INFORME ESPECIAL 19/2026 **ES**

Detección y respuesta ante incidentes relacionados con la ciberseguridad

Progresa el marco de cooperación de la UE, pero es solo parcialmente eficaz por los retrasos en la aplicación y el escaso intercambio de información

CURIA RATIONUM
TRIBUNAL DE CUENTAS EUROPEO

Índice

Apartados

Anexos

Anexo I – Sobre la auditoría

Anexo II – Entorno de ciberseguridad de la UE

Anexo III – Acciones de ciberseguridad seleccionadas

Anexo IV – Evaluación por el Tribunal de Cuentas Europeo de proyectos de ciberseguridad financiados por la UE

Siglas y acrónimos

Glosario

Respuestas de la Comisión

Respuestas del Centro Europeo de Competencia en Ciberseguridad

Respuestas de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Cronología

Equipo auditor

01

Mensajes principales

¿Por qué es importante este ámbito?

01 El riesgo de ciberataques aumenta a medida que nuestra economía y nuestra vida cotidiana se digitalizan. La ciberseguridad se define como «todas las actividades necesarias para la protección de las redes y los sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas»[1]. La ciberseguridad requiere un enfoque holístico de prevención, detección, respuesta y recuperación frente a estas.

02 El entorno de ciberseguridad de la UE afecta a numerosas entidades públicas y privadas regionales, nacionales y de la UE en el ámbito civil. La ciberseguridad es también un elemento clave de la seguridad y la defensa nacionales.

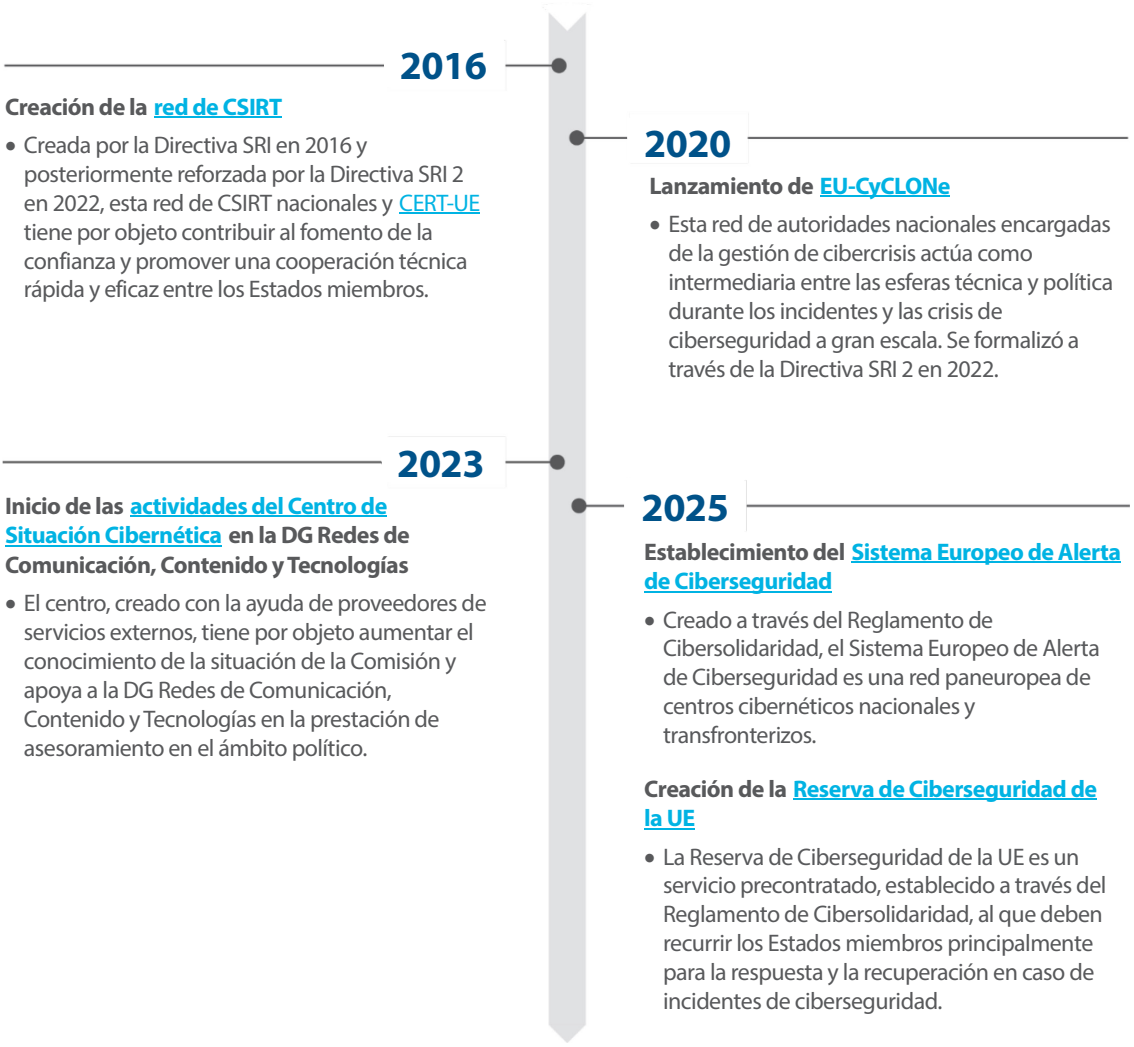
03 Los Estados miembros son los principales responsables de prevenir los incidentes y las crisis de ciberseguridad que les afecten, prepararse para ellos y darles respuesta. Puesto que estos incidentes pueden afectar al buen funcionamiento del mercado interior, la UE también desempeña un papel importante en caso de incidentes o crisis significativos. En los últimos años, la UE ha reforzado el marco regulador de la ciberseguridad[2], en constante evolución, y ha establecido redes y mecanismos, como puede apreciarse en la ***ilustración 1*** y en el ***anexo II***.

---

[1] Reglamento (UE) 2019/881 (Reglamento sobre la Ciberseguridad).

[2] Por ejemplo, la Comisión propuso el Reglamento Ómnibus Digital en noviembre de 2025 y unReglamento sobre la Ciberseguridad de la UE revisado en enero de 2026.

Ilustración 1 | Redes y mecanismos de ciberseguridad de la UE (2016-2025)



CSIRT: Equipos de respuesta a incidentes de seguridad informática
DG Redes de Comunicación, Contenido y Tecnologías Dirección General de Redes de Comunicación, Contenido y Tecnologías
EU-CyCLONe: Red de organizaciones de enlace nacionales para la gestión de cibercrisis
Directiva SRI: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
Directiva SRI 2: Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

Fuente: Tribunal de Cuentas Europeo.

04 En el actual marco financiero plurianual 2021-2027, la principal fuente de financiación de la ciberseguridad es el Programa Europa Digital. Cuenta con un presupuesto total de 8 100 millones de euros, de los cuales 1 400 millones se asignan a reforzar la ciberseguridad.

05 Nuestra auditoría tenía como objetivo evaluar si las acciones de la UE ayudan a los Estados miembros a detectar incidentes de ciberseguridad significativos y a gran escala y a responder a ellos de forma eficaz. Evaluamos si esto era así con respecto a:

- redes y mecanismos de la UE [es decir, los equipos de respuesta a incidentes de seguridad informática (red de CSIRT), la red de organizaciones de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe), el Sistema Europeo de Alerta de Ciberseguridad, el Centro de Análisis y Situación Cibernéticos y la Reserva de Ciberseguridad de la UE];
- acciones financiadas en el marco del Programa Europa Digital.

06 Esperamos que nuestras constataciones contribuyan a reforzar la ciberresiliencia de la UE al mejorar la eficacia y la eficiencia de las redes y los mecanismos de la UE, así como la selección y el seguimiento de las acciones financiadas por la UE.

07 La auditoría abarca el período comprendido entre 2022 y 2025. Se basa en un control documental y un análisis de documentos pertinentes, visitas de auditoría a tres Estados miembros (Irlanda, Grecia e Italia), y cuestionarios escritos y entrevistas con las partes interesadas. En el ***anexo I*** puede encontrarse más información general y detalles sobre el alcance y el enfoque de la auditoría.

Nuestras constataciones y recomendaciones

08 En general, concluimos que las acciones de la UE solo facilitan parcialmente la detección de incidentes de ciberseguridad significativos y a gran escala, y la respuesta a ellos. Aunque se ha instaurado gradualmente un marco de cooperación, aún se está trabajando para lograr su establecimiento definitivo. El intercambio limitado de información, las deficiencias en la notificación y los considerables retrasos en la aplicación impiden que las redes y los mecanismos de la UE alcancen todo su potencial. Los proyectos financiados por el Programa Europa Digital persiguen objetivos pertinentes, pero varios se enfrentan a retos y retrasos operativos, y existen deficiencias en el marco general de seguimiento del rendimiento.

09 El marco actual de las redes y los mecanismos de la UE destinado a facilitar la detección de incidentes de ciberseguridad significativos y darles respuesta se desarrolló gradualmente. En 2025, el Consejo adoptó el Plan Director de Ciberseguridad, en el que se establece el marco de la UE para la gestión de crisis de ciberseguridad. Constatamos que este plan explica en gran medida las funciones y las competencias relativas a la gestión de cibercrisis en la UE. Pese a ello, todavía están pendientes de formalización las disposiciones de procedimiento sobre cómo deben colaborar la red de CSIRT (establecida en 2016) y la red de organizaciones de enlace nacionales para la gestión de cibercrisis (la CyCLOne, formalizada en 2023) (apartados ***24*** a ***30***).

10 Constatamos que el intercambio de información a través de estas redes es limitado. Esto se debe sobre todo a los retrasos en la transposición de la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2), a las dificultades para determinar si un incidente tiene impacto transfronterizo y a la legislación en materia de seguridad nacional que impide el intercambio de información. El valor añadido de las redes disminuye significativamente si los Estados miembros no están dispuestos a compartir información práctica y puntual (apartados ***31*** a ***44***).

Recomendación 1

Reforzar el intercambio de información entre Estados miembros

Para mejorar la detección de incidentes de ciberseguridad significativos y darles respuesta, la Comisión, con el apoyo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), debería:

a) proponer al Grupo de cooperación en materia de seguridad de las redes y de la información realizar un análisis detallado de las restricciones de seguridad nacional que limitan el intercambio de información y afectan a la ciberresiliencia de la UE, y buscar soluciones legales y técnicas para incrementar el intercambio de información respetando los límites de la seguridad nacional;

b) sin perjuicio de las decisiones de los colegisladores, garantizar, en colaboración con los Estados miembros, que el punto de entrada único para la notificación de incidentes propuesto por el Reglamento Ómnibus Digital pueda detectar posibles incidentes transfronterizos;

c) trabajar en soluciones que permitan la notificación de incidentes en tiempo real a la ENISA.

Fecha de aplicación prevista: a) y b) en 2027, y c) en 2028

11 En 2022, la Comisión creó su sector de «centro de situación cibernética» para aumentar su conocimiento de la situación cibernética, con el objetivo de respaldar sus responsabilidades institucionales en materia de gestión de crisis. El funcionamiento del centro se apoya en gran medida en un contrato con proveedores de servicios externos. Hallamos que el trabajo efectuado por los proveedores de servicios externos duplica la capacidad existente de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en cuanto a conocimiento de la situación cibernética y seguimiento de amenazas. Consideramos que el modo en que se estableció el centro de situación cibernética no aprovechaba suficientemente el potencial de racionalización porque no utilizaba la información de que disponían la Comisión y la ENISA. Además, la ausencia de un plan exhaustivo y detallado para el período posterior a la expiración del contrato plantea un riesgo para el funcionamiento del centro de situación cibernética después de 2026 (apartados ***45*** a ***51***).

Recomendación 2

Racionalizar las capacidades de conciencia situacional de la UE en materia de ciberseguridad y optimizar la divulgación de la información

Para lograr mayor eficiencia, la Comisión, en colaboración con la ENISA, debería evaluar la viabilidad de la recogida y el análisis conjuntos de información a efectos de conciencia situacional. Asimismo, debería poner a disposición de los servicios y las agencias pertinentes de la UE esta información y los correspondientes informes de ciberseguridad.

Fecha de aplicación prevista: 2027

12 El Reglamento de Cibersolidaridad de 2024 establece la Reserva de Ciberseguridad de la UE, que tiene por objeto ayudar a los Estados miembros a responder ante incidentes cibernéticos graves y recuperarse de ellos. Está compuesta por proveedores de servicios seleccionados para cada Estado miembro capaces de responder a incidentes las veinticuatro horas del día. Si bien este enfoque contribuye a satisfacer los requisitos específicos de los Estados miembros y a generar confianza, el presupuesto disponible se reparte equitativamene entre ellos y no tiene en cuenta las necesidades específicas de uno (apartados ***52*** a ***57***).

13 Consideramos que el recurso a proveedores precontratados permite la rápida implantación de servicios de respuesta ante incidentes. Aunque la principal finalidad de la Reserva de Ciberseguridad de la UE es apoyar la respuesta y la recuperación, cuando no se usa para la respuesta a incidentes, se usa para la preparación. Este enfoque flexible podría prevenir que los servicios prepagados queden sin utilizar. Sin embargo, existe el riesgo de que la Reserva se utilice principalmente para la preparación y no para la respuesta, contrariamente a su propósito (apartados ***58*** a ***61***).

14 El Sistema Europeo de Alerta de Ciberseguridad es una red de centros cibernéticos nacionales y transfronterizos cuyo objetivo es mejorar la detección y el análisis de ciberamenazas y la respuesta ante estas. Constatamos que, en el momento de la auditoría, debido a considerables retrasos en la contratación de herramientas y servicios, los dos centros (ATHENA y ENSOC) todavía no estaban operativos, y que el Sistema Europeo de Alerta de Ciberseguridad todavía no estaba en funcionamiento (apartados ***62*** a ***70***).

15 Uno de los principales objetivos del Sistema Europeo de Alerta de Ciberseguridad es fomentar el intercambio de información significativa entre centros de los Estados miembros. Aunque esto puede resolver algunos problemas relativos al intercambio de información, también es complicado integrar centros cibernéticos en el ya complejo entorno de ciberseguridad. Constatamos que los acuerdos de cooperación exigidos, la taxonomía común y las normas de interoperabilidad necesarias para el pleno funcionamiento del Sistema Europeo de Alerta de Ciberseguridad todavía no se habían establecido (apartados ***71*** a ***74***).

Recomendación 3

Integrar el Sistema Europeo de Alerta de Ciberseguridad en el entorno de ciberseguridad de la UE

La Comisión, conjuntamente con la ENISA y los Estados miembros, debería garantizar que se han establecido mecanismos de cooperación y normas de interoperabilidad para facilitar el intercambio de información entre centros transfronterizos pertenecientes al Sistema Europeo de Alerta de Ciberseguridad, la red de CSIRT, y la de EU-CyCLONe.

Fecha de aplicación prevista: 2028

16 En 2018, la Comisión propuso la creación del Centro Europeo de Competencia en Ciberseguridad para gestionar el componente de ciberseguridad del Programa Europa Digital a partir de 2021. El Reglamento del Centro Europeo de Competencia Industrial pedía la creación de una Comunidad de Competencias en Ciberseguridad integrada por representantes de la industria, y las organizaciones académicas y de investigación. Posteriormente, miembros seleccionados de la Comunidad de Competencias en Ciberseguridad formaron un Grupo Consultivo Estratégico (apartados ***75*** a ***76***).

17 Constatamos que se produjeron retrasos en el logro de autonomía financiera por parte del Centro Europeo de Competencia en Ciberseguridad, y en el establecimiento de la Comunidad de Competencias en Ciberseguridad y el Grupo Consultivo Estratégico, y que estos dos últimos no pudieron aportar su contribución para conformar los programa de trabajo del Programa Europa Digital. En nuestra opinión, esta fue una oportunidad perdida (apartados ***77*** a ***81***).

18 Constatamos que todos los proyectos que examinamos tenían por finalidad contribuir al logro de los objetivos de ciberseguridad del programa Europa Digital. Sin embargo, hallamos casos en los que la calidad o los resultados alcanzados no eran satisfactorios, principalmente por retrasos en la aplicación (apartados ***82*** a ***87***).

19 El Reglamento sobre el Programa Europa Digital dispone que, por razones de seguridad, la financiación de la ciberseguridad podrá restringirse a las entidades jurídicas establecidas en los Estados miembros y controladas por Estados miembros o por nacionales de Estados miembros. El Servicio Central de Validación de laAgencia Ejecutiva Europea de Investigación realiza esta evaluación de la propiedad y el control en nombre del Centro Europeo de Competencia en Ciberseguridad (apartados ***88*** a ***91***).

20 En caso de apoyo financiero a terceros, la evaluación de la propiedad y el control corresponde a los beneficiarios del proyecto, con arreglo a su enfoque y a su metodología. Constatamos que el Centro Europeo de Competencia en Ciberseguridad no valida su metodología ni efectúa controles para garantizar que los terceros son propiedad de la UE y están controlados por esta. Consideramos que existe un riesgo considerable de que los beneficiarios no tengan la capacidad de realizar estos controles debidamente. Este riesgo no se ha reducido suficientemente y podría provocar la exposición de infraestructura sensible, datos operativos y tecnologías críticas para la seguridad (apartados ***92*** a ***96***).

Recomendación 4

Garantizar una evaluación rigurosa de la propiedad y el control de las entidades que perciben financiación de la UE en virtud del Programa Europa Digital

El Centro Europeo de Competencia en Ciberseguridad debería:

a) obtener garantías razonables de que los beneficiarios responsables de prestar ayuda financiera a terceros disponen de la capacidad administrativa y técnica necesaria para llevar a cabo evaluaciones adecuadas de la propiedad y el control basada en la metodología existente a disposición de los beneficiarios que ejecutan la ayuda financiera a terceros;

b) comprobar, por muestreo, si solo las entidades subvencionables han recibido financiación de la UE.

Fecha de aplicación prevista: a) en 2026 y b) en 2027

21 Los beneficiarios de proyectos financiados por la UE deben notificar sus progresos y resultados al Centro Europeo de Competencia en Ciberseguridad a través de hitos y entregables. Estos son fundamentales para la supervisión de los proyectos y deben definirse adecuadamente. Constatamos que ninguno de los proyectos de nuestra muestra seguía las instrucciones sobre la definición de hitos y entregables, y que muchos de ellos no servían para realizar un seguimiento de la evolución (apartados ***97*** a ***99***).

22 Constatamos que muchos de los indicadores de rendimiento empleados por los beneficiarios no son pertinentes o mensurables y carecen de un objetivo o de un valor de referencia. Además, la información relativa a estos indicadores era insuficiente y, por tanto, no puede servir de base para evaluar el rendimiento de los proyectos (apartados ***100*** a ***102***).

23 Para supervisar los logros del Programa Europa Digital en conjunto, todos los proyectos deben informar sobre indicadores de programa específicos que sirven de base a las declaraciones anuales de rendimiento de los programas de la Comisión. El Centro Europeo de Competencia en Ciberseguridad es responsable de recoger y verificar los datos proporcionados por estos indicadores. Hallamos varios problemas en el modo en que se recababan los datos y en la calidad global de estos. No encontramos pruebas de que el Centro verificara la exactitud de los datos notificados. Sobre la base de nuestros controles de la muestra, consideramos que los datos notificados no reflejan con exactitud los resultados logrados (apartados ***103*** a ***106***).

Recomendación 5

Reforzar el marco de seguimiento del rendimiento del componente de ciberseguridad del Programa Europa Digital

Para permitir un seguimiento adecuado del progreso y el rendimiento, el Centro Europeo de Competencia en Ciberseguridad debería:

a) garantizar, antes de la firma de las subvenciones, que todos los proyectos hayan definido hitos, entregables e indicadores de rendimiento que cumplan las instrucciones facilitadas en el formulario de solicitud;

b) diseñar y aplicar un sistema riguroso para la recogida, rastreo, verificación y agregación de los datos obtenidos de los indicadores de rendimiento sobre el componente de ciberseguridad del Programa Europa Digital a fin de garantizar que los indicadores reflejan debidamente los resultados alcanzados.

Fecha de aplicación prevista: 2027

02

Más detalles sobre nuestras observaciones

Aunque las redes y los mecanismos de ciberseguridad de la UE apoyan la cooperación ya respuesta, el intercambio limitado de información y la aplicación incompleta reducen su eficacia.

Las redes de la UE permiten la cooperación entre Estados miembros, pero el intercambio limitado de información les resta valor añadido.

24 El actual marco de redes y mecanismos de la UE para facilitar la detección de incidentes de ciberseguridad significativos y darles respuesta se desarrolló gradualmente, empezando con laDirectiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[3] (Directiva SRI), que entró en vigor en agosto de 2016. En el ***anexo II*** se muestra el panorama actual.

[3] Directiva (UE) 2016/1148.

Las redes de la UE permiten la cooperación de los Estados miembros en los ámbitos técnicos y operativos

25 La Directiva SRI estableció la red de CSIRT, que reúne el CERT-EU (el equipo de respuesta a emergencias informáticas de las instituciones, los órganos y los organismos de la unión) y los CSIRT designados por los Estados miembros. La finalidad de esta red es generar confianza y seguridad entre CSIRT nacionales y fomentar una cooperación operativa ágil y eficaz entre los Estados miembros.

26 La red EU-CyCLONe fue establecida en 2020 como red informal de cooperación para las autoridades nacionales encargadas de gestionar cibercrisis. Sirve de puente entre el nivel técnico en el que opera la red de CSIRT y el nivel político del Consejo de la Unión Europea y su Dispositivo de Respuesta Política Integrada a las Crisis. La entrada en vigor de la Directiva SRI 2 en 2023 formalizó el papel de la red EU-CyCLONe y le confirió un mandato claro.

27 Evaluamos si las funciones y competencias de estas redes del ámbito de la UE están bien definidas, y si facilitan la cooperación entre Estados miembros.

28 La ENISA actúa como secretaría de las redes de CSIRT y de EU-CyCLONe y les proporciona recursos, conocimientos especializados, infraestructura y las herramientas informáticas necesarias para la cooperación y la comunicación segura para el intercambio de información. En su encuesta de satisfacción de las partes interesadas[4] de principios de 2025, la ENISA obtuvo buenas calificaciones por su desempeño como secretaría de dichas redes. Esta opinión positiva también quedó confirmada durante nuestras vistas de auditoría, en las que las autoridades nacionales de ciberseguridad expresaron su complacencia.

[4] ENISA: informe anual de actividades consolidado de 2024, pp. 33 y 36.

29 En 2025, el Consejo adoptó el Plan Director de Ciberseguridad, que define las funciones y las competencias de los principales agentes (entre los que se cuentan las redes de CSIRT y EU-CyCLONe) y los mecanismos implicados en incidentes de ciberseguridad a gran escala o crisis de ciberseguridad. Constatamos que el Plan Director de Ciberseguridad explica en gran medida las funciones y las competencias relacionadas con la gestión de cibercrisis de la UE y tiene en cuenta los cambios que se han producido en el panorama general desde el primer plan director de 2017. Define tres niveles de cooperación: técnica, operativa y política. Describe las nuevas redes y estructuras establecidas desde 2017 (tales como EU-CyCLONe, los equipos de respuesta rápida de la UE contra amenazas híbridas, y el Sistema Europeo de Alerta de Ciberseguridad) y trata sobre cómo debería integrarse la gestión de cibercrisis en el marco más amplio de gestión de crisis de la UE.

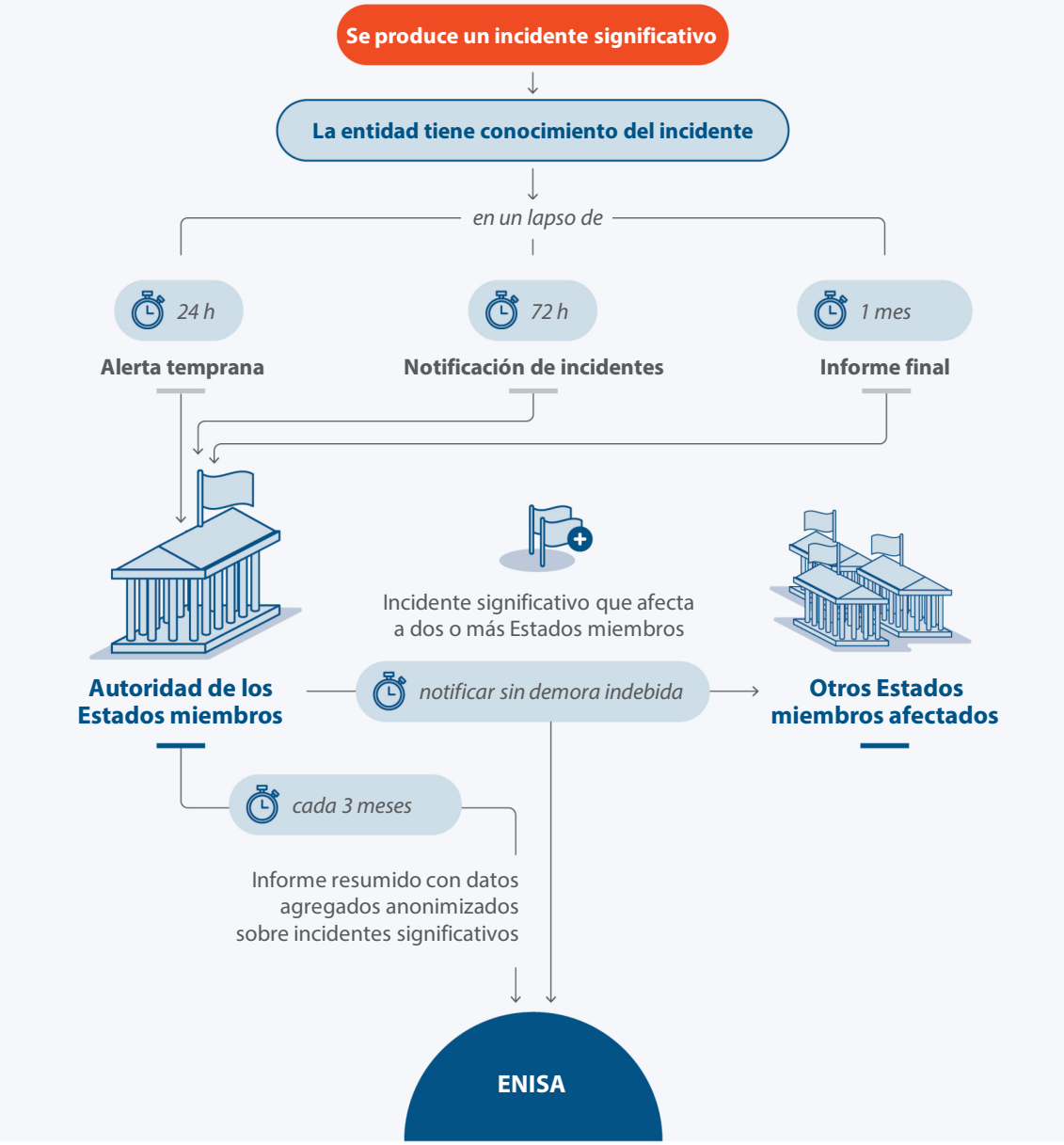
30 Sin embargo, pese a que la red de CSIRT se estableció en 2016 y la de EU-CyCLONe en 2023, ambas redes todavía tienen que formalizar las disposiciones de procedimiento sobre cómo trabajar juntas. Tampoco han acordado todavía los criterios que debe aplicar la red de CSIRT para proporcionar asesoramiento a la red de EU-CyCLONe a fin de informarle de que un incidente de ciberseguridad observado constituye un incidente de ciberseguridad a gran escala potencial o en curso. Ambas redes deben acordar asimismo una taxonomía común para los niveles de gravedad de los incidentes, así como para los principales conceptos («amenaza», «agente de riesgo», «incidente» o «impacto»), necesaria para permitir el intercambio automatizado de información. Actualmente, la calificación de un incidente como significativo o a gran escala está sujeta a interpretación. Las autoridades de ciberseguridad de los tres Estados miembros que visitamos aludieron a la falta de una taxonomía común.

Las limitaciones en el intercambio de información y la notificación reducen significativamente el valor añadido de estas redes

31 Las fronteras geográficas no impiden la ocurrencia y propagación de incidentes de seguridad y ciberataques. Por ejemplo, el intercambio de información entre Estados miembros sobre tácticas y técnicas empleadas por otros agentes de riesgo, y sobre indicios digitales de que se ha vulnerado una red o un sistema de información («indicadores de compromiso») puede contribuir considerablemente a aumentar la ciberseguridad.

32 Constatamos limitaciones en el intercambio de información, con la consiguiente reducción del valor añadido de estas redes. Las limitaciones que observamos corresponden principalmente a retrasos en la transposición de la Directiva SRI 2, problemas para determinar si un incidente tiene impacto transfronterizo, una legislación nacional en materia de seguridad que restringe el intercambio de información, y la falta de confianza. La Directiva SRI 2 introduce varios requisitos de notificación aplicables a las entidades incluidas en su ámbito de aplicación, así como para las autoridades de los Estados miembros, como se muestra en la ***ilustración 2***.

Ilustración 2 | Plazos de notificación de incidentes con arreglo a la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (SRI 2)



Fuente: Tribunal de Cuentas Europeo, a partir de datos de la ENISA.

33 Los Estados miembro s disponían hasta octubre de 2024 para transponer la Directiva SRI 2 a la legislación nacional, pero solo dos de ellos cumplieron el plazo. Los retrasos en la transposición tienen un impacto significativo en el intercambio de información, pues, mientras no la transpongan, las entidades cubiertas por la Directiva SRI 2 no tienen la obligación legal de notificar incidentes. Según las estimaciones de la Comisión[5], la Directiva SRI abarcaba a 15 500 entidades, mientras que la Directiva SRI 2 abarca a 110 000. Por ejemplo, las Administraciones públicas (el sector más afectado de la UE según el informe «Panorama de amenazas» de 2025 de la ENISA) no estaban obligadas a notificar incidentes en virtud de la Directiva SRI.

34 La notificación de datos relativos a incidentes a la ENISA cada tres meses (es decir, mucho después de que se produzca el incidente) limita su valor añadido. Estos datos tienen una utilidad meramente estadística y de notificación de las tendencias históricas, pero no mejoran la detección y la respuesta. La ENISA proporciona a los Estados miembros una herramienta en línea para presentar sus informes. La plantilla de notificación debe contener un conjunto mínimo de datos, como el tipo de incidente y el sector afectado. Además, la ENISA sugiere que los Estados miembros faciliten información adicional para permitir un análisis más exhaustivo de los datos, como por ejemplo la vinculación de incidentes con vulnerabilidades específicas. Sin embargo, no todos los Estados miembros optan por proporcionar esta información, por lo que se reduce significativamente la calidad y el valor añadido de los datos recabados.

35 La ENISA, en su informe sobre la situación de la ciberseguridad en la UE de 2024, señalaba que probablemente existiera una infradeclaración de los incidentes, ya que el número de incidentes notificados parecía bajo. En el período 2018-2021, los Estados miembros notificaron anualmente entre cien y quinientos incidentes a la ENISA. El número ha ido aumentando gradualmente y, en 2024, se elevó hasta 1 276[6].

---

[5] Comisión Europea, 2020 impact assessment report.

[6] Datos del sistema CIRAS correspondientes a 2024.

36 En su panorama de amenazas de 2025, que abarca el período comprendido entre junio de 2024 y junio de 2025, la ENISA identificó aproximadamente 4 800 incidentes de ciberseguridad[7] procedentes de inteligencia de fuentes abiertas, como artículos periodísticos. Estos incidentes no habrían sido notificables de conformidad con la Directiva SRI 2, ya que la ENISA, al recabar los datos, abarca un espectro más amplio de incidentes. Por el contrario, muchos incidentes significativos no se notifican mediante inteligencia de fuentes abiertas. Puesto que los datos facilitados por los Estados miembros se anonimizan, la ENISA no puede correlacionar los incidentes que identifica con los notificados por los Estados miembros. Por consiguiente, no es posible determinar con exactitud el alcance de la infradeclaración, pero nosotros consideramos que la diferencia entre el número de incidentes notificados por los Estados miembros y el recogido en el panorama de amenazas indica que no se notifican todos los incidentes significativos.

37 Otro indicio de infradeclaración es el número de notificaciones a otros Estados miembros afectados y a la ENISA respecto de incidentes transfronterizos significativos. En la Directiva SRI se establecía un requisito similar, pero se consideró ineficaz, pues la Comisión concluyó[8] en 2020 que las notificaciones rara vez se enviaban pese a la obligación. Atribuyó la ausencia de notificación a la falta de modalidades claras de intercambio de información y a la falta de objetivos comunes que incentivasen el intercambio.

38 La obligación de informar a otros Estados miembros es fundamental para prevenir la propagación de incidentes, pues no hacerlo afecta negativamente a la ciberseguridad de la UE. En 2025 solo fueron notificados catorce incidentes transfronterizos significativos por siete Estados miembros. Los Estados miembros presentaron dos informes de incidentes en 2024, ninguno en 2023 y tres en 2022 con posible efecto transfronterizo. Esto indica que la notificación de incidentes transfronterizos significativos es muy baja y no refleja el verdadero alcance de estos ataques. Para entenderlo en su contexto, en su panorama de amenazas de 2024, la ENISA identificó trescientos veintidós incidentes que afectaron específicamente a dos o más Estados miembros. El incidente Collins Aerospace (véase el ***recuadro 1***) constituye un ejemplo de ausencia de notificación de un incidente por los Estados miembros pese a su significativo impacto transfronterizo.

---

[7] Panorama de amenazas de 2025 de la ENISA.

[8] Comisión Europea, 2020 impact assessment report.

Recuadro 1

Incidente que perturbó las operaciones aeroportuarias

En septiembre de 2025, Collins Aerospace, un importante proveedor de tecnología de la industria de la aviación, sufrió un importante ataque con programas de secuestro de archivos contra su plataforma de gestión de pasajeros. Debido al ataque, los aeropuertos tuvieron que recurrir a operaciones manuales, lo cual provocó numerosos retrasos y cancelaciones de vuelos. La perturbación revistió mayor gravedad en el aeropuerto de Londres-Heathrow, en el aeropuerto de Bruselas, en el aeropuerto de Berlín-Brandemburgo y en el aeropuerto de Dublín.

Según la Directiva SRI 2, un incidente se considerará «significativo», entre otras circunstancias, si ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada. Sin embargo, ningún Estado miembro trató este incidente como significativo o transfronterizo a gran escala. En consecuencia, ninguno de los Estados miembros afectados notificó formalmente el incidente a la ENISA o a otros Estados miembros. La red de CSIRT no asesoró a la red de EU-CyCLONe, y, en consecuencia, esta no apoyó la gestión coordinada del incidente.

Fuente: Análisis del Tribunal de Cuentas Europeo basado en entrevistas con la ENISA.

39 Otro motivo por la escasa notificación de incidentes transfronterizos reside en el hecho de que corresponde a la autoridad de cada Estado miembro determinar si un incidente notificado tiene impacto transfronterizo, así como identificar otros Estados miembros afectados. Sobre la base de la información de que disponen, puede darse que la entidad notificadora o la autoridad del Estado miembro desconozcan la naturaleza transfronteriza de algunos ataques. Actualmente, no existe una plataforma de toda la UE que reciba información de los incidentes en tiempo real procedente de todos los Estados miembros que les permita correlacionar información sobre sectores o indicadores de compromiso para detectar incidentes transfronterizos. Existe, por tanto, un riesgo considerable de que algunos incidentes transfronterizos no sean detectados ni notificados.

40 Desde 2016 ningún incidente de ciberseguridad ha sido considerado «de gran escala» por ningún Estado miembro. En principio, esa es la definición de cualquier incidente que afecte significativamente a al menos dos Estados miembros. Sin embargo, ni siquiera incidentes de seguridad que han causado apagones mundiales y daños significativos, como los que figuran en la ***ilustración 3***, se han considerado de gran escala. En consecuencia, nunca se ha activado plenamente el mecanismo de escalada de la red EU-CyCLONe a raíz de un incidente de ciberseguridad de gran escala.

Ilustración 3 | Ejemplos de incidentes de ciberseguridad importantes

WannaCry

2017

Ataque mundial con programas de secuestro de archivos

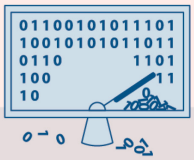
Infectó más de 200 000 ordenadores en más de 150 países, lo que paralizó a los operadores de infraestructuras críticas; datos cifrados sobre dispositivos infectados y solicitud de rescate para el descifrado

NotPetya

2017

Programa malicioso destructivo encubierto como programa de secuestro

Diseñada para borrar datos de forma permanente y dirigida principalmente a Ucrania, se propagó rápidamente por todo el mundo paralizando a empresas multinacionales y causando daños a escala mundial.



Interrupción informática relacionada con el CrowdStrike

Julio de 2024

Indisponibilidad informática masiva a escala mundial

Causado por una actualización defectuosa del *software* de la empresa de ciberseguridad CrowdStrike, que averió millones de ordenadores

Fuente: Adaptación del Tribunal de Cuentas de la Unión Europea, a partir de Cloudflare, ENISA, Europol, Wired, IBM y CrowdStrike.

41 Además de la obligación de notificación impuesta a entidades y Estados miembros, la red de CSIRT se creó para facilitar el intercambio de información. La confianza entre Estados miembros es la base esencial de la red de CSIRT, en la que la información se intercambia voluntariamente. El valor añadido de la red disminuye significativamente si los Estados miembros no están dispuestos a compartir información práctica y puntual.

42 El intercambio de información en la UE está restringido por la legislación nacional en materia de seguridad de cada Estado miembro. Si un Estado miembro considera que la información relativa a ciberataques a una entidad crítica es de carácter clasificado, o que informar sobre un incidente específico podría perjudicar su seguridad nacional, no está obligado a compartir la información. Durante nuestras visitas a Estados miembros, representantes de la red de CSIRT y de la red de EU-CyCLONe afirmaron que el intercambio solo puede realizarse dentro de los límites de la legislación nacional en materia de seguridad. En la UE no se ha llevado a cabo un análisis de los marcos jurídicos nacionales y de su impacto en el intercambio de información.

43 En 2016, la red de CSIRT estaba compuesta por veintiocho CSIRT nacionales, con dos representantes por Estado miembro. La falta de intercambio de información es un problema recurrente, y la evaluación de la Comisión de la Directiva SRI reconocía que los Estados miembros no intercambian información sistemáticamente, lo cual afecta especialmente a la eficacia de las medidas de ciberseguridad y al nivel de conocimiento conjunto de la situación en la UE. En virtud de la Directiva SRI 2, muchos Estados miembros han designado CSIRT sectoriales además de su CSIRT nacional, por lo que la red se ha ampliado considerablemente. Cuando realizábamos la auditoría, contaba con cuarenta y dos CIRST y más de setecientos participantes individuales, por lo que generar confianza resulta más difícil, pues mantener vínculos estrechos también lo es.

44 La red de CSIRT está al tanto del problema de intercambio de información y estudia medidas para reforzar la confianza en una red cada vez mayor. La creación de grupos más reducidos de Estados miembros para establecer agrupaciones transfronterizas, como se explica en los apartados ***62*** a ***74***, es un modelo alternativo de red de la UE que puede contribuir a solucionar este problema.

Los servicios contratados del centro de situación cibernética duplican parcialmente las capacidades existentes y no está claro cómo funcionará en el futuro

45 Con arreglo a la Directiva SRI 2, en los casos en que un incidente de ciberseguridad a gran escala potencial o en curso tenga o pueda tener un impacto significativo, la Comisión participará en las actividades de EU-CyCLONe en calidad de observador[9]. Esta nueva competencia, y la evolución del panorama de amenazas, llevaron a la Comisión a establecer un grupo operativo de coordinación cibernética en la DG Redes de Comunicación, Contenido y Tecnologías en 2022. En este grupo operativo existe un centro de situación cibernética cuyo propósito es ayudar a la Comisión a mejorar su nivel de conocimiento de la situación, con el objetivo de respaldar sus responsabilidades institucionales en materia de gestión de crisis. También debería ayudar a la DG Redes de Comunicación, Contenido y Tecnologías a proporcionar asesoramiento político.

46 Para establecer el centro de situación cibernética, la Comisión se apoya en gran medida en proveedores de servicios externos contratados en diciembre de 2022 por casi 18 millones de euros durante cuatro años. Evaluamos el establecimiento del centro, sus realizaciones, y los planes de la Comisión para su futuro funcionamiento.

---

[9] Artículo 16, apartado 2, de la Directiva SRI 2.

47 Entre los servicios prestados, los contratistas han creado un cuadro de indicadores basado en fuentes comerciales de inteligencia sobre ciberamenazas para presentar y compartir la información relativa a amenazas. También elaboran varios informes sobre inteligencia sobre ciberamenazas, diarios y semanales, e informes temáticos sobre países o sectores de la economía. El centro físico de situación cibernética, que consiste en una habitación equipada con estaciones de trabajo conectadas a distancia con el cuadro de indicadores ubicado en los locales de los contratistas, se ha montado en uno de los edificios de la Comisión. En el momento de la auditoría, el centro de situación cibernética estaba compuesto por un número reducido de efectivos de la Comisión, con el apoyo de numerosos analistas de los contratistas y expertos de la ENISA.

48 Constatamos que parte del trabajo realizado por los proveedores de servicios externos del centro de situación cibernética se solapa con la capacidad existente de la ENISA. La ENISA cuenta con capacidad permanente en cuanto a conocimiento de la situación cibernética y seguimiento de amenazas. Publica periódicamente informes sobre ciberamenazas, incluidos informes breves sobre incidentes específicos, e informes semanales que proporcionan una visión global de las amenazas. Los informes se basan en inteligencia procedente de fuentes de dominio público y son similares a los elaborados por los contratistas. Además, en tiempos de crisis, la ENISA elabora informes ejecutivos para responsables políticos o contribuye a ellos; tales informes son comparables a los que produce el centro situación cibernética.

49 Además, los datos empleados por el del centro de situación cibernética para elaborar estos informes están basados en fuentes comerciales de información sobre ciberamenazas y son similares a los datos empleados por otros servicios de la Comisión, como la Dirección General de Servicios Digitales y el CERT-EU. Consideramos que el modo en que se estableció el centro de situación cibernética no aprovechaba suficientemente el potencial de racionalización porque no utilizaba la información de que disponían la Comisión y la ENISA.

50 El contrato vence en diciembre de 2026 y, posteriormente, los contratistas dejarán de proporcionar los servicios para el centro de situación cibernética. Entre tales servicios cabe señalar la provisión de datos disponibles en el cuadro de indicadores, la elaboración de los informes sobre amenazas y la constitución de la mayor parte del personal del centro. El cuadro de indicadores se entregará a la Comisión, pero perderá su valor añadido si no se actualiza continuamente con inteligencia sobre ciberamenazas.

51 Cuando efectuábamos nuestra auditoría, la Comisión no tenía planes sobre el apoyo de los proveedores de servicios externos en el funcionamiento del centro de situación cibernética tras el vencimiento del contrato. Consideramos la ausencia de un plan exhaustivo y detallado para el período posterior a la expiración del contrato plantea un riesgo para el funcionamiento del centro de situación cibernética después de 2026.

La Reserva de Ciberseguridad de la UE permite el rápido despliegue de los servicios de respuesta a los incidentes

52 En 2022, tras la agresión militar de Rusia contra Ucrania, sabiendo que los ciberataques a gran escala eran cada vez más frecuentes, la Comisión proporcionó a la ENISA 15 millones de euros de financiación excepcional para que dirigiera la la acción de apoyo a la ciberseguridad, que se lanzó en 2023. En 2023, la Comisión facilitó financiación adicional (aproximadamente 20 millones de euros) para ampliar el programa hasta el final de 2026.

53 La Comisión también propuso el Reglamento de Cibersolidaridad, adoptado en diciembre de 2024, para prepararse frente a incidentes de seguridad de gran escala. El Reglamento establece la Reserva de Ciberseguridad de la UE, que incluye servicios de respuesta a incidentes prestados por proveedores de confianza. Comenzó a funcionar gradualmente en 2025 con un presupuesto de 36 millones de euros para el período 2025-2027.

54 Evaluamos cómo se organizó el programa de acción de apoyo a la ciberseguridad, pues constituye la base de la Reserva de Ciberseguridad de la UE. También comprobamos si los conocimientos adquiridos desde 2022 se habían incorporado al diseño de la Reserva de Ciberseguridad de la UE.

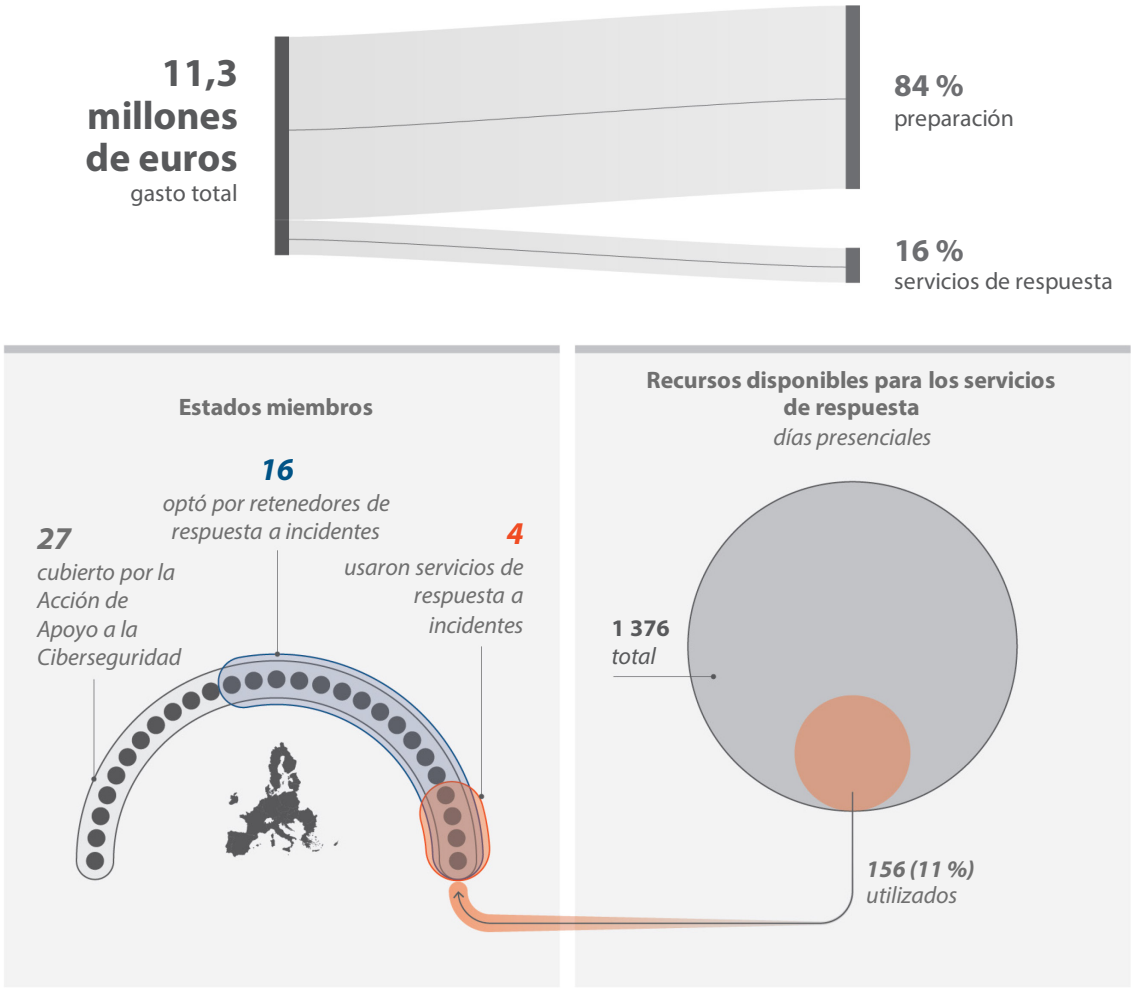
55 La ENISA diseñó la acción de apoyo a la ciberseguridad como mecanismo para prestar servicios de apoyo a la preparación y la respuesta de los Estados miembros frente a incidentes o crisis de ciberseguridad a gran escala. Todos los servicios son precontratados por la ENISA, lo cual significa que los prestadores de servicios pueden empezar a trabajar en cuanto los Estados miembros los necesiten. Esto se debe asimismo a la configuración de la ENISA, que asegura la permanencia de un agente las veinticuatro horas del día para atender las necesidades de los Estados miembros.

56 La ENISA decidió asignar el presupuesto disponible equitativamente entre los Estados miembros. En la práctica, la agencia lanzó un procedimiento abierto dividido en veintisiete lotes, uno por Estado miembro, para seleccionar un máximo de tres proveedores de seguridad privados que prestarán sus servicios hasta el final de 2026. Además, la ENISA seleccionó a algunos proveedores de un lote paneuropeo para prestar servicios a países terceros admisibles, así como a instituciones, órganos y organismos de la UE, o para apoyar la respuesta a incidentes transfronterizos.

57 Este enfoque permitió a la ENISA tener en cuenta requisitos nacionales específicos como el idioma, habilitaciones de seguridad nacionales o presencia establecida en los Estados miembros. Por otra parte, como los proveedores no fueron seleccionados para poder prestar servicios en toda la UE, un gran inconveniente de este enfoque es que, si un Estado miembro no usa los servicios precontratados, el presupuesto comprometido para tales servicios destinados a un Estado miembro no puede utilizarse para asistir a otro Estado miembro.

58 Respecto de la acción de apoyo a la ciberseguridad, los Estados miembros podían elegir entre servicios de preparación o de respuesta, o bien una combinación de ambos. Los Estados miembros optaron principalmente por utilizar la financiación disponible para su preparación (84 % del gasto en 2023). Los Estados miembros que optaron por tener un retén de respuesta a incidentes (es decir, un acuerdo predefinido con un proveedor que garantiza al Estado miembro, previa solicitud, el acceso a los servicios del proveedor para obtener una respuesta rápida a los incidentes de ciberseguridad) lo utilizaron poco, como se muestra en la ***ilustración 4***. En los tres Estados miembros visitados, las autoridades manifestaron su satisfacción por la gestión de la acción de apoyo a la ciberseguridad realizada por la ENISA.

Ilustración 4 | Acción de apoyo a la ciberseguridad de la ENISA hasta 2023



Fuente: Tribunal de Cuentas Europeo, a partir de datos de la ENISA.

59 Para el período 2024-2026, solo nueve Estados miembros han solicitado un retén de respuesta a incidentes. Nuestras entrevistas con la ENISA y las autoridades en tres Estados miembros han confirmado una clara preferencia por las actividades de preparación.

60 Aunque el principal objetivo de la Reserva de Ciberseguridad de la UE es apoyar la repuesta y la recuperación frente a incidentes graves de ciberseguridad, los servicios objeto de compromiso previo de esta reserva que no se usen para respuesta a incidentes pueden convertirse en servicios de preparación. Este enfoque flexible podría prevenir que los servicios prepagados queden sin utilizar.

61 Consideramos que el modelo elegido para la Reserva de Ciberseguridad de la UE se basa en los conocimientos adquiridos a partir del programa de acción de apoyo a la ciberseguridad. No obstante, los datos sobre el uso del programa de acción de apoyo a la ciberseguridad señalan el riesgo de que la Reserva de Ciberseguridad de la UE pueda usarse primordialmente para la preparación, y no para la respuesta, contrariamente al propósito establecido en el Reglamento de Cibersolidaridad.

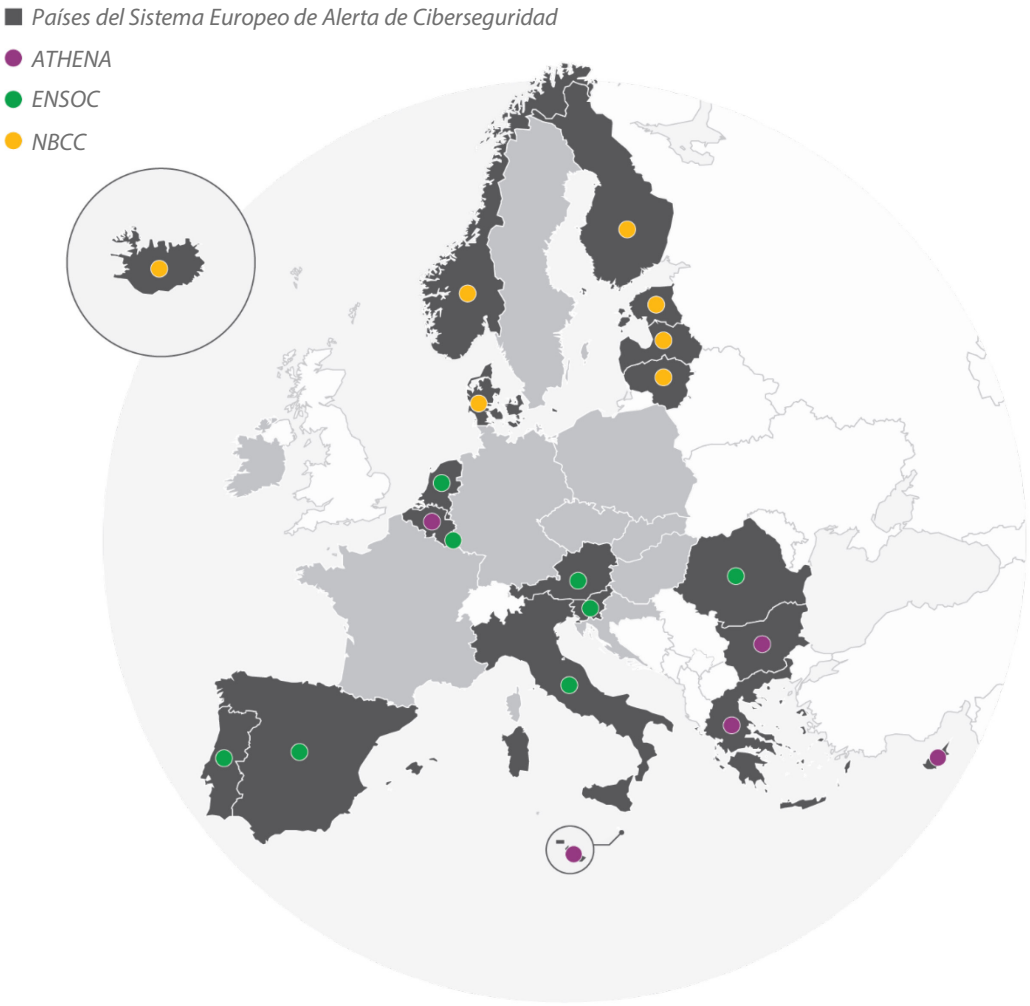
El Sistema Europeo de Alerta de Ciberseguridad busca mejorar las capacidades de detección de amenazas, pero no está operativo

62 Uno de los principales objetivos del Sistema Europeo de Alerta de Ciberseguridad es fomentar el intercambio de información significativa para mejorar la detección y el análisis de las ciberamenzas y responder a estas. La participación en el sistema de alerta es voluntaria, pero los Estados miembros que deciden unirse a un centro cibernético transfronterizo deben comprometerse a compartir información relevante con otros miembros. Trabajando juntos en grupos en un ambiente de confianza y seguridad, los Estados miembros pueden evitar algunos de los problemas de intercambio de información descritos en los apartados ***31*** a ***44***.

63 En el momento de la auditoría, trece Estados miembros habían decidido integrarse en el Sistema Europeo de Alerta de Ciberseguridad estableciendo dos centros transfronterizos: ATHENA y ENSOC. En 2026 se asignó financiación a un tercer centro cibernético transfronterizo, NBCC, lo que elevó los países miembros de la red a un total de veinte (dieciocho Estados miembros, Islandia y Noruega[10]), como se muestra en la ***ilustración 5***.

[10] Países terceros asociados de conformidad con el artículo 10, apartado 1), letra a), del Reglamento (UE) 2021/694.

Ilustración 5 | Países del Sistema Europeo de Alerta de Ciberseguridad



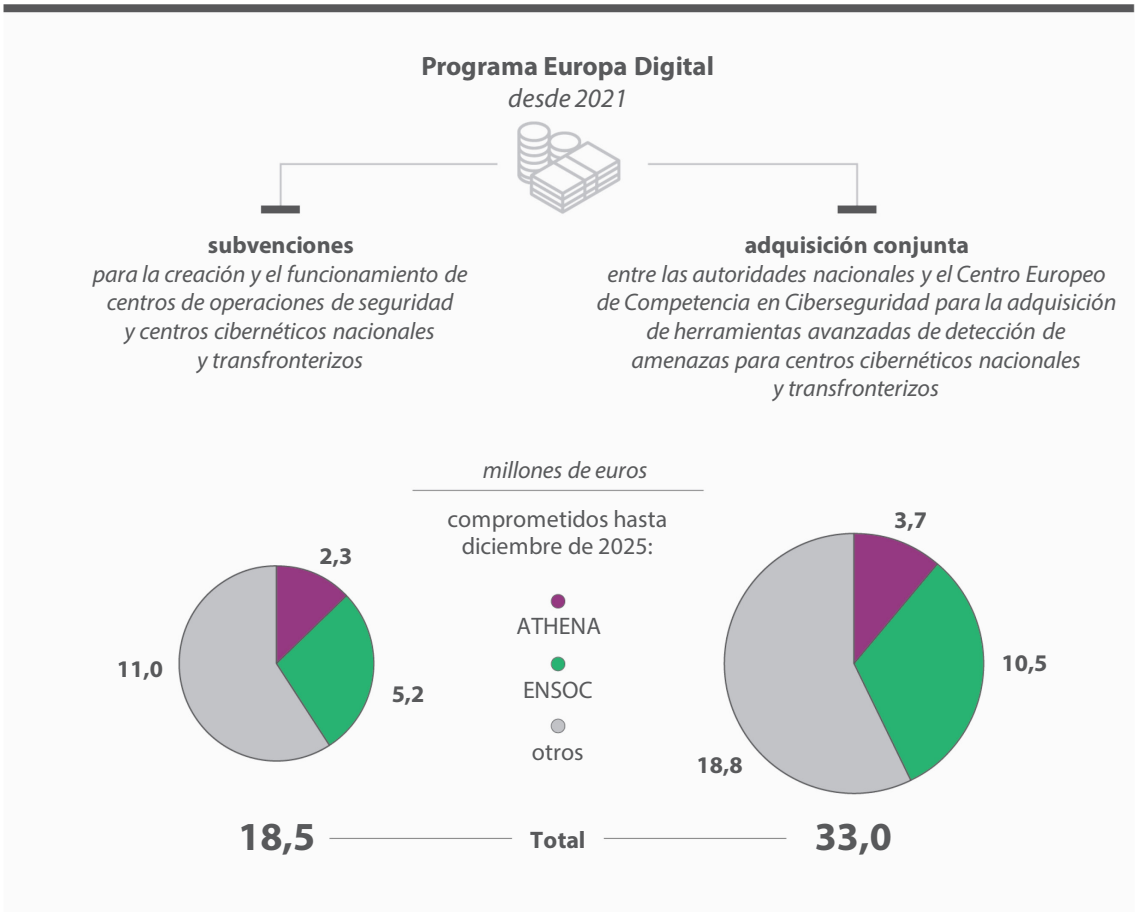
Fuente: Tribunal de Cuentas Europeo.

64 Evaluamos cómo se han establecido los dos primeros centros cibernéticos transfronterizos, así como su avance en el cumplimiento de los objetivos del Sistema Europeo de Alerta de Ciberseguridad. También examinamos cómo se integran en el entorno de ciberseguridad los centros cibernéticos transfronterizos establecidos, y cómo interactúan con las redes y estructuras existentes.

Hasta ahora no se han obtenido resultados concretos debido a retrasos considerables en la contratación

65 La financiación para apoyar el establecimiento de centros cibernéticos nacionales y transfronterizos está disponible desde 2021 a través del programa Europa Digital. Esta financiación se facilita mediante un complejo procedimiento que consta de dos flujos paralelos: subvenciones tradicionales para apoyar la creación y el funcionamiento del centro, y contratación conjunta para la adquisición de herramientas avanzadas de detección de amenazas, como se muestra en la ***ilustración 6***. Tras una convocatoria de propuestas en noviembre de 2022, ATHENA y ENSOC empezaron a funcionar en enero de 2024.

Ilustración 6 | Financiación del programa Europa Digital destinada a centros cibernéticos



Fuente: Tribunal de Cuentas Europeo, a partir de datos del Centro Europeo de Competencia en Ciberseguridad.

66 Los procedimiento restringidos de contratación pública en dos fases[11] fueron organizados por los miembros de ATHENA y ENSOC, así como por la DG Redes de Comunicación, Contenido y Tecnologías (primera fase) y por el recientemente establecido Centro Europeo de Competencia en Ciberseguridad (segunda fase). El enfoque en dos fases tiene por objeto limitar la circulación de información sensible porque únicamente proporciona especificaciones técnicas detalladas a los candidatos seleccionados en la primera fase.

67 La primera fase se lanzó en mayo de 2024 para ENSOC y en julio de 2024 para ATHENA. Las empresas interesadas tuvieron un mes para postularse. Sin embargo, los candidatos seleccionados no recibieron la notificación hasta abril de 2025, casi un año después del inicio de la convocatoria.

68 Además, ninguno de los procedimientos de contratación (ni de ENSOC ni de ATHENA) pudieron pasar a la segunda fase en aquel momento, pues los miembros del grupo y el Centro Europeo de Competencia en Ciberseguridad no pudieron facilitar a la lista de las empresas seleccionadas las especificaciones técnicas necesarias para que presentaran una oferta, ya que todavía estaban trabajando para finalizarlas.

69 La segunda fase de los procedimientos de contratación no se inició hasta agosto de 2025 en algunos lotes de ENSOC, y estaba prevista para el principio de 2026 en ATHENA. Cuando realizábamos la auditoría, dieciocho meses después del lanzamiento del procedimiento de contratación, no se había firmado contrato para ninguno de los lotes. Consideramos que la falta de preparación adecuada y la complejidad de los procedimientos de contratación contribuyeron a retrasar su finalización.

70 Por tanto, constatamos que los grupos transfronterizos no se encuentran en vías de alcanzar sus objetivos. Sin las herramientas para detectar amenazas y compartir información, se encuentran en pausa operativa, y el Sistema Europeo de Alerta de Ciberseguridad todavía no funciona, lo cual retrasa el desarrollo de capacidades avanzadas para la detección y prevención de amenazas e incidentes cibernéticos. Se han aprobado modificaciones para ampliar la duración del convenio de subvención a raíz de los retrasos registrados en los procedimientos de contratación pública hasta la fecha (quince meses en el caso de ATHENA y dieciocho en el de ENSOC).

[11] Licitación de ENSOC y licitación de ATHENA.

Los centros cibernéticos transfronterizos crean canales adicionales de comunicación que aumentan la complejidad

71 Una de las tareas principales de los centros cibernéticos transfronterizos es el intercambio de información pertinente para mejorar la detección de amenazas y la respuesta a estas, como información sobre ciberamenazas, vulnerabilidades, indicadores de compromiso y agentes de riesgo. Las tareas de los centros cibernéticos transfronterizos se solapan parcialmente con las de los CSIRT nacionales y las de la red de CSIRT, especialmente con respecto al intercambio de información sobre ciberamenazas y vulnerabilidades. No existe un límite claro entre el cometido de los centros cibernéticos transfronterizos y el de los CSIRT. Según el Plan Director de Ciberseguridad de 2025 (apartado ***29***), los centros cibernéticos transfronterizos están concebidos para funcionar tanto en el ámbito técnico (por ejemplo, el CSIRT nacional y la red de CSIRT) como en el operativo (por ejemplo, la red de EU-CyCLONe).

72 El Reglamento de Cibersolidaridad exige que los centros cibernéticos transfronterizos suscriban acuerdos de cooperación entre sí para facilitar el intercambio de información. La ENISA debería haber emitido orientaciones relativas a la interoperabilidad entre centros cibernéticos transfronterizos antes de febrero de 2026, como exige el Reglamento de Cibersolidaridad. Entretanto, en diciembre de 2025, el Centro Europeo de Competencia en Ciberseguridad concedió una subvención a un consorcio (del que formaban parte algunos miembros de ENSOC y ATHENA) para definir un marco técnico de interoperabilidad entre centros cibernéticos transfronterizos. Sin embargo, las orientaciones y el marco solo se completarán cuando los centros cibernéticos transfronterizos estén en funcionamiento. Como señalamos en nuestro dictamen de 2023 sobre la propuesta de Reglamento de Ciberseguridad[12], estas condiciones y requisitos deberían acordarse rápidamente para evitar el riesgo de desarrollo simultáneo de sistemas incompatibles entre sí y reducir los costes.

[12] Dictamen 02/2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos, apartado 26.

73 Los centros cibernéticos transfronterizos también deben intercambiar información pertinente sobre incidentes de seguridad a gran escala con las redes de EU-CyCLONe y de CSIRT sin retrasos indebidos. En los Estados miembros, la creación de centros cibernéticos nacionales y la participación en los centros cibernéticos transfronterizos crean capas adicionales de comunicación. La coordinación con Estados terceros[13], que no pertenecen a las redes de EU-CyCLONe y de CSIRT, también aumenta la complejidad.

74 Son necesarios acuerdos de cooperación claros para concertar una taxonomía común y modalidades de intercambio de información, así como para garantizar la interoperabilidad. Los conocimientos adquiridos sobre la red de CSIRT indican que esto plantea un reto significativo. Cuando realizábamos la auditoría pudimos constatar que no se habían acordado disposiciones de procedimiento sobre cooperación e intercambio de información. Consideramos que el establecimiento de centros cibernéticos nacionales y transfronterizos podría potenciar la eficacia del intercambio de información. No obstante, la integración de los centros transfronterizos en el ya complejo entorno de ciberseguridad no será fácil y requerirá canales de comunicación y acuerdos de cooperación adicionales.

[13] Islandia y Noruega.

Los proyectos financiados por la UE en virtud del Programa Europa Digital tienen por objeto reforzar la ciberseguridad, pero se enfrentan a retos de aplicación e información

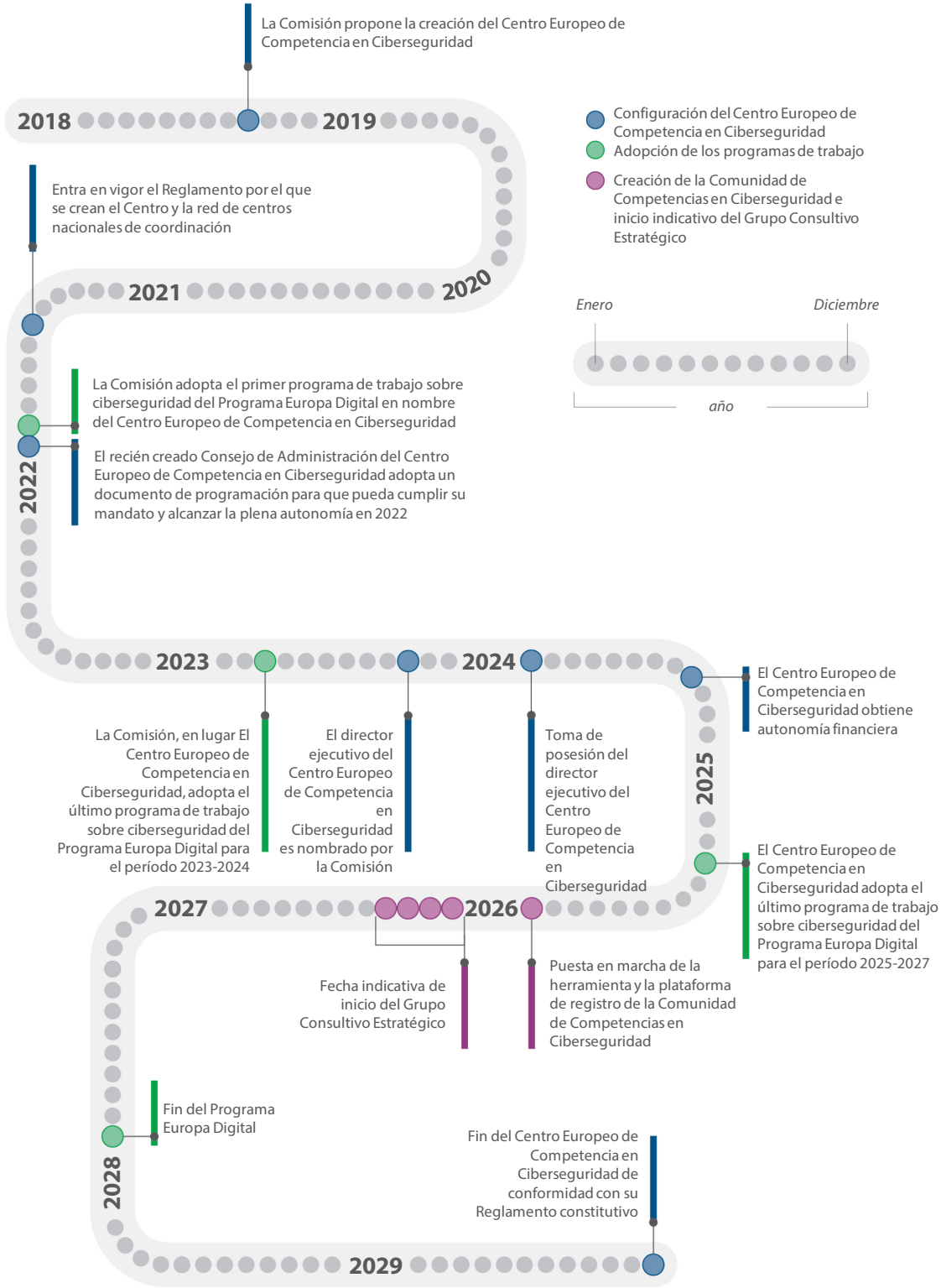
Los retrasos en su establecimiento impidieron que la Comunidad de Competencias en Ciberseguridad conformara el Programa Europa Digital según sus necesidades

75 Para gestionar el componente de ciberseguridad del programa Europa Digital, la Comisión propuso en 2018 la creación del Centro Europeo de Competencia en Ciberseguridad. El Reglamento por el que se establece el Centro Europeo de Competencia en Ciberseguridad preveía que el Centro contara con el apoyo de una red de veintinueve centros nacionales de coordinación, uno por Estado miembro, así como en Islandia y en Noruega. También instaba a la creación de la Comunidad de Competencias en Ciberseguridad (la Comunidad), compuesta por representantes de la industria, organizaciones académicas y de investigación, además de otras asociaciones de la sociedad civil pertinentes.

76 Se designarán hasta veinte miembros de la Comunidad para el Grupo Consultivo Estratégico, uno de los tres componentes de la estructura del Centro Europeo de Competencia Industrial. Una de las principales tareas del Grupo Consultivo Estratégico es organizar consultas públicas para enriquecer el programa estratégico del Centro Europeo de Competencia en Ciberseguridad y los programas de trabajo del Programa Europa Digital.

77 Evaluamos si el Programa Europa Digital y sus programas de trabajo se adoptaron sobre la base de un análisis riguroso de las necesidades, y si el Centro Europeo de Competencia en Ciberseguridad, la red de centros nacionales de coordinación, la Comunidad y el Grupo Consultivo Estratégico pudieron contribuir a los programas de trabajo. En la práctica, el Centro Europeo de Competencia en Ciberseguridad, la red de centros nacionales de coordinación, la Comunidad y el Grupo Consultivo Estratégico se establecieron gradualmente a lo largo de varios años (véase la ***ilustración 7***).

Ilustración 7 | Calendario del establecimiento del Centro Europeo de Competencia en Ciberseguridad, la red de centros nacionales de coordinación, la Comunidad y el Grupo Consultivo Estratégico



Fuente: Tribunal de Cuentas Europeo.

78 Puesto que el Centro Europeo de Competencia en Ciberseguridad no empezó a funcionar plenamente hasta septiembre de 2024, la Comisión, en su nombre, adoptó los programas de trabajo de los períodos 2021-2022 y 2023-2024. Los dos programas de trabajo adoptados por la Comisión no pudieron beneficiarse de las aportaciones de la Comunidad.

79 Entretanto, los Estados miembros empezaron a establecer sus propios centros nacionales de coordinación, que actúan como puntos de contacto nacionales para la Comunidad. Su creación y funcionamiento han sido cofinanciados por el programa Europa Digital, y ya había percibido más de 90 millones de euros de financiación de la UE cuando realizábamos la auditoría, entre los que se contaban aproximadamente 44 millones de euros que también se distribuirán a través de apoyo financiero a terceros. Se han presupuestado 38 millones de euros adicionales hasta 2027 para apoyar a los centros nacionales de coordinación.

80 Constatamos que, en diciembre de 2025, cuatro años después del establecimiento del Centro Europeo de Competencia en Ciberseguridad y de la red de centros nacionales de coordinación, todavía no se había establecido la Comunidad, y todavía no se había designado el Grupo Consultivo Estratégico. El Centro Europeo de Competencia en Ciberseguridad adoptó el último programa de trabajo sobre ciberseguridad del Programa Europa Digital para el período 2025-2027 el 14 de marzo de 2025. Si bien el Centro Europeo de Competencia en Ciberseguridad elaboró y adoptó su programa de trabajo tras consultar exhaustivamente a los Estados miembros y a la red de centros nacionales de coordinación, no pudo beneficiarse de las aportaciones y el asesoramiento de la Comunidad o del Grupo Consultivo Estratégico. Esto contraviene lo dispuesto en su reglamento de base, y lo consideramos una oportunidad perdida.

81 El Programa Europa Digital expira en 2027 y, si su mandato no se amplía, se prevé que el Centro Europeo de Competencia en Ciberseguridad se liquide en 2029. Por tanto, es posible que, cuando se haga efectivo, el apoyo a la red de centros nacionales de coordinación, a la Comunidad y al Grupo Consultivo Estratégico solo sea pertinente durante un período corto.

Los proyectos financiados por la UE persiguen objetivos pertinentes, pero muchos se enfrentan a problemas operativos

82 Seleccionamos una muestra de once proyectos pertinentes para detectar incidentes de ciberseguridad y darles respuesta financiados por el Programa Europa Digital en el período 2022-2025 (véanse la ***ilustración 5*** el ***anexo I*** y el ***anexo III***). Evaluamos si:

- los objetivos de los proyectos se ajustaban a los resultados previstos indicados en las convocatorias de propuestas y a los objetivos generales del Programa Europa Digital;
- los proyectos han alcanzado las realizaciones y los resultados previstos hasta la fecha;
- si los resultados del proyecto se han logrado a su debido tiempo.

Presentamos los resultados de esta evaluación en el ***anexo IV***.

Algunos proyectos arrojan resultados tempranos, pero muchos sufren dificultades operativas y retrasos

83 Hallamos que todos los proyectos tienen por finalidad contribuir al logro de los objetivos de ciberseguridad del Programa Europa Digital[14], y que abordan la mayoría de los objetivos de las convocatorias de propuestas[15].

84 Dos de los once proyectos de nuestra muestra se encontraban en una fase temprana de aplicación, por lo que no pudimos llegar a ninguna conclusión sobre su rendimiento. En cuanto a los proyectos restantes, evaluamos cuatro como satisfactorios en cuanto al logro de sus realizaciones y resultados previstos. Consideramos que dos proyectos presentan insuficiencias, y que otros dos eran insatisfactorios (véase el ***anexo IV***).

85 El Programa Europa Digital aspira explícitamente a elevar el nivel de ciberseguridad de las pequeñas y medianas empresas (pymes). En este sentido, varios proyectos ofrecen soluciones concretas para las pymes (véase el ***recuadro 2***).

---

[14] Artículo 6 del Reglamento (UE) 2021/694 por el que se establece el Programa Europa Digital.

[15] Convocatorias: Desarrollar las capacidades de los centros de operaciones de seguridad; Desplegar la red de centros nacionales de coordinación con los Estados miembros; Apoyar la preparación y la asistencia mutua, y Nuevas aplicaciones de inteligencia artificial (IA) y otras tecnologías generadoras para los centros de operaciones de seguridad.

Recuadro 2

Ejemplos de proyectos que logran resultados tangibles para las pymes

El proyecto GR-SME-SOC (proyecto 6 del ***anexo III***) tiene por objeto proporcionar herramientas y servicios de ciberseguridad a las pymes en Grecia mediante el establecimiento de un centro de operaciones de seguridad adaptado a sus necesidades. El proyecto se inició en enero de 2024 y está siendo llevado a cabo por un consorcio de cinco organizaciones griegas. El plan es proporcionar servicios de seguridad, gratuitos, a ciento veinte pymes durante un período de un año; una vez transcurrido este, los servicios serán comercialmente accesibles. El proyecto ofrece a las pymes servicios avanzados, como seguimiento en tiempo real, detección de amenazas basadas en la IA y respuesta ágil ante incidentes.

Con el proyecto NCC-IE (proyecto 3 del ***anexo III***), el coordinador del proyecto facilitó unos 1,8 millones de euros en subvenciones a más de cincuenta pymes irlandesas para mejorar su ciberseguridad. El régimen de subvenciones benefició a empresas de entre dos y doscientos empleados, incluidos negocios familiares, empresas emergentes y exportadores mundiales en varios sectores. Las subvenciones se destinaron exclusivamente a empresas que habían sido previamente sometidas a un análisis de ciberseguridad realizado por la agencia gubernamental Entreprise Ireland. La subvención cubría el 80 % de los costes (hasta 60 000 euros) para aplicar las recomendaciones derivadas del análisis.

Fuente: Tribunal de Cuentas Europeo.

86 Muchos proyectos de nuestra muestra tienen dificultades para cumplir los plazos o se enfrentan a retos operativos (véase el ***anexo IV***). Constatamos que cuatro proyectos tienen considerables retrasos. Tal es el caso de ENSOC y ATHENA, como se describe en los apartados ***65*** a ***70***. En el ***recuadro 3*** presentamos otros ejemplos.

Recuadro 3

Ejemplos de proyectos que se enfrentan a retos operativos y a retrasos

En Irlanda, la autoridad encargada de la administración de gobiernos locales es la única beneficiaria de la subvención asignada al proyectoILG-SOC (proyecto 8 del ***anexo III***). El objetivo del proyecto es establecer un centro de operaciones de seguridad central para treinta y una autoridades locales que emplee herramientas de detección de amenazas y de respuesta avanzadas. El proyecto se inició en octubre de 2023 y tuvo una duración de tres años. El examen intermedio dio lugar al rechazo de todos los entregables. El proyecto incluye varios procedimientos de contratación pública que se malograron o sufrieron retrasos. La duración del proyecto será ampliada (sin financiación adicional), de modo que este pueda disponer de tiempo suficiente para finalizar de manera satisfactoria.

En Grecia, el proyecto EL-SOC (proyecto 5 del ***anexo III***) tiene por objeto establecer un centro de operaciones de seguridad consolidado en el ámbito nacional, que reuniría la información de los centros sectoriales. De este modo se obtendría una visión exhaustiva en tiempo real de la situación en cuanto a ciberseguridad. El proyecto abarca el período comprendido entre enero de 2024 y diciembre de 2026. La adquisición prevista de equipos y servicios informáticos se retrasó por problemas surgidos al finalizar y publicar las especificaciones técnicas para la licitación. Como motivos del retraso, el coordinador también mencionó problemas para obtener la cofinanciación nacional y la disponibilidad limitada de personal de contratación.

Fuente: Tribunal de Cuentas Europeo.

87 Otros dos proyectos de nuestra muestra se enfrentan a retrasos moderados. Tres proyectos han entregado sus resultados a tiempo. Por último, dos proyectos se encuentran en una fase temprana de aplicación, por lo que no podemos extraer una conclusión.

Las restricciones de seguridad han causado dificultades operativas, y existen riesgos significativos cuando los controles son efectuados por beneficiarios

88 El Reglamento sobre el Programa Europa Digital dispone que, por razones de seguridad, la financiación de la ciberseguridad podrá limitarse a las entidades jurídicas establecidas en los Estados miembros y controladas por Estados miembros o por nacionales de Estados miembros. Esta restricción tiene por objeto mitigar el riesgo de intrusión o influencia de Estados terceros y evitar que información de seguridad sensible se comparta con autoridades de países terceros.

89 La obligación de la UE de propiedad y control no solo es aplicable a los beneficiarios de subvenciones, sino también a sus subcontratistas y a los perceptores de apoyo financiero a terceros. Salvo la última categoría (véanse los apartados ***92*** a ***96***), el Servicio Central de Validación de la Agencia Ejecutiva Europea de Investigación es el encargado de llevar a cabo la evaluación. Sin embargo, la decisión final relativa a la posibilidad de participar en convocatorias restringidas sigue correspondiendo a la autoridad que concede las ayudas, como, por ejemplo, la DG Redes de Comunicación, Contenido y Tecnologías o el Centro Europeo de Competencia en Ciberseguridad.

90 Durante nuestro trabajo de auditoría, los beneficiarios mencionaron reiteradamente los problemas prácticos que planteaban las evaluación de la propiedad y el control. La evaluación de la propiedad y el control de la UE puede resultar un proceso complejo y dilatado. Requiere un análisis completo de la estructura de la propiedad y la cadena de control de cada organización que comprenda todos los niveles de la propiedad hasta los propietarios últimos. El Servicio Central de Validación exige que cada entidad facilite amplia evidencia documental de su estructura de propiedad y sus derechos específicos, gobernanza corporativa y vínculos comerciales, financieros o de otro tipo que confieran control.

91 En tres proyectos de nuestra muestra financiados por la UE, al menos un beneficiario de un consorcio fue posteriormente excluido por considerarse que su propiedad y control correspondía a países terceros. La exclusión de miembros de consorcios muestra que no todos los participantes en el Programa Europa Digital comprenden del todo la noción de propiedad y control. En conjunto, a partir de datos del Servicio Central de Validación, el 7 % de los solicitantes de subvenciones o subcontratistas del Programa Europa Digital no superaron la evaluación en el período 2022-2025. La presentación de propuestas en respuesta a una convocatoria por participantes inadmisibles provoca retrasos, como se muestra en el ***recuadro 4***.

Recuadro 4

Ejemplo de un caso de exclusión de los beneficiarios porque no superaron los controles de seguridad

Dos de los miembros del consorcio del proyecto NG-SOC (proyecto 7 del ***anexo III***) no superaron la evaluación de la propiedad y el control. El resultado fue anunciado alrededor de un mes antes del plazo de firma del convenio de subvención.
El coordinador del proyecto tuvo que acceder a asumir el trabajo que se había asignado a los dos miembros excluidos, pues no había tiempo para buscar a un nuevo socio. Unos de los miembros excluidos pertenecía a un sector en el que iba a ponerse a prueba la solución desarrollada. Por tanto, una parte significativa del proyecto, consistente en probar las soluciones en la práctica, no podría llevarse a cabo según lo previsto. Posteriormente la situación se remedió modificando el convenio de subvención para aceptar miembros nuevos.

Fuente: Tribunal de Cuentas Europeo.

92 Dos de los proyectos que examinamos (NCC-IE y CYberSynchrony) proporcionan apoyo financiero a terceros. Este mecanismo de financiación permite a los beneficiarios de subvenciones utilizar parte de estos fondos para financiar a otras entidades a través de convocatorias abiertas. El apoyo financiero a terceros puede facilitar el acceso a financiación de la UE. En tal caso, los beneficiarios son los únicos responsable de realizar las evaluaciones de la propiedad y el control, sin la intervención del Servicio Central de Validación.

93 En 2021, la Comisión publicó orientaciones públicas generales para los solicitantes de convocatorias restringidas, actualizadas en 2026. Aunque el apoyo financiero a terceros existe desde 2021 para las convocatorias del Programa Europa Digital, ni la Comisión ni el Centro Europeo de Competencia en Ciberseguridad han facilitado a los beneficiarios una metodología pormenorizada sobre como practicar evaluaciones de la propiedad y el control a los terceros que reciben su apoyo financiero. En julio de 2025, el Centro Europeo de Competencia en Ciberseguridad emitió orientaciones no vinculantes, en las que proporcionaba a la red de centros nacionales de coordinación un enfoque estructurado sobre las evaluaciones de la propiedad y el control. El documento de orientación contiene principios y procedimientos generales que pueden adoptarse. Sin embargo, las orientaciones no especifican cómo deben llevarse a cabo las evaluaciones, y dejan a cargo de los beneficiarios el desarrollo de su propio enfoque.

94 Constatamos que el Centro Europeo de Competencia en Ciberseguridad no valida la metodología adoptada por los beneficiarios ni efectúa comprobaciones por muestreo para garantizar que la metodología es suficientemente rigurosa y que los perceptores de apoyo financiero seleccionados son verdaderamente de propiedad y control de la UE.

95 En nuestro Informe Anual relativo al ejercicio 2024 constatamos que los beneficiarios a los que la Comisión encomendó gestionar la ayuda financiera a terceros (en el ámbito de la investigación) no estaban obligados a demostrar la eficacia de sus controles para garantizar la regularidad del gasto de la UE. Tampoco el Centro Europeo de Competencia en Ciberseguridad evalúa la capacidad administrativa y técnica de los beneficiarios para gestionar adecuadamente las evaluaciones de la propiedad y el control. Como se explica en el apartado ***90***, esta evaluación puede ser compleja y en la UE es realizada por un servicio específico que cuenta con conocimientos especializados.

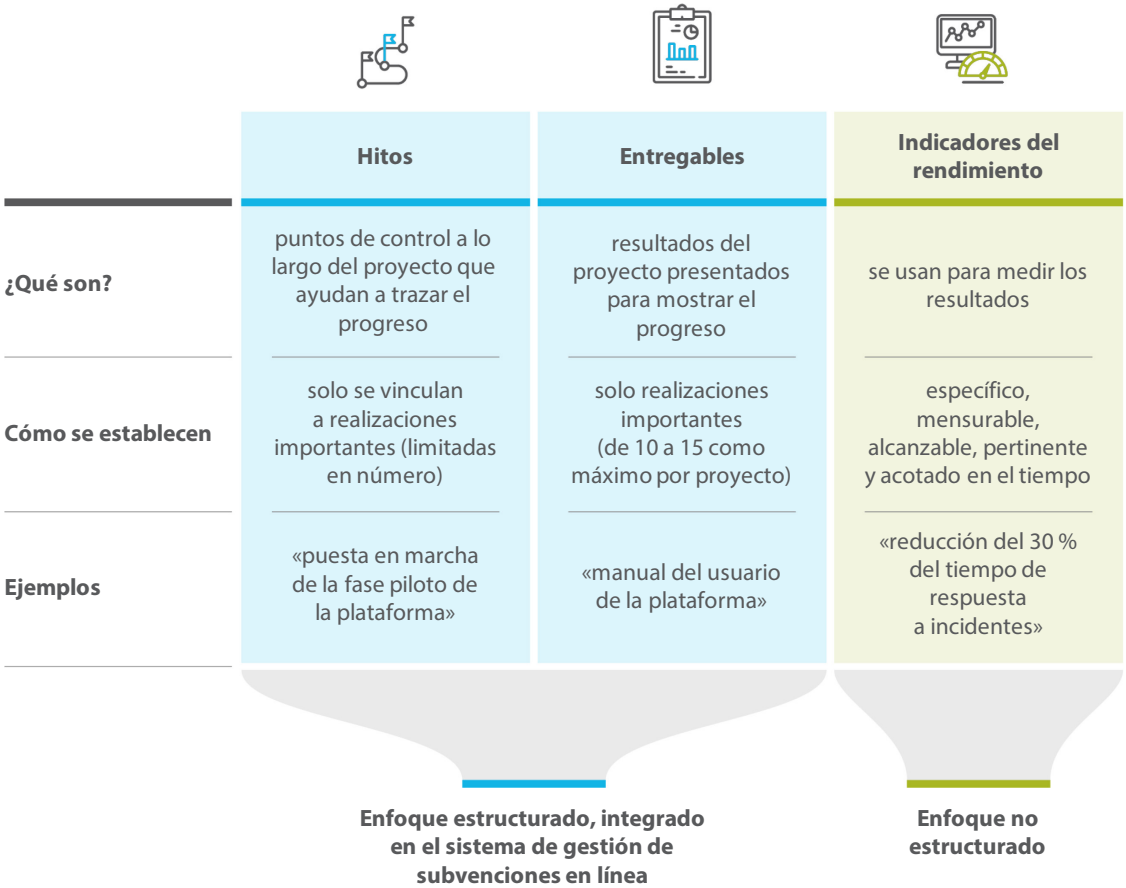
96 En este contexto, consideramos que existe un riesgo significativo de que los beneficiarios, responsables de las evaluaciones de la propiedad y el control, no sean capaces de practicarlas debidamente. Debido a la naturaleza de las actividades financiadas, esta deficiencia podría poner al descubierto infraestructura sensible, datos operativos y tecnologías críticas para la seguridad.

La mayoría de los proyectos financiados por la UE tienen marcos de rendimiento inadecuados, y los datos de rendimiento relativo a la ciberseguridad del Programa Europa Digital no son exactos

La mayoría de los proyectos financiados por la UE tienen marcos de rendimiento inadecuados

97 Los beneficiarios de proyectos financiados por la UE deben notificar sus progresos y resultados al Centro Europeo de Competencia en Ciberseguridad a través de hitos, entregables e indicadores, como se muestra en la ***ilustración 8***. Evaluamos si los hitos y los entregables establecidos para cada proyecto permiten adecuadamente el seguimiento de los proyectos. Evaluamos asimismo si los indicadores de rendimiento del proyecto son pertinentes y mensurables, y tienen una base de referencia y un objetivo.

Ilustración 8 | Hitos, entregables e indicadores de rendimiento en los proyectos del Programa Europa Digital



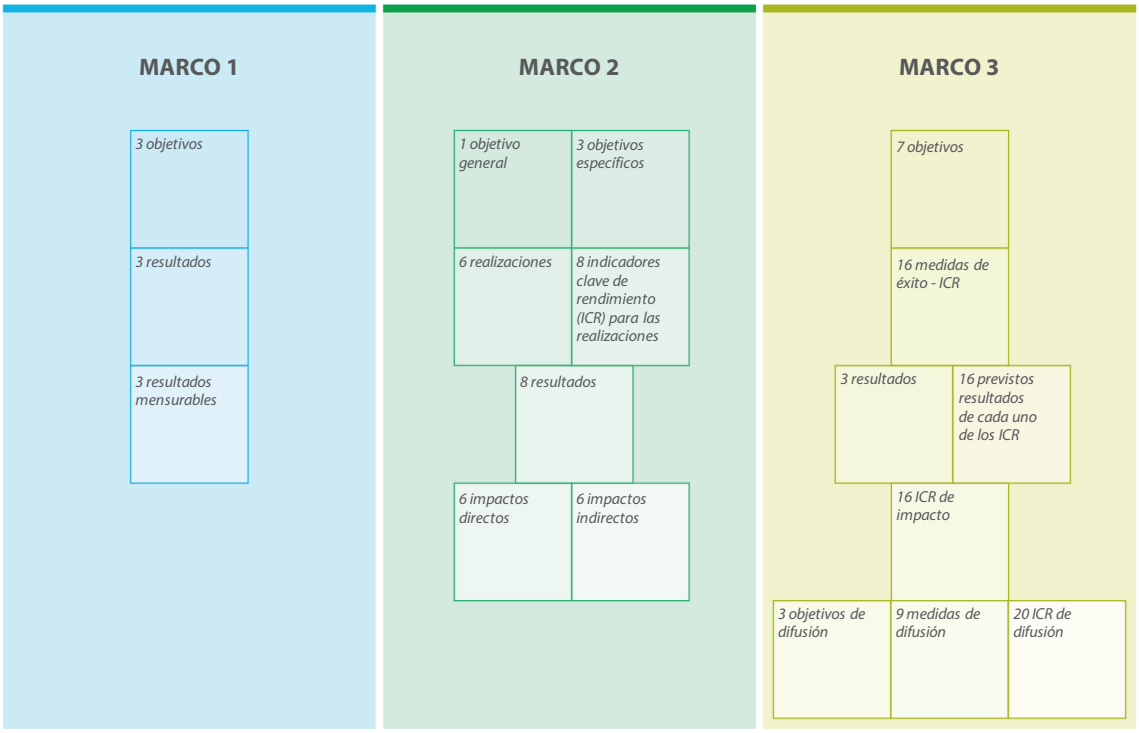
Fuente: Tribunal de Cuentas Europeo, a partir del formulario de solicitud de subvención.

98 En su propuesta de proyecto, los beneficiarios deben establecer una serie de hitos y entregables con arreglo a un sistema estructurado que se especifica en las instrucciones a los solicitantes. La lista de todos los hitos y entregables figura en el sistema de gestión de subvenciones en línea para facilitar su supervisión. El Centro Europeo de Competencia en Ciberseguridad examina normalmente cada proyecto dos veces: una a mitad del proyecto, y otra una vez que este se ha completado. Durante estos exámenes, los expertos externos verifican el cumplimiento de hitos y entregables, y el Centro los valida. Por consiguiente, los hitos y entregables son fundamentales para la supervisión de los proyectos y deben definirse adecuadamente.

99 Constatamos que casi ninguno de los proyectos de nuestra muestra seguía las instrucciones relativas al número de hitos y entregables: el número de hitos por proyecto oscila entre ocho y treinta y nueve, y el número de entregables, entre ocho y cuarenta y cinco. Muchos de los hitos y entregables no acatan las instrucciones (por ejemplo, «reunión para iniciar la elaboración de la convocatoria de propuestas de investigación» o «actas formales de la reunión sobre el proyecto») sobre cómo deben elaborarse, por lo que no sirven para supervisar el progreso. En tres proyectos, el comité de evaluación había detectado estos problemas antes de la firma de las subvenciones. En dos casos, los beneficiarios solo propusieron modificaciones menores (por ejemplo, de los plazos) sin abordar los problemas principales, mientras que el tercero no realizó ninguna modificación. En otros seis proyectos de nuestra muestra, nuestro análisis revela que los hitos o entregables no concuerdan con las instrucciones y no son siempre adecuados. Consideramos que contar con entregables e hitos mal definidos o en un número excesivo dificulta el seguimiento de sus avances.

100 A diferencia de los hitos y entregables, los indicadores de rendimiento no siguen un enfoque estructurado y no están consolidados en un cuadro del sistema de gestión de subvenciones, sino que pueden encontrarse en diferentes secciones de la propuesta. Este enfoque ha dado lugar a que los beneficiarios propongan múltiples marcos de rendimiento. Aunque algunos han establecido objetivos de proyectos vinculados a indicadores de rendimiento, otros han establecido marcos de rendimiento mucho más complejos. En la ***ilustración 9*** se presentan algunos ejemplos.

Ilustración 9 | Ejemplo de la diversidad de marcos de rendimiento diseñados para los proyectos



Fuente: Tribunal de Cuentas Europeo.

101 Tras nuestro análisis, concluimos que muchos de los indicadores de rendimiento empleados por los proyectos no son pertinentes o mensurables y carecen de un objetivo o de un valor de referencia (véase el ***recuadro 5***). Además, siete proyectos han definido veinte o más indicadores, y un proyecto, cincuenta y dos. Presentamos los resultados de esta evaluación en el ***anexo IV***.

Recuadro 5

Ejemplos de indicadores de rendimiento inadecuados

No mensurables:

- «Indicador de compromiso y otros servicios prestados refuerzan las capacidades de ciberseguridad de las pymes»
- «Entrega de herramientas y métodos de respuesta a incidentes que permiten la integración con canales de comunicación de EU-CyCLONe»

No provistos de valor de referencia u objetivo:

- «Mejora del ≥ 20 % en la preparación de la plantilla»
- «Reducción del ≥ 20 % del esfuerzo necesario para atenerse a las iniciativas de seguridad de la UE pertinentes y garantizar su cumplimiento»

No relativos al rendimiento:

- «Informe definitivo sobre el proyecto al final de la fase de financiación»
- «Número de personas en prácticas que participarán en todas las sesiones de formación»

Fuente: Tribunal de Cuentas Europeo, a partir de la documentación de los proyectos.

102 En conjunto, consideramos que la amplia variedad de marcos de rendimiento, la deficiente configuración de los indicadores y el número excesivo de estos complica considerablemente la supervisión del rendimiento. Por tanto, no es posible evaluar debidamente el rendimiento de los proyectos, y esto se complica aún más por el hecho de que la plantilla de notificación no contiene una sección específica sobre los indicadores de rendimiento del proyecto, por lo que la mayoría de los proyectos de nuestra muestra no facilitó información sobre estos.

Los datos de rendimiento del componente de ciberseguridad del Programa Europa Digital no son exactos

103 Para supervisar los logros del Programa Europa Digital, el Reglamento proporciona indicadores de los programas sobre los cuales deben informar todos los proyectos, como se explica en el ***recuadro 6***.

Recuadro 6

Indicadores del Programa Europa Digital relativos a la ciberseguridad

1.a Número de infraestructuras o herramientas de ciberseguridad contratadas conjuntamente, también en el contexto del Sistema Europeo de Alerta de Ciberseguridad

1.b Número de infraestructuras o herramientas de ciberseguridad desplegadas

2. Número de usuarios y de comunidades de usuarios con acceso a instalaciones europeas de ciberseguridad

3. Número de acciones de apoyo a la preparación frente a incidentes de ciberseguridad y la respuesta a ellos en el marco del Mecanismo de Emergencia en materia de Ciberseguridad

Fuente: Anexo II al Reglamento (UE) 2021/694 por el que se establece el Programa Europa Digital., y el marco de supervisión y evaluación del Programa Europa digital (SWD(2024) 37).

104 Evaluamos si los proyectos de nuestra muestra habían informado sobre estos indicadores y examinado cómo recaba y verifica los datos el Centro Europeo de Competencia en Ciberseguridad.

105 Todos los proyectos deben informar sobre los indicadores del Programa Europa Digital antes de los exámenes intermedio y final en el sistema de gestión de subvenciones. Constatamos que, solo tres de los siete proyectos que estaban a mitad de su ejecución durante nuestra auditoría y que, por tanto, deberían haber informado sobre estos indicadores, lo habían hecho. Dos de estos tres no habían comunicado información exacta: uno informó sobre el indicador equivocado, y el otro facilitó valores objetivos en lugar de resultados logrados.

106 Cada año, la Comisión informa sobre estos indicadores en sus declaraciones de rendimiento de los programas. Esto permite a las partes interesadas evaluar si el programa está obteniendo sus objetivos. Según las declaraciones de rendimiento de los programas de 2024, los indicadores de ciberseguridad del Programa Europa Digital están en vías de lograr sus objetivos. El Centro Europeo de Competencia en Ciberseguridad nos ha explicado que utilizó una serie de encuestas enviadas a los beneficiarios de los proyectos para contabilizar estos indicadores en lugar de basarlos en el sistema de gestión de subvenciones. Examinamos los datos desagregados facilitados por el Centro y encontramos numerosos problemas en la recogida de datos y en su calidad global. Constatamos que los datos recabados no concuerdan con los valores presentados en a declaración de rendimiento del programa, por lo que no está claro cómo se han calculado los valores notificados. No encontramos pruebas de que el Centro verificara la exactitud de los datos notificados. Basándonos en nuestros controles de los proyectos de la muestra, teniendo en cuenta que la mayoría de los valores faltan o no son exactos, consideramos que los datos notificados no reflejan adecuadamente los resultados obtenidos.

El presente informe ha sido aprobado por la Sala III, presidida por George Marius Hyzler, Miembro del Tribunal de Cuentas, en Luxemburgo, en su reunión de 16 de junio de 2026.

Por el Tribunal de Cuentas Europeo

Tony Murphy
Presidente

Anexos

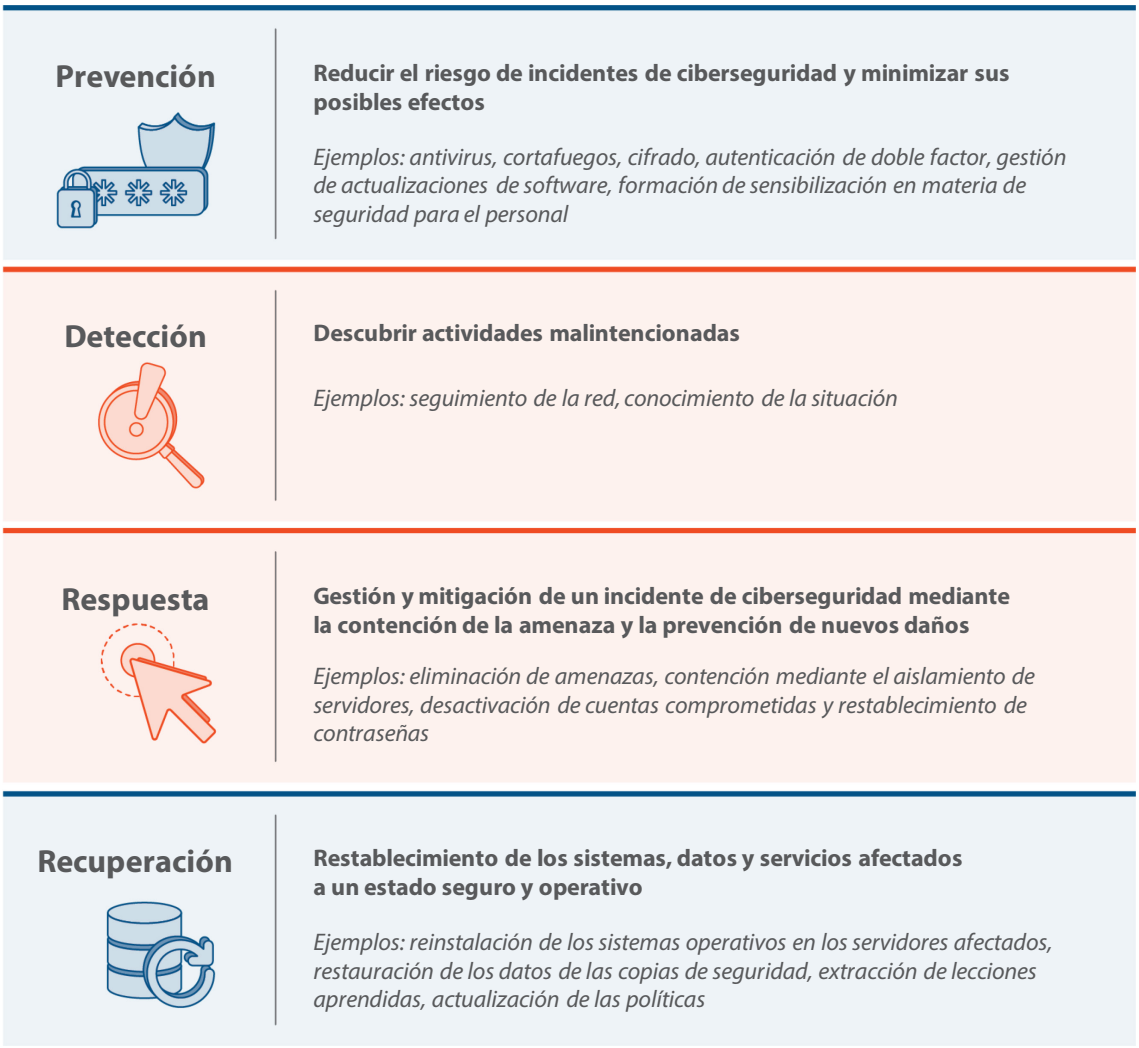
Anexo I – Sobre la auditoría

01 La ciberseguridad se define como «todas las actividades necesarias para la protección de las redes y los sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas»[1]. Se entiende por «ciberamenaza» cualquier «situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas»[2]. La ciberseguridad exige un enfoque holístico, consistente en una serie de actividades interrelacionadas para la prevención y la detección de ciberamenazas, y para la respuesta y la recuperación frente a estas, como se muestra en la ***ilustración 1***.

[1] Reglamento (UE) 2019/881 (Reglamento sobre la Ciberseguridad).

[2] Artículo 2 del Reglamento sobre la Ciberseguridad

Ilustración 1 | Ejemplos de actividades de ciberseguridad

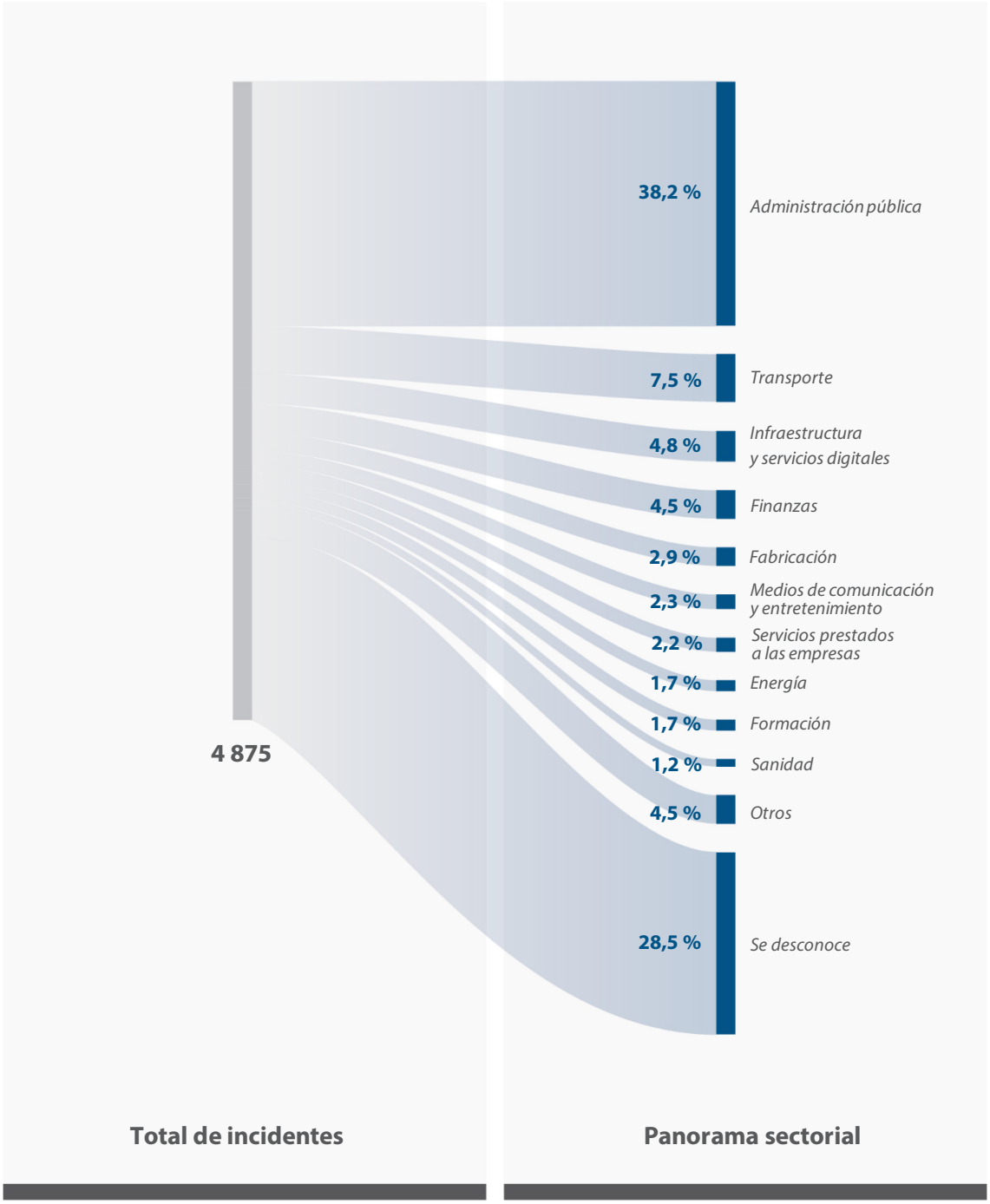


Fuente: Tribunal de Cuentas Europeo, a partir del considerando 78 de la Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2).

02 La Agencia de la Unión Europea para la Ciberseguridad (ENISA) considera que el nivel de ciberamenaza es sustancial, y observa que el panorama de ciberamenazas ha llegado a ser y sigue siendo significativamente más complejo[3]. Estas amenazas revelan la vital importancia de la ciberseguridad en economías y sociedades cada vez más digitales. En su panorama de amenazas de 2025, la ENISA identificó los programas de secuestro como la amenaza más crítica en la UE. En la ***ilustración 2*** se muestran los sectores afectados.

[3] Informe de 2024 sobre la situación de la ciberseguridad en la Unión de la ENISA.

Ilustración 2 | Sectores objeto de ciberataques



Fuente: Tribunal de Cuentas Europeo, a partir de datos de la ENISA.

Incidentes de ciberseguridad significativos o a gran escala

03 Los incidentes de ciberseguridad, entre los que se cuentan las ciberamenzas y los incidentes accidentales (como los mencionados en la ***ilustración 3*** y en el apartado ***40***), «pueden obstaculizar la prestación de servicios públicos, [y] el desarrollo de actividades económicas, […] generar pérdidas económicas sustanciales, socavar la confianza de los usuarios, causar graves daños a las economías y a los sistemas democráticos de la Unión e incluso suponer una amenaza para la salud o la vida[4]». Los incidentes de ciberseguridad se consideran[5]:

- **significativos** si han causado o pueden causar alteraciones operativas importantes de los servicios o pérdidas financieras para la entidad, o han afectado o puedan afectar a otras personas físicas o jurídicas al causar daños materiales o inmateriales considerables;

- **a gran escala** si han causado perturbaciones que superan la capacidad de un Estado miembro para responder a ellos o afecta significativamente por lo menos a dos Estados miembros.

04 Los incidentes de ciberseguridad a gran escala pueden intensificarse y convertirse en una **crisis propiamente dicha en el ámbito de la Unión** que impida el correcto funcionamiento del mercado interior o plantee graves riesgos para la seguridad y la protección públicas de las entidades o los ciudadanos de varios Estados miembros o del conjunto de la Unión[6].

---

[4] Considerando 2 del Reglamento (UE) 2025/38 (el Reglamento de Cibersolidaridad).

[5] Artículos 6 y 23 de la Directiva SRI 2, más detallados en el Reglamento de Ejecución (UE) 2024/2690 de la Comisión para algunos proveedores del sector de la infraestructura digital.

[6] Considerando 69 de la Directiva SRI 2

Marco político de la UE

05 El ecosistema cibernético de la UE es complejo, multidimensional y afecta a varios ámbitos políticos internos, como Justicia y Asuntos de Interior, Mercado Único Digital y Políticas de Investigación[7]. En política exterior, la ciberseguridad afecta a la diplomacia y cada vez está más integrada en la emergente política de defensa de la UE[8].

06 En los últimos años, la UE ha reforzado su marco normativo en materia de ciberseguridad. En la ***ilustración 3*** se presenta la legislación y los instrumentos políticos más relevantes en la UE. De acuerdo con el alcance de nuestra auditoría (véanse los apartados ***13*** y ***14***), nos hemos centrado en los instrumentos destinados a detectar incidentes de ciberseguridad significativos y a gran escala, y darles respuesta.

[7] Documento informativo del Tribunal de Cuentas Europeo «Desafíos de una política eficaz de ciberseguridad en la UE», p. 13.

[8] Por ejemplo, la Posición de la Unión Europea en materia de ciberseguridad (2022), el marco para una respuesta coordinada de la UE a las campañas híbridas (2022), la política de ciberdefensa de la UE (2023), y los Instrumentos de ciberdiplomacia (2023) revisados.

Ilustración 3 | Legislación e instrumentos políticos relevantes de la UE

Fuente: Tribunal de Cuentas Europeo.

Funciones y competencias

07 El entorno de ciberseguridad de la UE abarca numerosos agentes públicos y privados a escala regional, nacional y de la UE en el ámbito civil, incluidas las fuerzas policiales. La ciberseguridad es también un elemento clave de la seguridad y la defensa nacionales[9]. En el ***anexo II*** se muestra el panorama actual.

08 Los Estados miembros son los principales responsables de prevenir los incidentes y crisis de ciberseguridad que les afecten, prepararse para ellos y darles respuesta. Conforme al artículo 4, apartado 2, del Tratado de la Unión Europea la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro. Puesto que estos incidentes pueden ocasionar perturbaciones y daños en las infraestructuras críticas, de las que depende el correcto funcionamiento del mercado interior, la UE también desempeña un papel importante en caso de incidentes o crisis significativos[10]. Las principales entidades en el ámbito de la UE se presentan en la ***ilustración 4***.

[9] Dictamen 02/2023 sobre la propuesta relativa al Reglamento de Cibersolidaridad de la UE.

[10] Plan Director de la UE para la Gestión de Crisis de Ciberseguridad.

Ilustración 4 | Entidades de la UE que desempeñan una función clave en ciberseguridad

Fuente: Tribunal de Cuentas Europeo.

Financiación de la UE

09 En el actual marco financiero plurianual 2021-2027, la principal fuente de financiación de la ciberseguridad es el Programa Europa Digital. Lanzado en 2021, es el primer programa de la UE destinado específicamente a impulsar la transformación digital de la UE, con un presupuesto total de 8 100 millones de euros[11].

10 El Programa Europa Digital financia acciones de ciberseguridad en virtud de su objetivo específico 3: «Ciberseguridad y confianza». Concretamente, existe un presupuesto de 1 400 millones de euros para:

- reforzar la coordinación en ciberseguridad entre las herramientas y las infraestructuras de datos de los Estados miembros;
- apoyar el amplio despliegue de las recientes soluciones en materia de ciberseguridad en toda la economía.

11 La mayor parte de la financiación del Programa Europa Digital destinada a la seguridad se proporciona a través de convocatorias de propuestas, y se han lanzado doce convocatorias entre noviembre de 2021 y diciembre de 2025. La financiación de la UE disponible para estas convocatorias asciende a 825 millones de euros. Se han previsto nuevas convocatorias para 2026 y 2027, a fin de asignar otros 212 millones de euros en subvenciones.

12 Otro programa importante de la UE que apoya la ciberseguridad es Horizonte Europa. Los proyectos de ciberseguridad se financian principalmente a través del bloque 3: «Seguridad civil para la sociedad», y suelen estar en una fase temprana de madurez debido a que Horizonte Europa se centra en la investigación y la innovación. El Mecanismo de Recuperación y Resiliencia también aporta financiación para medidas de ciberseguridad.

[11] Programa Europa Digital.

Alcance y enfoque de la auditoría

13 El aumento de las ciberamenazas y su posible repercusión han puesto de manifiesto la necesidad de reforzar nuestra ciberresiliencia colectiva. Nuestra auditoría tenía como objetivo evaluar si las acciones de la UE ayudan a los Estados miembros a detectar incidentes de ciberseguridad significativos y a gran escala y a responder a ellos. En particular, evaluamos si esto era así con respecto a:

- las redes y los mecanismos de la UE (a saber, la red de CSIRT, la red de EU-CyCLONe, el Sistema Europeo de Alerta de Ciberseguridad, el centro de situación cibernética y la Reserva de Ciberseguridad de la UE);
- acciones financiadas en el marco del Programa Europa Digital.

No abarcamos la cooperación policial en el ámbito de la UE ni las medidas de ciberdisuasión emprendidas en la UE a través de medidas diplomáticas o actividades de defensa.

14 La auditoría abarca el período comprendido entre 2022 y 2025. Se basa en un control documental y un análisis de documentos pertinentes, visitas de auditoría a tres Estados miembros (Irlanda, Grecia e Italia), y cuestionarios escritos y entrevistas con las partes interesadas. En la ***ilustración 5*** se muestra cómo recabamos las pruebas para nuestras observaciones.

Ilustración 5 | Trabajo de auditoría realizado

Examinamos

- El **marco jurídico** aplicable a la detección de incidentes de ciberseguridad significativos y a gran escala y a la respuesta a ellos
- Las **funciones y responsabilidades** de las redes y estructuras creadas en el ámbito de la UE

Analizamos

- Documentos sobre el funcionamiento de las **redes de CSIRT** y de **EU-CyCLONe**
- Documentación sobre el **marco de programación y seguimiento del rendimiento del Programa Europa Digital**
- Documentación sobre **13 acciones financiadas por la UE seleccionadas** (11 subvenciones y 2 contratos; véase la lista detallada en el anexo III)

* Hemos seleccionado acciones financiadas por la UE en tres países (Irlanda, Grecia e Italia) en los que la financiación pertinente del Programa Europa Digital era más significativa. Las 11 subvenciones se extrajeron de una lista de 137 proyectos financiados por la UE pertinentes para detectar amenazas y darles respuesta, a efectos de abarcar una combinación diversa de proyectos.

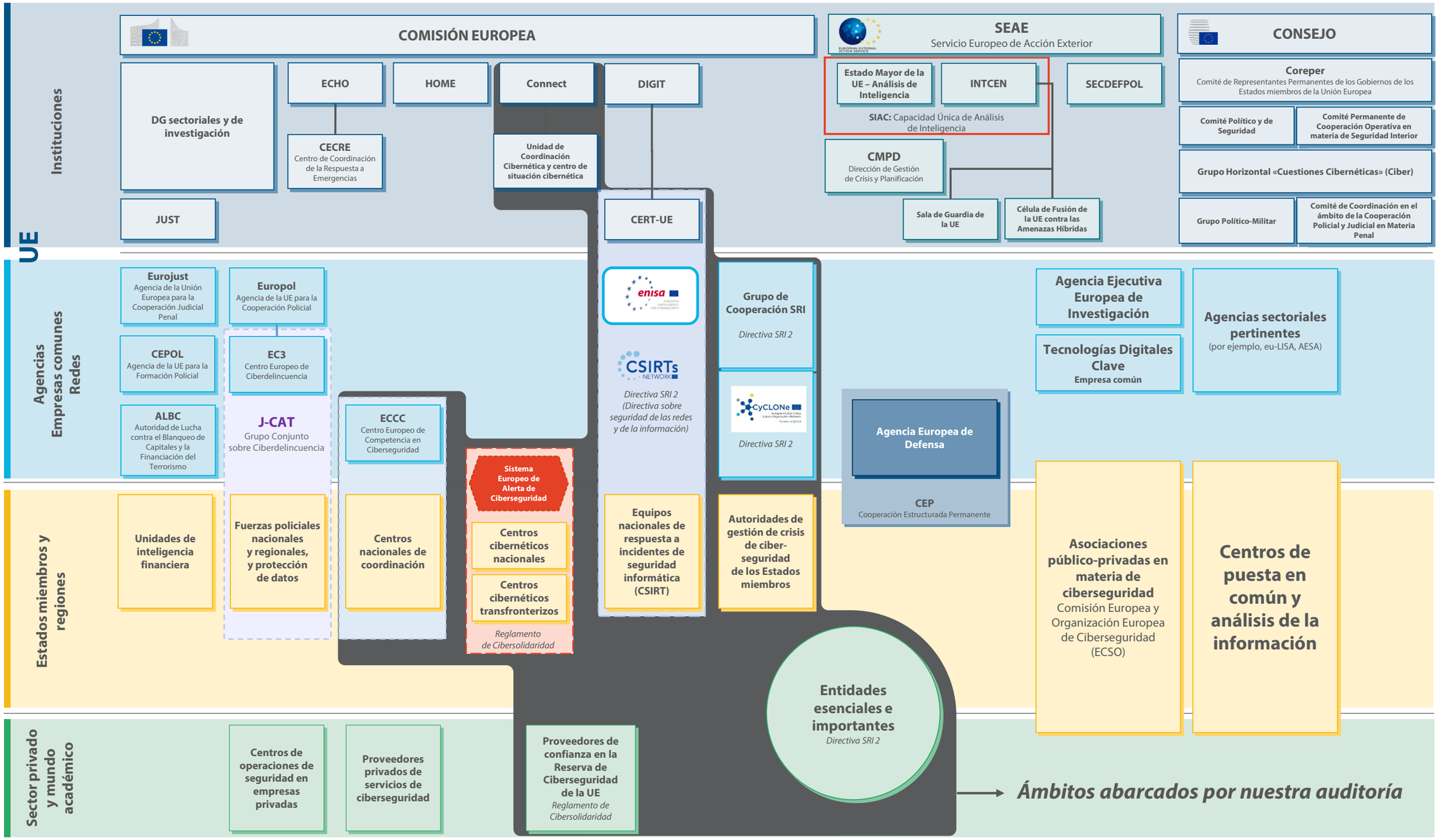
Entrevistamos a

- Beneficiarios de las **11 subvenciones financiadas por la UE incluidas en la muestra**
- Representantes de las autoridades nacionales de ciberseguridad de **tres Estados miembros** (Irlanda, Grecia e Italia)
- Representantes de la Comisión Europea (**DG Redes de Comunicación, Contenido y Tecnologías**), la **ENISA** y el **Centro Europeo de Competencia en Ciberseguridad**

Fuente: Tribunal de Cuentas Europeo.

15 Esperamos que nuestras conclusiones contribuyan a mejorar la eficacia y la eficiencia de la UE para detectar incidentes de ciberseguridad significativos y a gran escala, y para darles respuesta, y el modo en que las acciones financiadas por la UE se seleccionan y supervisan. Nuestra metodología de auditoría cumple con las normas internacionales de auditoría emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI).

Anexo II – Entorno de ciberseguridad de la UE



DG Connect: Dirección General de Redes de Comunicación, Contenido y Tecnologías
DG ECHO: Dirección General de Protección Civil y Operaciones de Ayuda Humanitaria Europeas

DG HOME: Dirección General de Migración y Asuntos de Interior
DG JUST: Dirección General de Justicia y Consumidores
DG Servicios Digitales: Dirección General de Servicios Digitales
AESA: Agencia de la Unión Europea para la Seguridad Aérea

EU-CyCLONe: Red de organizaciones de enlace nacionales para la gestión de cibercrisis
eu-LISA: Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia

INTCEN: Centro de Inteligencia y de Situación de la Unión Europea
SECDEFPOL: Política de Seguridad y Defensa **Centro de operaciones de seguridad**

Anexo III – Acciones de ciberseguridad seleccionadas

Código	Título	Países	Fecha de inicio	Fecha de finalización	Coste total (en millones de euros) y contribución de la UE (%)	Enlace al Portal de Financiación y Licitaciones de la UE.
Subvenciones para centros cibernéticos transfronterizos que forman parte del Sistema Europeo de Alerta de Ciberseguridad						
1	**Establecimiento de centros de operaciones de seguridad transfronterizos (ATHENA)**	Bulgaria, Grecia, Chipre y Malta	1.1.2024	31.3.2028	4,7 (50 %)	
2	**PLATAFORMA TRANSFRONTERIZA ENSOC (ENSOC)**	España, Italia, Luxemburgo, Países Bajos, Austria, Portugal y Rumanía	1.1.2024	30.6.2028	10,4 (50 %)	
Subvenciones para desplegar la red de centros nacionales de coordinación en los Estados miembros						
3	**Desarrollo y aplicación del Centro Nacional de Coordinación y Desarrollo de la Ciberseguridad de Irlanda (NCC-IE)**	Irlanda	2.10.2023	1.10.2026	4,2 (47 %)	
4	**Centro Nacional de Coordinación de Italia (NCC-IT)**	Italia	1.11.2023	31.10.2025	2,0 (50 %)	

Código	Título	Países	Fecha de inicio	Fecha de finalización	Coste total (en millones de euros) y contribución de la UE (%)	Enlace al Portal de Financiación y Licitaciones de la UE.
Subvenciones para desarrollar la capacidad de los centros de operaciones de seguridad, promover nuevas aplicaciones de IA y otras tecnologías facilitadoras para los centros de operaciones de seguridad, y facilitar apoyo y asistencia mutua a la preparación						
5	**Mejora de la capacidad del Centro Helénico de Operaciones de Seguridad Consolidado (EL-SOC)**	Grecia y Chipre	1.1.2024	31.12.2026	9,7 (50 %)	
6	**Centro Griego de Operaciones de Seguridad para las Pequeñas y Medianas Empresas (GR-SME-SOC)**	Grecia	1.1.2024	31.12.2026	12,1 (50 %)	
7	**Centros de Operaciones de Seguridad de Próxima Generación (NG-SOC)**	Grecia, España, Chipre, Luxemburgo, Eslovenia y Noruega.	1.1.2024	31.12.2026	4,8 (50 %)	
8	**Centro de Operaciones de Seguridad de la Administración Local Irlandesa (ILG-SOC)**	Irlanda	1.10.2023	30.9.2026	8,3 (50 %)	
9	**Un ecosistema interconectado de redes de coordinación y respuesta en materia de ciberseguridad (Cyber-CORE-Network)**	Irlanda	1.1.2024	31.12.2026	3,6 (50 %)	
10	**Armonización de personas, procesos y tecnología para una ciberseguridad rigurosa (CYberSynchrony)**	Bélgica, Grecia, Italia, Chipre y Países Bajos.	1.6.2024	31.5.2027	7,0 (100 %)	
11	**Centros Avanzados de Operaciones de Seguridad Cooperativa (ACSOC)**	Grecia, Italia y Rumanía	1.1.2025	31.12.2027	3,0 (50 %)	

Código	Título	Países	Fecha de inicio	Fecha de finalización	Coste total (en millones de euros) y contribución de la UE (%)	Enlace al Portal de Financiación y Licitaciones de la UE.
Contrato marco para la acción de apoyo a la ciberseguridad de la ENISA						
12	**Apoyo a la ENISA en el suministro de servicios en virtud de la acción de apoyo a la ciberseguridad (28 lotes)**	27 lotes de los Estados miembros 1 lote paneuropeo	1.12.2022[1]	31.12.2025	28,3 (100 %)	
Contrato de servicios para el centro de situación cibernética de la DG Redes de Comunicación, Contenido y Tecnologías						
13	**Servicio a medida para prestar apoyo al centro de situación cibernética de la Comisión Europea**	-	30.12.2022	30.12.2026	18,0 (100 %)	

Fuente: Tribunal de Cuentas Europeo.

[1] Múltiples contratos suscritos a los largo de diciembre de 2022.

Anexo IV – Evaluación por el Tribunal de Cuentas Europeo de proyectos de ciberseguridad financiados por la UE

Satisfactorio
Insatisfactorio
Algunas insuficiencias
No es posible llegar a una conclusión (demasiado pronto para la convocatoria)

Código	Proyecto	El proyecto aborda la mayoría de las necesidades identificadas en la convocatoria	El proyecto ha alcanzado las realizaciones y los resultados previstos hasta la fecha	Los resultados del proyecto se han obtenido en la fecha prevista	Los indicadores de rendimiento del proyecto son pertinentes y mensurables, y tienen una base de referencia y un objetivo
1	Establecimiento de centros de operaciones de seguridad transfronterizos (ATHENA)	Satisfactorio	Insatisfactorio	Insatisfactorio	Insatisfactorio
2	PLATAFORMA TRANSFRONTERIZA ENSOC (ENSOC)	Satisfactorio	Insatisfactorio	Insatisfactorio	Insatisfactorio
3	Desarrollo y aplicación del Centro Nacional de Coordinación y Desarrollo de la Ciberseguridad de Irlanda (NCC-IE)	Satisfactorio	Satisfactorio	Algunas insuficiencias	Algunas insuficiencias
4	Centro Nacional de Coordinación de Italia (NCC-IT)	Satisfactorio	Satisfactorio	Satisfactorio	Algunas insuficiencias
5	Mejora de la capacidad del Centro Helénico de Operaciones de Seguridad Consolidado (EL-SOC)	Satisfactorio	Algunas insuficiencias	Insatisfactorio	Insatisfactorio
6	Centro Griego de Operaciones de Seguridad para las Pequeñas y Medianas Empresas (GR-SME-SOC)	Satisfactorio	Satisfactorio	Satisfactorio	Algunas insuficiencias
7	Centros de Operaciones de Seguridad de Próxima Generación (NG-SOC)	Satisfactorio	Satisfactorio	Satisfactorio	Algunas insuficiencias
8	Centro de Operaciones de Seguridad de la Administración Local Irlandesa (ILG-SOC)	Satisfactorio	Insatisfactorio	Insatisfactorio	Insatisfactorio
9	Un ecosistema interconectado de redes de coordinación y respuesta en materia de ciberseguridad (Cyber-CORE-Network)	Satisfactorio	Algunas insuficiencias	Algunas insuficiencias	Algunas insuficiencias
10	Armonización de personas, procesos y tecnología para una ciberseguridad rigurosa (CYberSynchrony)	Algunas insuficiencias	No es posible llegar a una conclusión (demasiado pronto para la convocatoria)	No es posible llegar a una conclusión (demasiado pronto para la convocatoria)	Algunas insuficiencias
11	Centros Avanzados de Operaciones de Seguridad Cooperativa (ACSOC)	Satisfactorio	No es posible llegar a una conclusión (demasiado pronto para la convocatoria)	No es posible llegar a una conclusión (demasiado pronto para la convocatoria)	Insatisfactorio

Siglas y acrónimos

Sigla/Acrónimo	Definición/Explicación
CSIRT	Equipo de respuesta a incidentes de seguridad informática
DG Connect	Directorate-General for Communications Networks, Content and Technology
DIGITAL	Digital Europe Programme
ECCC	European Cybersecurity Competence Centre
ENISA	Agencia de la Unión Europea para la Ciberseguridad
EU-CyCLONe	Red de organizaciones de enlace nacionales para la gestión de cibercrisis
NCC	National coordination centre
OCA	Ownership and control assessment
PTSA	Ayuda financiera a terceros
Pyme	Pequeña y mediana empresa
SAG	Strategic Advisory Group
SOC	Security operations centre
SRI	Seguridad de las redes y de la información

Glosario

Término	Definición/Explicación
Agente de riesgo	Individuo o grupo de individuos que, con intención maliciosa, daña, interrumpe servicios o roba información al explotar vulnerabilidades en sistemas, redes y dispositivos informáticos.
Centro cibernético	Plataforma centralizada que combina distintos servicios, herramientas y profesionales informáticos para mejorar la supervisión, la detección y el análisis de ciberamenazas, prevenir incidentes de ciberseguridad y apoyar la producción de inteligencia contra las ciberamenazas.
Centro de operaciones de seguridad	Unidad organizativa que trabaja para prevenir ciberamenazas y ciberincidentes y recopila información relacionada
Ciberamenaza	Uso potencial del ciberespacio para comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos o sistemas de información.
Incidente de ciberseguridad	Hecho que compromete la disponibilidad, autenticidad, integridad o confidencialidad de los datos o sistemas de información.
Incidente de ciberseguridad a gran escala	Incidente de ciberseguridad que causa perturbaciones que superan la capacidad de un Estado miembro para responder a él o que afecta significativamente por lo menos a dos Estados miembros.
Incidente de ciberseguridad significativo	Incidente de ciberseguridad que ha causado o puede causar perturbaciones o pérdidas económica graves para una organización, o daños considerables para otras entidades o individuos.
Programa de secuestro	Programa malicioso que niega a las víctimas el acceso a un sistema informático o que encripta los archivos para volverlos ilegibles, y que con frecuencia obliga a la víctima a pagar un rescate para restablecer el acceso.
Taxonomía	En el contexto de la ciberseguridad, sistema de clasificación empleado para organizar, categorizar y estructurar los conocimientos sobre conceptos clave como amenazas e incidentes.

Respuestas de la Comisión

https://www.eca.europa.eu/es/publications/SR-2026-19

Respuestas del Centro Europeo de Competencia en Ciberseguridad

https://www.eca.europa.eu/es/publications/SR-2026-19

Respuestas de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

https://www.eca.europa.eu/es/publications/SR-2026-19

Cronología

https://www.eca.europa.eu/es/publications/SR-2026-19

Equipo auditor

En los informes especiales del Tribunal de Cuentas Europeo se exponen los resultados de las auditorías de las políticas y programas de la UE o de cuestiones de gestión a partir de ámbitos presupuestarios específicos. El Tribunal selecciona y concibe estas tareas de auditoría con el fin de que tengan la máxima repercusión teniendo en cuenta los riesgos relativos al rendimiento o a la conformidad, el nivel de ingresos y de gastos correspondiente, las futuras modificaciones y el interés político y público.

La presente auditoría de gestión fue llevada a cabo por la Sala III (Acciones exteriores, seguridad y justicia), presidida por George-Marius Hyzler, Miembro del Tribunal de Cuentas Europeo. La auditoría fue dirigida por George-Marius Hyzler, Miembro del Tribunal, con la asistencia de Romuald Kayibanda, jefe de Gabinete, y Annette Farrugia, agregada de Gabinete; Cyril Messein, gerente principal; Frédéric Soblet, jefe de tarea, y los auditores Jurgen Manjé y Flavia Di Marco. Zoe Amador Martínez prestó asistencia lingüística. Dunja Weibel proporcionó apoyo gráfico.

De izquierda a derecha: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé y Cyril Messein.

DERECHOS DE AUTOR

HTML	ISBN 978-92-849-7861-8	ISSN 1977-5687	doi:10.2865/5435479	QJ-01-26-032-ES-Q
PDF	ISBN 978-92-849-7862-5	ISSN 1977-5687	doi:10.2865/3766654	QJ-01-26-032-ES-N

CÓMO CITAR EL DOCUMENTO

Tribunal de Cuentas Europeo, Informe Especial 19/2026 «Detección y respuesta ante incidentes relacionados con la ciberseguridad – Progresa el marco de cooperación de la UE, pero es solo parcialmente eficaz por los retrasos en la aplicación y el escaso intercambio de información», Oficina de Publicaciones de la Unión Europea, 2026.

En los últimos años, la UE ha reforzado el marco regulador de la ciberseguridad y ha establecido redes y mecanismos para afrontar los incidentes de ciberseguridad. La UE también financia proyectos de ciberseguridad a través del Programa Europa Digital.

Concluimos que las acciones de la UE solo facilitan parcialmente la detección de incidentes de ciberseguridad significativos y a gran escala, y la respuesta ante estos. Aunque se ha instaurado gradualmente un marco de cooperación, aún se está trabajando para lograr su establecimiento definitivo. El intercambio limitado de información, las deficiencias en la notificación y los considerables retrasos en la aplicación impiden que las redes y mecanismos de la UE alcancen todo su potencial. Los proyectos persiguen objetivos pertinentes, pero varios se enfrentan a retos operativos y retrasos. Además, el marco general de seguimiento del rendimiento presenta insuficiencias. Formulamos recomendaciones para abordar estas deficiencias.

Informe Especial del Tribunal de Cuentas Europeo con arreglo al artículo 287, apartado 4, párrafo segundo, del TFUE.

TRIBUNAL DE CUENTAS EUROPEO

Oficina de Publicaciones de la Unión Europea

TRIBUNAL DE CUENTAS EUROPEO
12, rue Alcide De Gasperi
L-1615 Luxemburgo
LUXEMBURGO

Tel. +352 4398-1

Preguntas: eca.europa.eu/es/contact
Sitio web: eca.europa.eu
Redes sociales: @EUauditors