Consejo de la Unión Europea

Bruselas, 6 de diciembre de 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
A:	Delegaciones
Asunto:	Conclusiones del Consejo sobre la ENISA

Adjunto se remite a la atención de las delegaciones las Conclusiones del Consejo sobre la ENISA, adoptadas por el Consejo en su sesión del 6 de diciembre de 2024.

ANEXO

Proyecto de Conclusiones del Consejo sobre la ENISA

EL CONSEJO DE LA UNIÓN EUROPEA,

1. PONE DE RELIEVE que los retos derivados del ciberespacio global nunca habían sido tan complejos, diversos y graves como lo son ahora, debido a la sofisticación de las ciberamenazas emergentes, a la constante evolución del entorno de seguridad y a las tensiones geopolíticas actuales. Por lo tanto, la UE y sus Estados miembros no deben cejar en su esfuerzo por ser más resilientes para detectar y afrontar con eficacia las amenazas y los retos actuales y emergentes. HACE HINCAPIÉ en que se debe seguir trabajando para conseguir un mayor grado de ciberresiliencia, con un enfoque que implique a toda la sociedad. DESTACA que, en los próximos años, la UE y sus Estados miembros deben centrarse en la ejecución efectiva de las iniciativas legislativas y no legislativas que sustenten todas las medidas al respecto adoptadas hasta la fecha y contribuyan a ellas.

2. RECORDANDO que la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro, TOMA CONSTANCIA de que la UE y sus Estados miembros han colaborado en sumo grado en los últimos años para establecer la configuración institucional y las formas de colaboración necesarias en el ámbito cibernético tanto a escala nacional como a escala de la UE. VALORA POSITIVAMENTE las diversas iniciativas legislativas y no legislativas que han proporcionado a la Unión y a sus Estados miembros un marco firme y sólido en este ámbito, lo que aumenta la ciberresiliencia general de la Unión. Ese marco ha ido evolucionando hasta abarcar varios aspectos del ámbito cibernético: la seguridad, la diplomacia, la aplicación de las leyes y la defensa. SEÑALA que un gran número de agentes, entre ellos las autoridades de ciberseguridad de los Estados miembros, el Grupo de Cooperación SRI, la red de CSIRT, la red europea de organizaciones de enlace para crisis cibernéticas (CyCLONe), la Red de Centros Nacionales de Coordinación, el Grupo Europeo de Certificación de la Ciberseguridad (GECC), la Comisión, el Servicio Europeo de Acción Exterior (SEAE), la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Centro Europeo de Competencia en Ciberseguridad, el CERT-EU, la Agencia Europea de Defensa (AED) y el Centro Europeo de Ciberdelincuencia (EC3) de Europol forman parte del ecosistema de ciberseguridad de la UE, y cada uno de ellos cumple su función en la aplicación del marco de ciberseguridad a escala de la UE.

3. RECONOCE que, en las dos últimas décadas, la ENISA ha demostrado ser una entidad de valor inestimable en el ecosistema europeo de la ciberseguridad, ejerciendo una función crucial al ayudar de forma activa a los Estados miembros y a las instituciones, órganos y organismos de la UE a que apliquen y desarrollen políticas de ciberseguridad, desarrollen capacidades y aumenten su preparación, cooperen y fomenten la concienciación y la certificación en materia de ciberseguridad.

RECOMENDACIONES DE ACTUACIÓN DE CARÁCTER GENERAL

4. INVITA a la Comisión a que aproveche la oportunidad que constituye la **evaluación del Reglamento sobre la Ciberseguridad** para examinar cómo puede contribuir a simplificar el complejo ecosistema de la ciberseguridad y mejorar así la eficacia y el uso eficiente de los recursos. Por consiguiente, INSTA a la Comisión a que vele por que el mandato de la ENISA para apoyar a los Estados miembros y a las instituciones, órganos y organismos de la UE sea preciso y esté definido claramente, con objetivos estratégicos concretos y un orden de prioridad en las tareas, además de una división más afinada entre sus tareas y competencias y las de otros agentes. A este respecto, INVITA a la Comisión a que examine y refuerce en mayor medida la función que cumple la ENISA en apoyo a la cooperación operativa a escala de la UE y entre los Estados miembros para mejorar la ciberresiliencia, teniendo en cuenta las competencias de los Estados miembros en este ámbito. Además, INSTA a la Comisión a que refuerce la función consultiva de la ENISA de proporcionar orientaciones y recomendaciones expertas y basadas en datos contrastados acerca de la aplicación de las iniciativas legislativas y no legislativas actuales y futuras de la UE asegurando al mismo tiempo la coherencia del marco de ciberseguridad de la UE.

5. Con esa misma intención, ANIMA a la Comisión a que considere la posibilidad de racionalizar el papel de la ENISA en lo que respecta a las tareas que no son parte fundamental de su misión. SUBRAYA que iniciativas legislativas recientes, como la Directiva SRI 2, el Reglamento de Ciberresiliencia y el Reglamento de Cibersolidaridad, entre otras, **han ampliado sustancialmente las responsabilidades** de la ENISA. Si bien SEÑALA que la ENISA obtuvo recursos adicionales a resultas de algunas de estas iniciativas, PONE DE RELIEVE que la ampliación de las responsabilidades de la Agencia y la creciente complejidad de las ciberamenazas y los retos cibernéticos han provocado un aumento considerable de sus tareas, lo que debería traducirse en unos **recursos** humanos, financieros y técnicos **adecuados** para que pueda ejecutar plenamente todas las tareas que le competen, sin ánimo de anticipar la negociación del marco financiero plurianual. A tal fin, INSTA a la Comisión a que, cuando prepare el proyecto de presupuesto general de la Unión, jerarquice las acciones y confiera prioridad a las tareas relativas al apoyo a los Estados miembros en la mejora de su ciberresiliencia, su cooperación operativa y el desarrollo y la aplicación del Derecho de la Unión.

APOYO DE LA ENISA AL DESARROLLO Y LA APLICACIÓN DE POLÍTICAS

6. RECUERDA que, en el marco jurídico vigente en materia de ciberseguridad, la ENISA tiene atribuidas varias responsabilidades fundamentales de apoyo y asesoramiento en toda la UE. VALORA POSITIVAMENTE a este respecto la función de la ENISA de prestar **asistencia a los Estados miembros** en la aplicación efectiva de iniciativas legislativas y no legislativas. INSTA a la ENISA a que, en estrecha cooperación con el Grupo de Cooperación SRI y con la Comisión, siga proporcionando información y análisis generales sobre el entorno jurídico actual referente a la ciberseguridad. ANIMA a la ENISA a que comparta y promueva activamente, de manera periódica y estructurada, orientaciones técnicas y mejores prácticas que ayuden a los Estados miembros a aplicar la política y la legislación en materia de ciberseguridad.

7. RECONOCE el papel crucial que desempeña la ENISA en el desarrollo de los **esquemas europeos de certificación de la ciberseguridad** al afianzar la confianza en los productos, servicios y procesos de las TIC y también en los servicios de seguridad gestionados con vistas a la próxima modificación específica del Reglamento sobre la Ciberseguridad. DESTACA que a los Estados miembros y a la industria les preocupa el prolongado proceso de selección, elaboración y adopción de los esquemas de certificación de la ciberseguridad; por lo tanto, INSTA a la Comisión a que aproveche la oportunidad que constituye la evaluación del Reglamento sobre la Ciberseguridad para encontrar formas de adoptar un enfoque más sencillo, basado en el riesgo, más transparente y más rápido para el desarrollo de los esquemas europeos de certificación de la ciberseguridad, sin dejar de DESTACAR el importante papel de los Estados miembros en este proceso. Además, PONE DE RELIEVE la importancia de atribuir explícitamente la responsabilidad del mantenimiento de cada uno de los esquemas de certificación. Por otra parte, RECUERDA que la ENISA, cuando prepare las propuestas de esquemas, debe consultar a todas las partes interesadas pertinentes en tiempo oportuno mediante un proceso formal, abierto, transparente e inclusivo, y que la Comisión debe realizar una consulta de manera abierta, transparente e inclusiva cuando evalúe la eficiencia y la utilización de los esquemas adoptados. ANIMA a la ENISA a que refuerce en mayor medida la colaboración con la comunidad de la protección de datos, en particular con el Comité Europeo de Protección de Datos, cuando proceda, y con las autoridades nacionales competentes, prestando especial atención a fomentar sinergias en el contexto del desarrollo de futuros esquemas europeos de certificación de la ciberseguridad.

8. Para evitar la carga administrativa innecesaria que podría derivarse de un marco de comunicación complejo, INSTA a la ENISA a que, en cooperación con la Comisión, siga intercambiando información con los Estados miembros sobre los aspectos prácticos, la simplificación y la racionalización del procedimiento de comunicación de información. Además, RECUERDA su invitación a la Comisión para que elabore, con el apoyo de la ENISA y de otras entidades pertinentes de la UE, un inventario de las obligaciones de comunicación de información pertinentes establecidas en los respectivos actos legislativos de la UE en materia de cuestiones cibernéticas y digitales. RECUERDA que el intercambio de información entre la ENISA y los Estados miembros se basa en una relación de confianza en la que la seguridad y la confidencialidad están garantizadas en virtud del Reglamento sobre la Ciberseguridad y de las normas y protocolos pertinentes, y que debe limitarse a lo que sea relevante y proporcionado para la finalidad del intercambio. HACE HINCAPIÉ en la necesidad de que los datos y la información se traten con la debida diligencia.

9. PONE DE RELIEVE que, con arreglo al Reglamento de Ciberresiliencia, la ENISA es la encargada de crear y mantener **la plataforma única de notificación**, que tendrá un valor añadido operativo concreto, especialmente para las vulnerabilidades aprovechadas activamente y los incidentes graves que afecten a la seguridad de los productos con elementos digitales. Habida cuenta de la amplitud del ámbito de aplicación de esta legislación horizontal, la plataforma única de notificación debe ser una herramienta eficaz y segura para facilitar el intercambio de información entre los CSIRT nacionales y la ENISA. Por consiguiente, INSTA a la ENISA a que, además de asignar recursos humanos suficientes, acelere la creación de la plataforma como prioridad fundamental para asegurarse de que esté preparada en el plazo fijado en el Reglamento de Ciberresiliencia.

10. TOMA CONSTANCIA del papel de la ENISA en la creación de una **base de datos europea de vulnerabilidades**, cuyo objetivo es mejorar la transparencia relativa a la divulgación de vulnerabilidades velando al mismo tiempo por el tratamiento adecuado de los datos confidenciales. Teniendo en cuenta el término del período de transposición de la Directiva SRI 2, INSTA a la ENISA a que acelere todos los trabajos necesarios para asegurar el correcto funcionamiento de esta base de datos. Al mismo tiempo, INVITA al Grupo de Cooperación SRI a que, con la asistencia de la ENISA, publicite en mayor medida las orientaciones, las políticas y los procedimientos sobre la divulgación de vulnerabilidades.

11. RECONOCE los beneficios de la **acción de apoyo a la ciberseguridad** que realiza la ENISA, que funciona como un conjunto de servicios de ciberseguridad que se ofrece a los Estados miembros para complementar la labor de estos, así como la experiencia que ha adquirido la ENISA con su ejecución. A este respecto, PONE DE RELIEVE que la ENISA debe desempeñar una función central en la administración y el funcionamiento de la Reserva de Ciberseguridad de la UE. INVITA a la ENISA a que empiece a catalogar los servicios necesarios y su disponibilidad inmediatamente después de la entrada en vigor del Reglamento de Cibersolidaridad, con el fin de que la Reserva de Ciberseguridad de la UE sea lo más útil y esté lo más adaptada posible a las necesidades de los usuarios en todos los Estados miembros. INVITA a la ENISA a que, una vez que se le atribuya esta función, implique a los Estados miembros, concretamente recabando información sobre los criterios necesarios e informando sobre las próximas licitaciones, en una fase temprana del proceso de creación de la Reserva de Ciberseguridad de la UE. INVITA a la ENISA a que, una vez que se le atribuya esta función, se asegure de que el proceso de selección de los proveedores de confianza de servicios de seguridad gestionados sea transparente, abierto y ecuánime y propicie la participación de proveedores procedentes de todos los Estados miembros, independientemente de su tamaño. Además, RECUERDA que la ENISA debe emitir, sin demora indebida, las directrices de interoperabilidad para los centros cibernéticos transfronterizos.

12. SUBRAYA que el **seguimiento de las tendencias sobre las tecnologías emergentes** en un ámbito en rápida evolución como el de la ciberseguridad tiene una importancia capital para mantener y seguir reforzando nuestra postura de ciberseguridad. RECONOCE la labor realizada por la ENISA para señalar a la atención pública los riesgos y las posibilidades que entrañan tecnologías como la inteligencia artificial y la computación cuántica, facilitando así una mejor comprensión de los retos actuales. ANIMA a la ENISA a que contribuya en mayor medida a estas tareas, aliente de forma activa a la aplicación de sus recomendaciones y asesore al Centro Europeo de Competencia en Ciberseguridad y colabore con él, cuando proceda.

APOYO DE LA ENISA A LOS ESTADOS MIEMBROS PARA MEJORAR LA CIBERRESILIENCIA Y LA COOPERACIÓN OPERATIVA

13. DESTACA que la ENISA cumple una importante función **como secretaría de las dos redes de cooperación cibernética de la UE impulsadas por los Estados miembros, la red de CSIRT y CyCLONe**. HACE HINCAPIÉ en la valiosa participación de la ENISA en el Grupo de Cooperación SRI, concretamente con su intervención activa y sus contribuciones técnicas en las distintas líneas de trabajo. ANIMA a la ENISA a que siga apoyando en el futuro el funcionamiento y la cooperación de estas redes, ya que constituyen canales fundamentales para que los Estados miembros colaboren en distintos niveles.

14. REITERA la necesidad de mejorar el **conocimiento común de la situación** a escala de la UE, que contribuye a la postura de ciberseguridad de la UE junto a la detección, la prevención y la respuesta a incidentes de ciberseguridad. A este respecto, DESTACA la importancia de las actividades de prospectiva, los informes periódicos y las evaluaciones de amenazas de la ENISA, todo lo cual contribuye a mejorar el conocimiento de la situación. ANIMA a la ENISA a que trabaje en estrecha cooperación con los Estados miembros para contribuir a desarrollar el conocimiento de la situación a escala de la UE. En este contexto, RECONOCE la importante función que desempeña la ENISA, junto con el CERT-EU y Europol, de apoyar al Consejo, en el contexto del conjunto de instrumentos de ciberdiplomacia, con sesiones informativas sobre la situación como complemento al conocimiento de la situación que proporciona la Capacidad Única de Análisis de Inteligencia (SIAC), y DESTACA la necesidad de elaborar una panorámica completa de las amenazas a partir de diversas fuentes, entre ellas el sector privado. A este respecto, ABOGA por que siga desarrollándose la cooperación de la ENISA con el SEAE, y en particular con el INTCEN, respetando plenamente sus mandatos respectivos.

15. PONE DE RELIEVE que el Centro de Análisis y Situación Cibernéticos de la Comisión cumple una función interna dentro de la Comisión y se sustenta en su colaboración con la ENISA y el CERT-EU. INVITA a la Comisión a que, al objeto de generar el máximo potencial de sinergias y reducir la complejidad dentro del ecosistema de la ciberseguridad de la UE, tenga en cuenta los resultados de la evaluación del Reglamento sobre la Ciberseguridad, así como los debates sobre la evaluación del Plan Director Cibernético, a fin de racionalizar las tareas del Centro de Análisis y Situación Cibernéticos de la Comisión y las tareas conexas de la ENISA. ANIMA a la Comisión a que evite la duplicación innecesaria de tareas, salvaguardando al mismo tiempo la función primordial de la ENISA de contribuir al desarrollo de un conocimiento común de la situación a escala de la Unión en apoyo de los Estados miembros, respetando debidamente sus competencias nacionales.

16. DESTACA que el desarrollo de un conocimiento común de la situación es una condición indispensable para una gestión oportuna y eficaz de las crisis por parte de la Unión en su conjunto. SUBRAYA que, a escala de la Unión, una serie de agentes clave participan en **la respuesta a ciberincidentes a gran escala** y que, en caso de que se produzcan tales ciberincidentes, la cooperación eficaz entre los Estados miembros se sustenta principalmente en la red de CSIRT y en CyCLONe. La ENISA, como secretaría de la red de CSIRT y de CyCLONe, cumple una importante función en la gestión de crisis cibernéticas. INVITA a la Comisión a que utilice la evaluación del Plan Director Cibernético para reflejar adecuadamente las tareas y las responsabilidades adicionales orientadas a contribuir al desarrollo de una respuesta cooperativa a ciberincidentes o crisis cibernéticas transfronterizos a gran escala, y también el papel atribuido a la ENISA como secretaría de la red de CSIRT y de CyCLONe y por la reciente legislación en materia de ciberseguridad.

17. SUBRAYA la importancia de que se organicen **ejercicios** periódicos **de ciberseguridad** que refuercen de forma notable la preparación de la UE para responder a incidentes y crisis. TOMA CONSTANCIA de que la ENISA ha adquirido una valiosa y extensa experiencia en este ámbito en su apoyo a los Estados miembros. TOMA CONSTANCIA de la importante función que desempeña la ENISA en las fases de planificación, preparación, ejecución y evaluación de los ejercicios de ciberseguridad, y HACE HINCAPIÉ en que debe seguir siendo uno de los principales agentes a escala de la UE, teniendo en cuenta que tales ejercicios deben efectuarse sobre la base de marcos estructurados y terminologías comunes. INVITA a la ENISA, a la red de CSIRT y a CyCLONe a que utilicen de forma más eficiente los ejercicios periódicos ya existentes para probar y mejorar el marco de gestión de crisis de la UE y velen por el máximo aprovechamiento de las enseñanzas extraídas.

COOPERACIÓN DE LA ENISA CON OTROS AGENTES DEL ECOSISTEMA DE LA CIBERSEGURIDAD

18. REITERA que, debido al carácter horizontal de la ciberseguridad, la **colaboración entre todos los agentes a escala de los Estados miembros y de la Unión** resulta vital, por lo que RECALCA que para aumentar la ciberresiliencia general a escala europea también se requiere un trabajo conjunto entre la ENISA y otras entidades pertinentes en el ámbito cibernético.

19. SUBRAYA que la capacidad de las instituciones, órganos y organismos de la UE de seguir siendo ciberseguros es de gran importancia para la ciberresiliencia general a escala de la UE, para la cual la función del CERT-EU tiene a su vez un valor inestimable. A este respecto, VALORA POSITIVAMENTE la cooperación estructurada establecida entre el CERT-EU y la ENISA, y los ANIMA a que prosigan en el futuro su estrecha cooperación.

20. Con la autonomía financiera que ha conseguido, el Centro Europeo de Competencia en Ciberseguridad contribuirá de forma notable al desarrollo de un ecosistema europeo sólido de investigación, industria y tecnología cibernéticas que englobe capacidades para el desarrollo de los trabajadores en consonancia con su mandato. ANIMA a la ENISA y al Centro Europeo de Competencia en Ciberseguridad a que prosigan su estrecha cooperación, especialmente en relación con las necesidades y prioridades de investigación e innovación y con las capacidades de ciberseguridad, a fin de aumentar la competitividad de la industria de la ciberseguridad de la Unión. INVITA a la Comisión a que estudie cómo pueden optimizarse en mayor medida las sinergias en el funcionamiento de la ENISA y el Centro Europeo de Competencia en Ciberseguridad y cómo racionalizar mejor las actividades con arreglo a sus mandatos respectivos.

21. SUBRAYA que la presentación de actualizaciones periódicas sobre el panorama de amenazas contribuye a determinar mejor qué medidas e instrumentos se necesitan para combatir la ciberdelincuencia de forma efectiva. PONE DE RELIEVE el valor añadido de los informes de evaluación conjunta cibernética de la UE, que son el resultado de la colaboración conjunta de la ENISA, el EC3 de Europol y el CERT-EU y ya han proporcionado valiosas aportaciones para dar respuesta a los distintos retos, entre ellos la lucha contra la ciberdelincuencia. INVITA a la ENISA y a Europol a que sigan colaborando de manera estructurada en el futuro.

22. DESTACA que la ciberdefensa constituye una parte importante y en constante evolución de la lucha contra las amenazas procedentes del ciberespacio. PONE DE RELIEVE la necesidad de que la ENISA colabore con el SEAE y con la Comisión en aquellos casos en los que la ENISA cumpla una función de apoyo a la aplicación de la política de ciberdefensa de la UE, en estrecha cooperación con la AED, el Centro Europeo de Competencia en Ciberseguridad y la comunidad de la ciberdefensa. HACE HINCAPIÉ en el papel de la ENISA como agencia civil. SUBRAYA la importancia de profundizar en la cooperación cívico-militar en el ámbito cibernético dentro de la UE y racionalizarla, incluyendo una clara división de funciones y responsabilidades entre ambas comunidades, y entre la UE y la OTAN, y respetando plenamente los principios de inclusividad, reciprocidad, apertura mutua y transparencia, así como la autonomía decisoria de ambas organizaciones. ANIMA a la ENISA a que siga persiguiendo acuerdos de colaboración con la Agencia de Comunicaciones e Información de la OTAN.

23. ANIMA a la UE a que siga promoviendo en los foros mundiales nuestros valores comunes y nuestra labor conjunta a fin de salvaguardar un ciberespacio libre, mundial, abierto y seguro. DESTACA que el carácter transfronterizo de las ciberamenazas y los ciberincidentes requiere una colaboración sólida y eficaz no solo a escala de la UE, sino también **con organizaciones y socios internacionales**. SEÑALA que la participación internacional de la ENISA debe centrarse en los socios estratégicos y en los países candidatos a la adhesión a la UE, en consonancia con la política exterior y de seguridad común de la UE. DESTACA que, en su participación internacional, la ENISA debe actuar de conformidad con su mandato y con las disposiciones correspondientes del Reglamento sobre la Ciberseguridad. TOMA CONSTANCIA de la necesidad de aclarar, en consonancia con los procedimientos pertinentes, la participación internacional de la ENISA, velando, en particular, por que su Consejo de Administración esté debidamente informado de las actividades conexas. ABOGA por la participación de la ENISA en los marcos internacionales de cooperación en materia de ciberseguridad que sean pertinentes, entre ellos organizaciones como la OTAN y la OSCE.

24. REITERA que con frecuencia la UE y sus Estados miembros han puesto de relieve los déficits de **capacidades de ciberseguridad**. RECUERDA que la Comisión y la ENISA han introducido un marco amplio de carácter general para proporcionar orientaciones a todas las partes interesadas, como el Marco Europeo de Capacidades en Ciberseguridad, la Comunicación sobre una Academia de Cibercapacidades y la Conferencia Europea de Cibercapacidades, de periodicidad anual, y ANIMA a la Comisión y a la ENISA a que se basen en esas iniciativas, con especial consideración al debate en curso sobre el Consorcio de Infraestructuras Digitales Europeas (EDIC). A tal fin, INVITA a la Comisión a que se ponga en contacto con los Estados miembros que estén interesados en crear un EDIC. TOMA CONSTANCIA DE que tanto la ENISA como el Centro Europeo de Competencia en Ciberseguridad tienen el mandato de fomentar las capacidades en toda la Unión. INVITA a la ENISA a que priorice el apoyo a la labor de los Estados miembros en materia de capacidades y educación, reforzando la concienciación de la opinión pública y a que colabore con el Centro Europeo de Competencia en Ciberseguridad cuando proceda.

25. TOMA CONSTANCIA de que en los últimos años la ENISA ha desarrollado la **cooperación con el sector privado**. RECUERDA que, dado que el sector privado supervisa continuamente el panorama de ciberamenazas, la información recabada por la industria podría contribuir a mejorar el conocimiento común de la situación. Por lo tanto, ANIMA a la ENISA a que, en estrecha cooperación con los Estados miembros y todas las entidades de la UE, potencie la cooperación con el sector privado.

26. INSTA a la Comisión y a la ENISA a que estudien las formas de mejorar la colaboración entre la ENISA y los organismos europeos de **normalización**. DESTACA la necesidad de que la ENISA aumente sus conocimientos especializados sobre normalización de la ciberseguridad europea mediante, entre otras cosas, el seguimiento de las actividades de normalización y la participación en estas.

27. INSTA a la Comisión y a la ENISA a que estudien la manera de seguir optimizando el funcionamiento del marco de ciberseguridad de la UE teniendo en cuenta las recomendaciones y propuestas formuladas en las presentes Conclusiones. La cooperación continua, la jerarquización de tareas y recursos y la simplificación del complejo panorama cibernético serán elementos fundamentales para afrontar los retos actuales y futuros.