempeñen su papel en el refuerzo de la seguridad de la Unión.