ES 2022

05

Informe especial

Ciberseguridad de las instituciones, órganos y organismos de la UE:

En general, el nivel de preparación no es proporcional a las amenazas

TRIBUNAL
DE CUENTAS
EUROPEO

Índice

Apartados

Resumen I-VII

Introducción 01-12

¿Qué es la ciberseguridad? 01-03

Ciberseguridad en las instituciones, órganos y organismos de la UE 04-12

Alcance y enfoque de la auditoría 13-19

Observaciones 20-94

El grado de madurez de las IOUE con respecto a la ciberseguridad es muy variable, y no siempre se ajusta a la buena práctica 20-44

La gobernanza de la seguridad informática en las IOUE no suele estar bien desarrollada y las evaluaciones de riesgo no son exhaustivas 21-29

Las IOUE no abordan la ciberseguridad de manera uniforme y no siempre cuentan con controles esenciales 30-38

Varias IOUE carecen de medidas de ciberseguridad sujetas a garantías independientes regulares 39-44

Las IOUE han establecido mecanismos de cooperación, pero presentan deficiencias 45-63

Existe una estructura formal para que las IOUE coordinen sus actividades, aunque presentan algunos problemas de gobernanza 46-53

Todavía no se han aprovechado plenamente las potenciales sinergias a través de la cooperación 54-63

La ENISA y el CERT-UE todavía no han proporcionado a las IOUE todo el apoyo que necesitaban 64-94

La ENISA es un actor clave en la ciberseguridad de la UE, pero su apoyo solo ha llegado a muy pocas IOUE 65-73

El CERT-UE por sus componentes, pero sus medios no están a la altura de los actuales desafíos de ciberseguridad 74-94

Conclusiones y recomendaciones 95-100

Anexos

Anexo I — Lista de IOUE incluidas en la encuesta

Anexo II — Información adicional sobre los principales comités interinstitucionales

Siglas y acrónimos

Glosario

Respuestas de la Comisión

Respuestas del CERT-UE y la ENISA

Plazo

Resumen

I El Reglamento sobre la Ciberseguridad de la UE define la ciberseguridad como «todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas». Debido a la información delicada que tratan, las instituciones, órganos y organismos de la UE (IOUE) son un blanco atractivo para los posibles atacantes, en particular para los grupos capaces de ejecutar ataques sigilosos muy sofisticados con fines de ciberespionaje, entre otros. Las IOUE están estrechamente interconectadas pese a su independencia institucional y si autonomía administrativa. En consecuencia, los puntos débiles de una IOUE pueden exponer a las demás a amenazas de seguridad.

II Dado que el número de ciberataques contra ellas está aumentando considerablemente, el objetivo de esta auditoría era determinar si las IOUE, en conjunto, han establecido mecanismos adecuados para protegerse contra las ciberamenazas. Concluimos que el nivel de preparación la comunidad de IOUE no está a la altura de las amenazas.

III Constatamos que no siempre se aplicaban buenas prácticas esenciales de ciberseguridad, como algunos controles esenciales, y que los gastos en ciberseguridad en varias IOUE son insuficientes. En algunas IOUE tampoco existe una buena gobernanza de la ciberseguridad: en muchos casos, no existen estrategias de seguridad informática, o estas no están respaldadas por la alta dirección, las políticas de seguridad no siempre se formalizan y las evaluaciones de riesgos no abarcan todo el entorno informático. No todas las IOUE disponen de medidas regulares de ciberseguridad sujetas a una garantía independiente.

IV La formación sobre ciberseguridad no es siempre sistemática. Poco más de la mitad de las IOUE ofrecen formación sobre ciberseguridad para el personal informático y para especialistas en seguridad informática. Pocas IOUE ofrecen formación obligatoria sobre ciberseguridad a los responsables de los sistemas informáticos que contienen información delicada. Los ejercicios de *phishing* son una herramienta importante para formar y concienciar al personal, pero no todas las IOUE los utilizan sistemáticamente.

V Aunque las IOUE han establecido estructuras de cooperación e intercambio de información sobre ciberseguridad, hemos observado que no se aprovechan plenamente las posibles sinergias. Las IOUE no comparten sistemáticamente entre sí

información sobre proyectos relacionados con la ciberseguridad, evaluaciones de seguridad y contratos de servicios. Además, las herramientas básicas de comunicación, como las soluciones de correo electrónico cifrado y videoconferencia, no son totalmente interoperables. Esto puede dar lugar a intercambios de información menos seguros, a una duplicación de los esfuerzos y a un aumento de los costes.

VI El Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE) y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) son las dos principales entidades encargadas de apoyar a las IOUE en materia de ciberseguridad. Sin embargo, debido a que los recursos son limitados o a que se ha dado prioridad a otras áreas, no han podido proporcionar a las IOUE todo el apoyo que necesitan, sobre todo en relación con el desarrollo de capacidades de aquellas que poseen menor experiencia. Aunque el CERT-UE es muy apreciado por las IOUE, su eficacia queda comprometida por la creciente carga de trabajo, la inestabilidad de la financiación y la dotación de personal, así como la insuficiente cooperación de algunas IOUE, que no siempre comparten información oportuna sobre vulnerabilidades e incidentes significativos de ciberseguridad que les hayan afectado o puedan afectar a otras.

VII Basándonos en estas conclusiones, recomendamos que:

- la Comisión mejore la preparación de las IOUE mediante una propuesta legislativa por la que se introduzcan normas comunes vinculantes sobre ciberseguridad para todas las IOUE y un incremento de los recursos del CERT-UE.
- la Comisión, en el contexto del Comité interinstitucional para la transformación digital, promueva nuevas sinergias entre las IOUE en determinados ámbitos;
- el CERT-UE y la ENISA se centren en las IOUE con menor madurez en ciberseguridad;

Introducción

¿Qué es la ciberseguridad?

01 El Reglamento sobre la Ciberseguridad de la UE[1] define la ciberseguridad como «todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas». La ciberseguridad depende de la seguridad de la información, que consiste en preservar la confidencialidad, la integridad y la disponibilidad de la información[2], ya sea en formato físico o electrónico. Además, la protección de las redes y sistemas de información en los que se almacena dicha información se denomina seguridad de tecnología de la información (véase la ***ilustración 1***).

Ilustración 1 – la ciberseguridad está ligada a la seguridad de la información y a la seguridad informática

Fuente: Tribunal de Cuentas Europeo.

02 Como disciplina, la ciberseguridad implica identificar, prevenir y detectar incidentes cibernéticos, responder a ellos y recuperarse de ellos. Los incidentes pueden abarcar, por ejemplo, desde revelación accidental de información hasta ataques dirigidos a comprometer infraestructuras críticas y robo de identidades y datos personales[3].

---

[1] Reglamento (UE) 2019/881.

[2] ISO/IEC 27000:2018.

[3] Tribunal de Cuentas Europeo Análisis 2/2019: Desafíos de una política eficaz de ciberseguridad en la UE (Documento informativo).

03 Un marco de ciberseguridad abarca muchos elementos, en particular requisitos y controles técnicos para la seguridad de las redes y sistemas de información, así como acuerdos de gobernanza apropiados y programas de concienciación en materia cibernética para el personal.

Ciberseguridad en las instituciones, órganos y organismos de la UE

04 Debido a la información delicada que tratan, las instituciones, órganos y organismos de la UE (IOUE) son objetivos atractivos para los posibles atacantes, en particular para los grupos capaces de ejecutar ataques sigilosos («amenazas persistentes avanzadas») muy sofisticados con fines de ciberespionaje y otros fines[4]. Los ciberataques contra las IOUE que llegan a consumarse pueden tener importantes consecuencias políticas, dañar la reputación general de la UE y socavar la confianza en sus instituciones.

05 La pandemia de COVID-19 ha obligado a las IOUE, así como a otras organizaciones de todo el mundo, a acelerar abruptamente la transformación digital y a adoptar el trabajo a distancia. Esto ha aumentado considerablemente el número de posibles puntos de acceso para los atacantes («superficie de ataque»), al ampliarse el perímetro de las organizaciones a hogares y dispositivos móviles conectados a Internet, donde pueden explotarse nuevas vulnerabilidades. Los servicios de acceso remoto son una de las rutas más comunes por las que los grupos que lanzan amenazas persistentes avanzadas a las IOUE obtienen acceso inicial a sus redes[5].

06 El número de ciberincidentes va en aumento y una tendencia especialmente preocupante es el espectacular aumento de incidentes significativos que afectan a las IOUE[6]; en el año 2021 se ha batido el récord en este sentido. Los incidentes significativos no son repetitivos ni básicos. Normalmente implican el uso de nuevos métodos y tecnologías y pueden requerir semanas o incluso meses de investigación y de recuperación. Los incidentes significativos se decuplicaron con creces entre 2018 y 2021[7]. Al menos veintidós IOUE han sufrido incidentes significativos solo en los dos

---

[4] CERT-UE, Informe «Panorama de amenazas» de ENISA, junio de 2021.

[5] *Ibidem*.

[6] *Ibidem*.

[7] *Ibidem*.

últimos años. Un ejemplo reciente fue el ciberataque a la Agencia Europea de Medicamentos, en el que se filtraron y manipularon datos delicados con el propósito de socavar la confianza en las vacunas[8].

07 Las IOUE son un grupo muy heterogéneo, formado por instituciones, organismos y diversos órganos. Las siete instituciones de la UE están establecidas por los Tratados, mientras que las agencias descentralizadas y otros organismos de la UE se crean mediante actos de Derecho derivado y son entidades jurídicas independientes. Existen distintas formas jurídicas de agencias: seis agencias ejecutivas de la Comisión y treinta y siete agencias descentralizadas de la UE[9]. Entre las IOUE también se cuentan oficinas de la UE, un cuerpo diplomático (el Servicio Europeo de Acción Exterior), empresas comunes y otros órganos. Cada IOUE es responsable de definir sus propios requisitos de ciberseguridad y aplicar sus propias medidas de seguridad.

08 Para reforzar la ciberseguridad de las IOUE, en 2012 la Comisión creó el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE) como grupo de trabajo permanente. El CERT-UE actúa como centro de intercambio de información sobre ciberseguridad y de coordinación de la respuesta a incidentes para las IOUE, y coopera con otros equipos de respuesta a incidentes de seguridad informática (CSIRT) de los Estados miembros y empresas de seguridad informática especializadas. El CERT-UE se organiza y opera con arreglo a un acuerdo interinstitucional[10] (ACI) de 2018 entre las IOUE a las que presta servicio, también conocidas como las «Partes». Actualmente cuenta con ochenta y siete Partes.

09 Otro agente clave que apoya a las IOUE es la Agencia de la Unión Europea para la Ciberseguridad (ENISA), dedicada a lograr un elevado nivel común de ciberseguridad en la Unión. La misión de la ENISA, creada en 2004, es mejorar la fiabilidad de los productos, procesos y servicios de las tecnologías de la información y las comunicaciones (TIC) mediante sistemas de certificación de la ciberseguridad, cooperar con las IOUE y los Estados miembros, y ayudarles a prepararse contra las ciberamenazas. La ENISA ayuda a las IOUE en el desarrollo de capacidades y en cooperación operativa.

---

[8] Ciberataque a la EMA – actualización 6, 25.1.2021.

[9] Informe Especial 22/2020 del Tribunal de Cuentas Europeo: Futuro de las agencias de la UE – Es posible reforzar la flexibilidad y la cooperación, apartado 01.

[10] DO C 12 de 13.1.2018, p. 1.

10 A pesar de su independencia institucional, las IOUE están estrechamente interconectadas. Intercambian información a diario y comparten una serie de sistemas y redes comunes. Los puntos débiles de una IOUE podrían exponer a otras a amenazas de seguridad, ya que muchos ciberataques pasan por varias fases hasta alcanzar su objetivo final[11]. Un ataque eficaz contra una IOUE más débil puede utilizarse como puerta de acceso para atacar a otras. Las OIUE también están interconectadas con organizaciones públicas y privadas en los Estados miembros, pero, en caso de no estar ciberpreparados, también pueden exponerlas a ciberamenazas.

11 Actualmente no existe un marco legal para la seguridad de la información y la ciberseguridad en las IOUE. No están sujetas a la legislación más amplia de la Unión en materia de ciberseguridad, la Directiva SRI 2016[12], ni a su propuesta de revisión, la Directiva SRI2[13]. Tampoco existe información completa sobre el importe invertido por las IOUE en ciberseguridad.

12 En julio de 2020, la Comisión publicó una Comunicación sobre la Estrategia de la UE para una Unión de la Seguridad[14] para el período 2020-2025. Sus acciones clave abarcan el establecimiento de «normas comunes en materia de seguridad de la información y ciberseguridad para todas las instituciones, órganos y organismos de la UE». Este nuevo marco contribuirá a lograr una cooperación operativa sólida y eficiente centrada en el papel del CERT-UE. En la Estrategia de Ciberseguridad de la UE para la Década Digital[15], publicada en diciembre de 2020, la Comisión se comprometió a proponer un reglamento relativo a las normas de ciberseguridad comunes para las instituciones, órganos y agencias de la UE. También propuso el establecimiento de un nuevo fundamento legal para que CERT-UE refuerce su mandato y su financiación.

---

[11] ENISA, Threat Landscape 2020, Sectoral/thematic threat analysis.

[12] 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.

[13] Propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión.

[14] COM(2020) 605 final.

[15] JOIN(2020) 18 final.

Alcance y enfoque de la auditoría

13 Dado que el número de ciberataques está aumentando considerablemente y que los puntos débiles de una IOUE pueden exponer a las demás a amenazas de seguridad, el objetivo de esta auditoría era determinar si las IOUE, en conjunto, han establecido mecanismos adecuados para protegerse contra las ciberamenazas. Para responder a esta pregunta principal de la auditoría, formulamos tres subpreguntas:

1) ¿Se han adoptado las prácticas de ciberseguridad principales en todas las IOUE?

2) ¿Existe una cooperación eficaz entre las IOUE en materia de ciberseguridad?

3) ¿Proporcionan la ENISA y el CERT-UE un apoyo adecuado a las IOUE en el ámbito de la ciberseguridad?

14 El calendario de la auditoría se ajusta a la Estrategia de la UE para una Unión de la Seguridad. Mediante la evaluación de las medidas de ciberseguridad actuales de las IOUE, pretendemos detectar qué ámbitos necesitan mejorar para que la Comisión los tenga en cuenta al elaborar su propuesta legislativa sobre normas comunes vinculantes en materia de ciberseguridad para todas las IOUE.

15 La auditoría abarcó los avances e iniciativas en el ámbito de la ciberseguridad desde enero de 2018 (cuando se estableció el acuerdo interinstitucional con el CERT-UE) hasta octubre de 2021.

16 Limitamos el alcance de nuestra auditoría a la ciberresiliencia y los sistemas no clasificados. Nos centramos en aspectos relativos a la preparación (actividades correspondientes a «identificar, proteger, detectar»). Las actividades correspondientes a «responder» y «recuperar» quedaban fuera de nuestro alcance. Sin embargo, examinamos algunos elementos organizativos de la respuesta ante incidentes. Además, quedan fuera del ámbito de nuestra auditoría la protección de datos, la aplicación de las leyes, la ciberdefensa y la ciberdiplomacia (véase la ***ilustración 2***).

Ilustración 2 – Alcance de la auditoría

** Solo examinamos algunos aspectos organizativos de la respuesta ante incidentes. Otros aspectos quedaban fuera del alcance de nuestro examen.*

Fuente: Tribunal de Cuentas Europeo.

17 Los resultados de auditoría se basan en un amplio análisis de la documentación disponible, complementado por entrevistas. Realizamos una encuesta de autoevaluación en la que participaron sesenta y cinco IOUE para recabar información sobre sus medidas de ciberseguridad y sus opiniones sobre la cooperación interinstitucional. Encuestamos a todas las IOUE sujetas a los derechos de auditoría del Tribunal de Cuentas Europeo y que gestionan su propia infraestructura informática, incluida nuestra propia institución. Entre ellas se encontraban instituciones, agencias descentralizadas, empresas comunes y órganos. También encuestamos a misiones civiles, que son entidades autónomas temporales financiadas por el presupuesto de la UE e independientes en cuanto a TI. En el ***anexo I*** figura una lista completa de las IOUE incluidas en la encuesta. El Defensor del Pueblo Europeo y el Supervisor Europeo de Protección de Datos no estaban incluidos en el ámbito de esta auditoría.

18 La encuesta obtuvo una tasa de respuesta del 100 % y sirvió como punto de partida para análisis posteriores. Además, seleccionamos una muestra de siete IOUE que es representativa de la heterogeneidad de las IOUE, y realizamos un seguimiento de sus respuestas mediante entrevistas y solicitudes de documentación. Los criterios de selección que consideramos comprendían la base jurídica, el tamaño (en términos de personal y presupuesto) y el sector. La muestra de IOUE se componía de la Comisión Europea, el Parlamento Europeo, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la Autoridad Bancaria Europea (ABE), la Agencia Europea de

Seguridad Marítima (AESM), la Misión asesora de la Unión Europea para la reforma del sector de la seguridad civil en Ucrania (EUAM Ucrania) y la Empresa Común para la ejecución de la iniciativa tecnológica conjunta sobre medicamentos innovadores (EC IMI).

19 También mantuvimos videoconferencias con el CERT-UE, el Comité consultivo sobre las TIC de la Red de Agencias de la UE (ICTAC), el Comité interinstitucional para la transformación digital (ICDT) y otras partes interesadas pertinentes.

Observaciones

El grado de madurez de las IOUE con respecto a la ciberseguridad es muy variable, y no siempre se ajusta a la buena práctica

20 En esta sección se examinan y los mecanismos y los marcos de ciberseguridad de cada IOUE. Evaluamos si abordan la ciberseguridad de forma coherente y adecuada, en términos de gobernanza de la seguridad informática, gestión de riesgos, asignación de recursos, formación de concienciación, controles y fiabilidad independiente.

La gobernanza de la seguridad informática en las IOUE no suele estar bien desarrollada y las evaluaciones de riesgo no son exhaustivas

En muchas IOUE existen lagunas en la gobernanza de la seguridad informática

21 La buena gobernanza desempeña un papel esencial en un marco eficaz para la seguridad de la información y de los sistemas informáticos, ya que define los objetivos de la organización y proporciona orientación mediante la priorización y la toma de decisiones. Según la Information Systems Audit and Control Association (ISACA)[16], un marco de gobernanza de la seguridad informática debe incluir, por lo general, varios elementos:

- una estrategia de seguridad global intrínsecamente vinculada a los objetivos de la empresa;
- políticas de seguridad reguladoras que aborden cada aspecto de la estrategia, los controles y la regulación;
- un conjunto completo de normas para cada política que describa las medidas operativas necesarias para cumplir con la misma;
- procedimientos de seguimiento institucionalizados para garantizar el cumplimiento y facilitar información sobre la eficacia;
- una estructura organizativa eficaz sin conflictos de intereses.

[16] ISACA, Certified Information System Auditor review manual, 2019.

22 Hemos detectado deficiencias en la gobernanza de la seguridad informática en muchas IOUE. Solo el 58 % de las IOUE (38 de 65) cuenta con una estrategia de seguridad informática o, como mínimo, un plan de seguridad informática aprobado por el consejo o por el equipo de alta dirección. Un desglose por tipo de IOUE revela que las misiones civiles y las agencias descentralizadas (en conjuntamente representan el 71 % de las IOUE incluidas en la encuesta) presentan los menores porcentajes (véase el ***cuadro 1***). La ausencia de una estrategia de seguridad informática o de un plan de seguridad de informática aprobados por la alta dirección implica el riesgo de que este no tenga conocimiento de los problemas de seguridad informática o no les otorgue suficiente prioridad.

Cuadro 1 – Porcentaje de las IOUE que cuentan con una estrategia o un plan de seguridad informática aprobados por el equipo de alta dirección

Desglose por número de empleados

< 100 empleados (22 IOUE)	100 a 249 empleados (17 IOUE)	250 a 1 000 empleados (16 IOUE)	>1 000 empleados (10 IOUE)
45 %	53 %	69 %	80 %

Desglose por tipo de IOUE

Agencias descentralizadas (35 IOUE)	Misiones civiles (11 IOUE)	Órganos (4 IOUE)	Instituciones (6 IOUE)	Empresas comunes (9 IOUE)
45 %	56 %	75 %	83 %	89 %

Fuente: Encuesta del Tribunal de Cuentas Europeo.

23 Examinamos las estrategias o planes de seguridad informática facilitadas por las siete IOUE de la muestra (véase el apartado ***18***), y consideramos que estaban razonablemente relacionadas con sus objetivos. Por ejemplo, la estrategia de seguridad informática de la Comisión abarca la dimensión de seguridad informática de la Estrategia digital de la Comisión Europea[17] y está diseñada para respaldar su hoja de ruta y sus objetivos. Sin embargo, solo tres IOUE de nuestra muestra habían incluido en sus estrategias/planes de seguridad informática objetivos concretos y un plazo para su consecución.

24 Las políticas de seguridad establecen normas y procedimientos que deben seguir los usuarios o gestores de recursos de información e informáticos. Ayudan a reducir los

[17] Communication to the Commission, European Commission digital Strategy: A digitally transformed, user-focused and data-driven Commission, C(2018) 7118 final, 21.11.2018.

riesgos de ciberseguridad e indican qué hacer en caso de incidentes. Constatamos que el 78 % de las IOUE cuentan con un modelo formal de política de seguridad de la información, mientras que solo el 60 % cuentan con un modelo formal de política de seguridad informática (véanse, en la ***ilustración 1***, las definiciones fpolítica de seguridad de la información y de política de seguridad informática). También descubrimos que cuatro de las siete IOUE incluidas en nuestra muestra tienen políticas de seguridad acordes con sus estrategias de seguridad informática. Sin embargo, en tres de estas cuatro, las políticas de seguridad informática solo se complementan parcialmente con normas de seguridad detalladas y actualizadas que describen las medidas operativas necesarias para aplicar las políticas. La falta de normas de seguridad formales aumenta el riesgo de que los problemas de seguridad informática no se aborden de manera adecuada y coherente en la misma IOUE. Además, dificulta la medición del cumplimiento por parte de la organización de su política de seguridad informática. De las siente IOUE de la muestra, solo la Comisión cuenta con procedimientos estructurados para supervisar el cumplimiento de sus políticas y normas de seguridad informática, pese a que solo los aplique un número reducido de direcciones generales (DG) (véase el ***recuadro 1***).

Recuadro 1

Cumplimiento de las normas de seguridad informática en la Comisión

Con arreglo a la gobernanza informática descentralizada de la Comisión, el máximo responsable de cada DG es el titular del servicio y el responsable de que sus sistemas cumplan las normas de seguridad informática. La DG Informática y la DG Recursos Humanos y Seguridad supervisan y facilitan la aplicación de prácticas de gestión del cumplimiento. La DG Informática ha establecido una herramienta (denominada «GRC») que permite a las DG medir su cumplimiento de los controles de las políticas de seguridad informática e informar al respecto.

Los 580 controles se dividen en tres grupos: controles generales (principalmente de gobernanza), controles específicos de la DG y controles específicos del sistema. La herramienta está operativa, pero hasta el momento solo la utilizan cinco DG. Por consiguiente, la DG Informática no tiene una visión general del cumplimiento en el conjunto de la Comisión. No obstante, el Consejo de Tecnologías de la Información y Ciberseguridad (ITCB) de la Comisión podrá solicitar a la DG Informática que investigue el cumplimiento de una norma específica (por ejemplo, la autenticación de doble factor en 2021) y podrá emitir dictámenes y recomendaciones no vinculantes o, en caso de que se detecten riesgos críticos, también requisitos formales.

25 Otro elemento importante en la buena gobernanza de la ciberseguridad es el nombramiento de un responsable central de seguridad informática. Aunque la familia

de normas ISO 27000 no lo exige explícitamente[18], contar con un responsable central de seguridad informática o una función equivalente se ha convertido en una práctica generalizada en todas las organizaciones y forma parte de las directrices de la ISACA. Normalmente, el responsable central de seguridad informática asume la responsabilidad general de los programas de seguridad de la información y seguridad informática de la organización. Para evitar conflictos de intereses, debe tener cierto grado de independencia de la función o departamento informático[19].

26 Según nuestra encuesta, el 60 % de las IOUE no han designado a un responsable central de seguridad informática independiente o una función equivalente. Aunque se nombren responsable central de seguridad informática (o equivalentes), la naturaleza de sus funciones difiere enormemente –y dichas funciones se entienden de manera diferente– entre las IOUE. Especialmente en las IOUE de tamaño pequeño y mediano, los responsables centrales de seguridad informática tienden a asociarse con más funciones operativas y no son funcionalmente independientes del departamento informático.
Esto puede limitar su autonomía para aplicar sus prioridades en relación con la seguridad. La ENISA trabaja actualmente en un marco de competencias de ciberseguridad de la UE que, entre otros, tiene el objetivo de lograr una interpretación común de las funciones, las competencias y las capacidades.

CIFRAS CLAVE: **Gobernanza de la seguridad informática en las IOUE**

El **58 %** de las IOUE tienen una estrategia o un plan de seguridad informática **aprobado por el equipo de alta dirección**

El **78 %** tienen una **política de seguridad de la información formal**

El **60 %** tienen políticas y normas de **seguridad informática** formales

El **40 %** han designado a un **responsable central de seguridad informática independiente**

[18] Norma ISO/IEC 27000:2018, capítulo 5.

[19] COBIT 5 para la seguridad de la información, apartado 4.2.

Las evaluaciones de riesgos de seguridad informática de las IOUE no abarcan todo su entorno informático

27 Todas las normas internacionales relativas a la seguridad informática subrayan la importancia de establecer un método adecuado para evaluar y gestionar los riesgos de seguridad que afectan a los sistemas informáticos y a los datos que contienen. Deben realizarse evaluaciones de riesgos periódicamente para responder a los cambios en los requisitos de seguridad de la información de una organización y los riesgos a los que esta se enfrenta[20]. Las evaluaciones deben ir seguidas de un plan de reducción de riesgos (o de un plan de seguridad informática).

28 La mayoría de las IOUE encuestadas (58 de 65) indicaron que siguen un marco o una metodología para realizar evaluaciones de riesgos en sus sistemas informáticos. Sin embargo, no existe una metodología común para todas las IOUE. Al menos veintiséis de ellas utilizan total o parcialmente las metodologías desarrolladas por la Comisión, en particular el 31 % utilizaron la metodología de gestión de riesgos de seguridad informática de 2018 (ITSRM2). Las demás siguen metodologías basadas en normas bien conocidas del sector [como ISO 27001, ISO 27005, el marco de ciberseguridad del National Institute of Standards and Technology (NIST-CSF) o controles del Center for Internet Security (CIS)] o utilizan otras metodologías internas.

29 De las siete IOUE incluidas en la muestra, solo dos realizan evaluaciones de riesgos exhaustivas que abarcan todo su entorno informático (es decir, todos sus sistemas informáticos). La mayoría solo realiza evaluaciones de riesgos individuales de sus sistemas informáticos más importantes. Hemos detectado algunos ejemplos de evaluaciones de riesgos realizadas antes de desplegar sistemas nuevos. Sin embargo, no encontramos pruebas de evaluaciones de riesgos de seguimiento vinculadas, por ejemplo, a cambios posteriores en sus sistemas/infraestructuras.

Las IOUE no abordan la ciberseguridad de manera uniforme y no siempre cuentan con controles esenciales

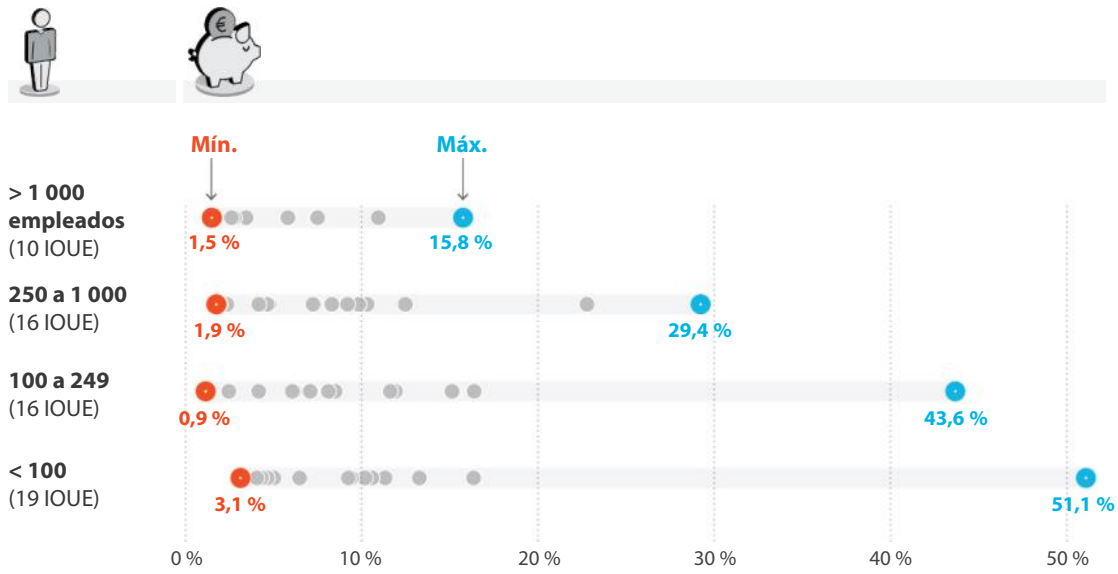
La asignación de recursos a la ciberseguridad varía mucho entre las IOUE

30 En nuestra encuesta, pedimos a las IOUE que indicaran su gasto total en TI en 2020 y una estimación del importe gastado en ciberseguridad. Nuestros datos muestran variaciones significativas en el porcentaje de gasto en TI que las IOUE destinan a ciberseguridad. Esto ocurre incluso en las IOUE de tamaño similar, con

[20] Véase, por ejemplo, ISO/IEC 27000:2018, apartado 4.5.

respecto al número de efectivos. Como se muestra en la ***ilustración 3***, las diferencias suelen ser especialmente notables en las IOUE que cuentan con menos personal.

Ilustración 3 – Gasto en ciberseguridad como porcentaje del gasto total en tecnologías de la información (IOUE agrupadas por número de efectivos)



Notas: Cuatro IOUE no han facilitado cifras sobre gasto en ciberseguridad.

Fuente: Encuesta del Tribunal de Cuentas Europeo.

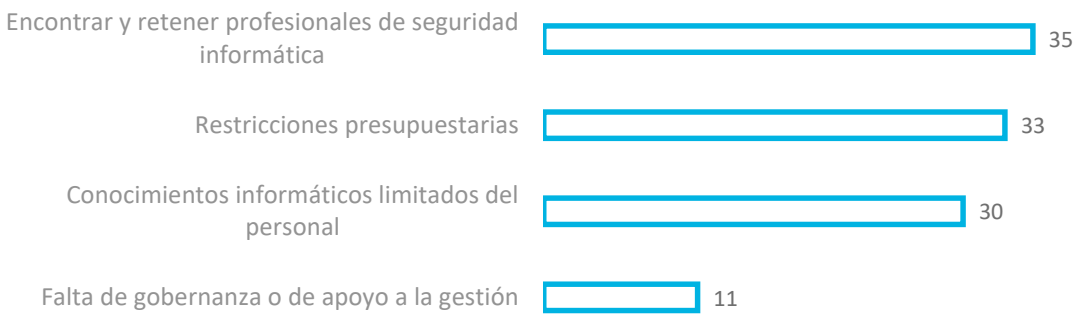
31 Es difícil evaluar en términos absolutos el nivel óptimo de gasto en ciberseguridad. Depende de muchos factores, como la superficie de ataque de la organización, la sensibilidad de los datos que maneja, su perfil y apetito de riesgo y los requisitos legales/reglamentarios sectoriales. Sin embargo, nuestros datos destacan que las diferencias son sustanciales y las razones para ello no siempre son obvias. El gasto en ciberseguridad de algunas IOUE es considerablemente menor que el de sus homólogas de tamaño similar, lo cual es indicio de gasto insuficiente cuando estén expuestas a amenazas y riesgos similares.

32 La mayoría de las IOUE son pequeñas o medianas en términos de personal y gasto en tecnologías de la información, y dos tercios de ellas tienen menos de 350 empleados. La IOUE más pequeña tiene solo quince empleados. Gestionar la ciberseguridad es más difícil y requiere más recursos para las IOUE más pequeñas. En la mayoría de los casos, no pueden beneficiarse de economías de escala y carecen de suficiente experiencia interna. Según nuestra encuesta y de las entrevistas, las instituciones más importantes, como la Comisión y el Parlamento Europeo, cuentan con equipos de expertos que gestionan la ciberseguridad a tiempo completo. Sin embargo, en las IOUE más pequeñas, donde el personal y los recursos son

especialmente limitados, no hay expertos en absoluto, y la ciberseguridad la gestiona a tiempo parcial personal con formación en TI. Dado que las IOUE están estrechamente interconectadas, esto contribuye a aumentar el riesgo (véase asimismo el apartado ***10***).

33 En nuestra encuesta, preguntamos a las IOUE cuáles eran los principales desafíos de la aplicación de políticas eficaces de ciberseguridad en sus organizaciones (véase la ***ilustración 4***). El mayor reto es que los expertos en ciberseguridad son un recurso escaso y que muchas IOUE tienen dificultades para atraerlos, debido a la competencia tanto del sector privado como de otras IOUE. Entre los problemas recurrentes figuran los largos procedimientos de contratación, las condiciones contractuales poco competitivas y la falta de perspectivas profesionales atractivas. La escasez de personal especializado supone un riesgo importante para la gestión eficaz de la ciberseguridad.

Ilustración 4 – Desafíos para la aplicación de políticas de ciberseguridad eficaces en IOUE (podía seleccionarse más de un factor)



Fuente: Encuesta del Tribunal de Cuentas Europeo.

La mayoría de las IOUE ofrecen algún tipo de formación sobre concienciación en materia cibernética, pero no es sistemática ni están bien orientada

34 Los posibles atacantes no solo causan daños aprovechando las vulnerabilidades de los sistemas y dispositivos; también pueden inducir a los usuarios a revelar información delicada o a descargar software malicioso, por ejemplo mediante *phishing* o ingeniería social. El personal forma parte de la primera línea de defensa de todas las organizaciones. Por lo tanto, los programas de formación y concienciación en materia cibernética son un elemento clave en un marco de ciberseguridad eficaz.

35 La gran mayoría de las IOUE encuestadas (95 %) ofrecen algún tipo de formación de concienciación sobre el ciberespacio a todo el personal, pero tres de ellas no lo hacen. Sin embargo, solo el 41 % de las IOUE organizan sesiones específicas de

formación o concienciación para directivos y solo el 29 % imparten formación obligatoria sobre ciberseguridad a responsables de sistemas informáticos que contienen información delicada. La concienciación y el compromiso de la dirección son cruciales para una gobernanza eficaz de la ciberseguridad. De las once IOUE que aludieron a la falta de apoyo a la gestión como dificultad para lograr una ciberseguridad eficaz, solo tres ofrecían formación para concienciar a su dirección. El 58 % y el 51 % de las IOUE, respectivamente, ofrecen formación continua sobre ciberseguridad destinada al personal informático y a los especialistas en seguridad informática.

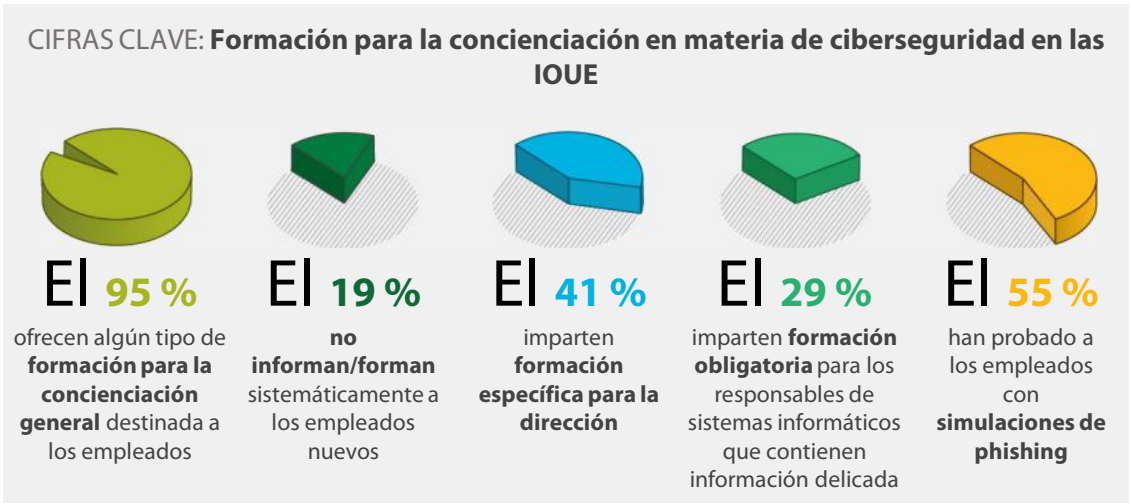
36 No todas las IOUE disponen de mecanismos para supervisar la asistencia del personal a la formación sobre ciberseguridad y el cambio ulterior operado en su conducta y su concienciación. Especialmente en las organizaciones más pequeñas pueden impartirse sesiones de concienciación sobre el ciberespacio en el contexto de reuniones informales de personal. Las organizaciones miden la concienciación del personal principalmente mediante pruebas periódicas sobre sus comportamientos, como encuestas de madurez o ejercicios de *phishing*. En los últimos cinco años, el 55 % de las IOUE ha organizado una o varias campañas simuladas de *phishing* (o ejercicios similares). Dado que el *phishing* es una de las principales amenazas a las que se enfrenta el personal de las administraciones públicas[21], estos ejercicios son una herramienta importante para su formación y concienciación. Constatamos que las acciones de la Comisión de concienciación en materia cibernética constituían una buena práctica y estaban a disposición de todas las IOUE interesadas (véase el ***recuadro 2***).

[21] ENISA, Thread Landscape 2020, Sectoral/Thematic threat analysis.

Recuadro 2

Formación sobre concienciación en materia cibernética en la Comisión

La Comisión cuenta con un equipo específico «Cyber Aware» en la DG Informática que dirige el programa corporativo de concienciación en materia cibernética. El programa se gestiona conjuntamente con la DG Recursos Humanos y Seguridad, la Secretaría General, la DG Redes de Comunicación, Contenido y Tecnologías y el CERT-UE. La formación es de alta calidad y en muchos casos tiene un alcance interinstitucional. Las sesiones de formación se anuncian a través del Learning Bulletin, que llega a unos 65 000 empleados de la UE. A través de la plataforma «Cyber Aware», la Comisión ha organizado quince ejercicios de *phishing* en los últimos cinco años y ha realizado recientemente el primer ejercicio en toda la Comisión.



Los controles esenciales no siempre se aplican o no se formalizan en normas

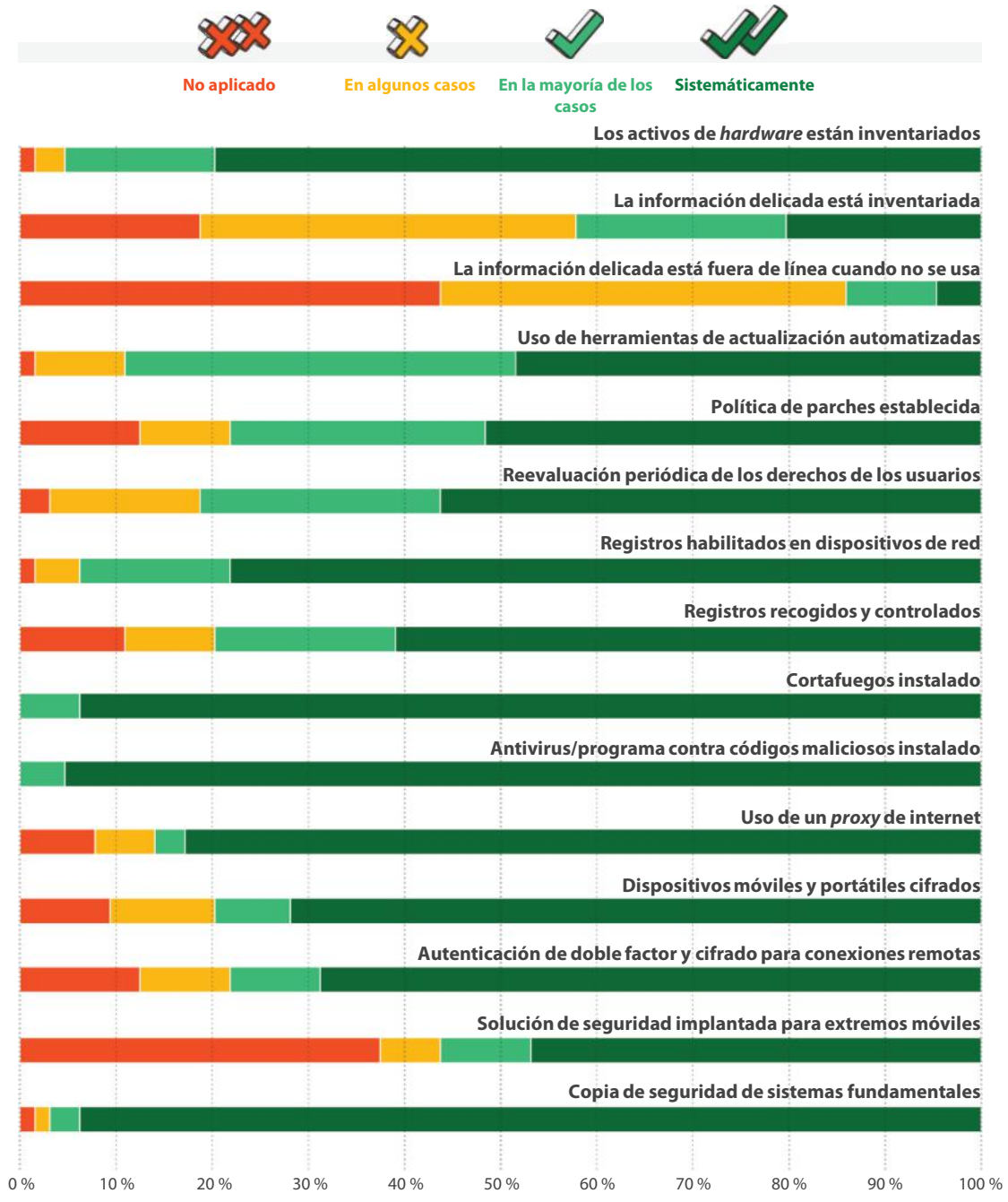
37 Pedimos a las IOUE que autoevaluaran su aplicación de una selección de controles esenciales[22]. Seleccionamos un conjunto de buenas prácticas que incluso las organizaciones más pequeñas podrían aplicar razonablemente[23]. Los resultados se presentan en el ***cuadro 5***. La mayoría de las IOUE encuestadas han adoptado los

[22] Conjunto de controles derivados de los controles 7.1 del CIS, un marco de buenas prácticas comisariado por el Centre for Internet Security.

[23] Grupo de aplicación 1 (IG1) de los controles del CIS.

controles esenciales seleccionados. Sin embargo, en algunas áreas, los controles parecen ser deficientes o limitados en al menos el 20 % de las IOUE.

Ilustración 5 – Aplicación de controles esenciales en IOUE (resultados de la autoevaluación)



Fuente: Encuesta del Tribunal de Cuentas Europeo.

38 Solicitamos a las siete IOUE incluidas en la muestra los justificantes y las correspondientes normas/políticas para cada control que declararon aplicado. Obtuvimos estos documentos en el 62 % de los controles. Como se aclaró en las entrevistas, en varios casos existían controles técnicos, pero no se habían formalizado

(hasta la fecha) en normas o políticas, lo cual incrementa el riesgo de que los problemas de seguridad informática no se solucionen de manera uniforme en la misma IOUE (véase asimismo el apartado ***24***).

Varias IOUE carecen de medidas de ciberseguridad sujetas a garantías independientes regulares

39 Según la ISACA[24], la auditoría interna es una de las tres líneas de defensa esenciales de una organización, y las otras dos son la gestión y gestión de riesgos. Las auditorías internas contribuyen a mejorar la gestión de la seguridad de la información y la seguridad informática. Examinamos la frecuencia con que las IOUE obtienen garantías independientes sobre su marco de seguridad informática, mediante auditorías internas o externas y pruebas proactivas de sus ciberdefensas.

40 El Servicio de Auditoría Interna (SAI) de la Comisión es responsable, entre otras cosas, de realizar auditorías informáticas de la Comisión y de las agencias descentralizadas, las empresas comunes y el SEAE. El mandato del servicio abarca a cuarenta y seis (el 70 %) de las sesenta y cinco IOUE encuestadas, y el SAI ha realizado auditorías relacionadas con la seguridad informática en seis IOUE diferentes en los últimos cinco años. Además, la DG Recursos Humanos y Seguridad es competente para llevar a cabo inspecciones de seguridad informática que abarquen aspectos técnicos de seguridad de la información[25]. De las restantes IOUE, siete declararon tener su propia función de auditoría interna que abarcaba aspectos informáticos, pero, en doce de ellas, las respuestas a nuestra encuesta no fueron suficientes para determinar si tenían esa capacidad de auditoría interna.

41 Las auditorías de seguridad informática externas realizadas por entidades independientes son otra forma de obtener garantías independientes. A pesar de la rápida evolución del panorama cibernético, entre principios de 2015 y el primer trimestre de 2021, el 34 % de las IOUE no había sido objeto de ninguna auditoría de seguridad informática interna o externa. Un desglose de esta última cifra por tipo de IOUE revela que el 75 % de los órganos de la UE, el 66 % de las empresas conjuntas y el 45 % de las misiones civiles no han sido objeto de una auditoría de seguridad informática interna o externa desde 2015.

---

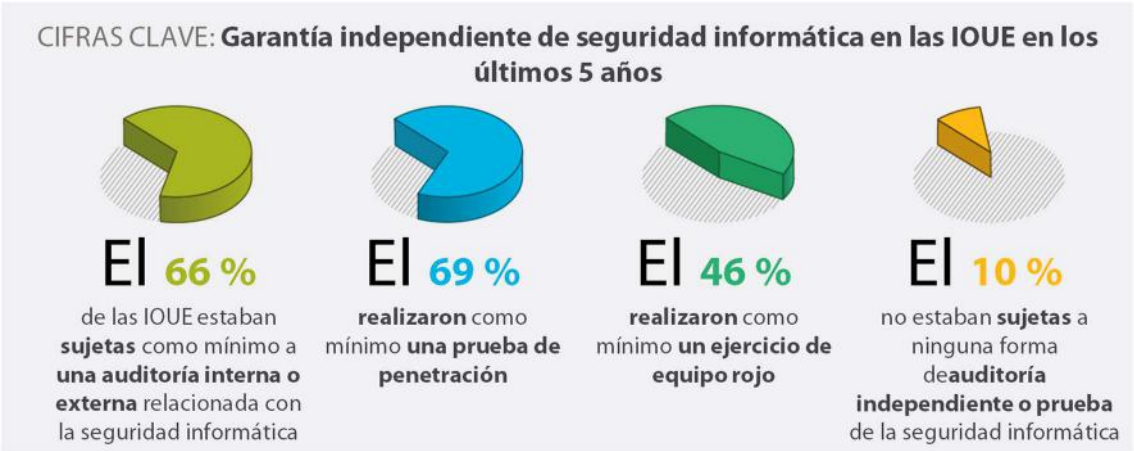
[24] ISACA, Auditing Cyber Security: Evaluating Risk and Auditing Controls, 2017.

[25] Decisión 46/2017 sobre la seguridad de los sistemas de información y comunicaciones en la Comisión Europea.

42 Además de las auditorías internas y externas, otra forma de que las organizaciones obtengan garantías sobre su marco de seguridad informática es probando proactivamente sus ciberdefensas para detectar vulnerabilidades. Las pruebas de penetración (también conocidas como *hacking* ético), que consisten en ciberataques simulados autorizados a sistemas informáticos individuales, son un método para hacerlo. En respuesta a nuestra encuesta, el 69 % de las IOUE declararon haber realizado al menos una prueba de penetración en los últimos cinco años. En el 45 % de los casos, el CERT-UE fue la entidad que realizó estas pruebas.

43 Los ejercicios de «equipo rojo» son otra forma de poner a prueba las ciberdefensas mediante ataques simulados, utilizado técnicas usadas recientemente en ataques reales. Estos ejercicios son más complejos y completos que las pruebas de penetración, ya que implican varios sistemas y posibles vías de ataque. Las IOUE los realizan con menos frecuencia: El 46 % de las IOUE refirieron al menos un ejercicio de equipo rojo en los últimos cinco años. El CERT-UE realizó el 75 % de estos ejercicios. Los ejercicios de equipo rojo requieren una cantidad considerable de trabajo para su preparación y realización, y el CERT-UE no tiene actualmente capacidad para realizar más de cinco a seis ejercicios al año.

44 A excepción de dos IOUE de reciente creación, dieciséis (25 %) de las IOUE encuestadas no se habían sometido a pruebas de penetración ni ejercicios en equipo rojo en los últimos cinco años. En total, siete IOUE (10 %) no han sido objeto de ningún tipo de garantía independiente sobre sus medidas de seguridad informática: una empresa común, una agencia descentralizada y cinco misiones civiles.



Las IOUE han establecido mecanismos de cooperación, pero presentan deficiencias

45 En esta sección se examinan los agentes y los comités creados para promover la cooperación entre las IOUE en el ámbito de la ciberseguridad, así como los acuerdos interinstitucionales de gobernanza y coordinación. Más concretamente, examinamos dos agentes interinstitucionales, la ENISA y el CERT-UE, y dos comités interinstitucionales, el Comité interinstitucional para la transformación digital (ICDT), en particular su subgrupo de ciberseguridad (CSSG), y el Comité consultivo sobre las tecnologías de la información y de las comunicaciones (ICTAC). También evaluamos el grado en que estos han generado sinergias para mejorar la preparación de las IOUE.

Existe una estructura formal para que las IOUE coordinen sus actividades, aunque presentan algunos problemas de gobernanza

46 El ICDT y el ICTAC son los dos comités principales que promueven la cooperación en materia de TI entre las IOUE. El ICDT, integrado por los responsables de los departamentos informáticos de las instituciones y órganos de la UE, es un foro para fomentar el intercambio de información y la cooperación. Cuenta con un subgrupo de ciberseguridad (ICDT CSSG) que depende de ICDT y puede recomendar tomar decisiones sobre cuestiones específicas. Por otra parte, el ICTAC es un subgrupo de la Red de Agencias de la UE (EUAN), red informal creada por los directores de las agencias de la UE que se centra en la cooperación entre agencias y empresas comunes. Tanto el ICDT como el ICTAC tienen funciones claramente definidas y complementarias: El ICTAC abarca las agencias descentralizadas y las empresas comunes, mientras que el ICDT abarca las instituciones y los órganos. Por naturaleza, el ICDT y el ICTAC son grupos consultivos informales y foros para el intercambio de información y buenas prácticas. En el ***anexo II*** puede encontrarse más información sobre estos comités interinstitucionales.

La representación de las IOUE en foros pertinentes no siempre es suficiente

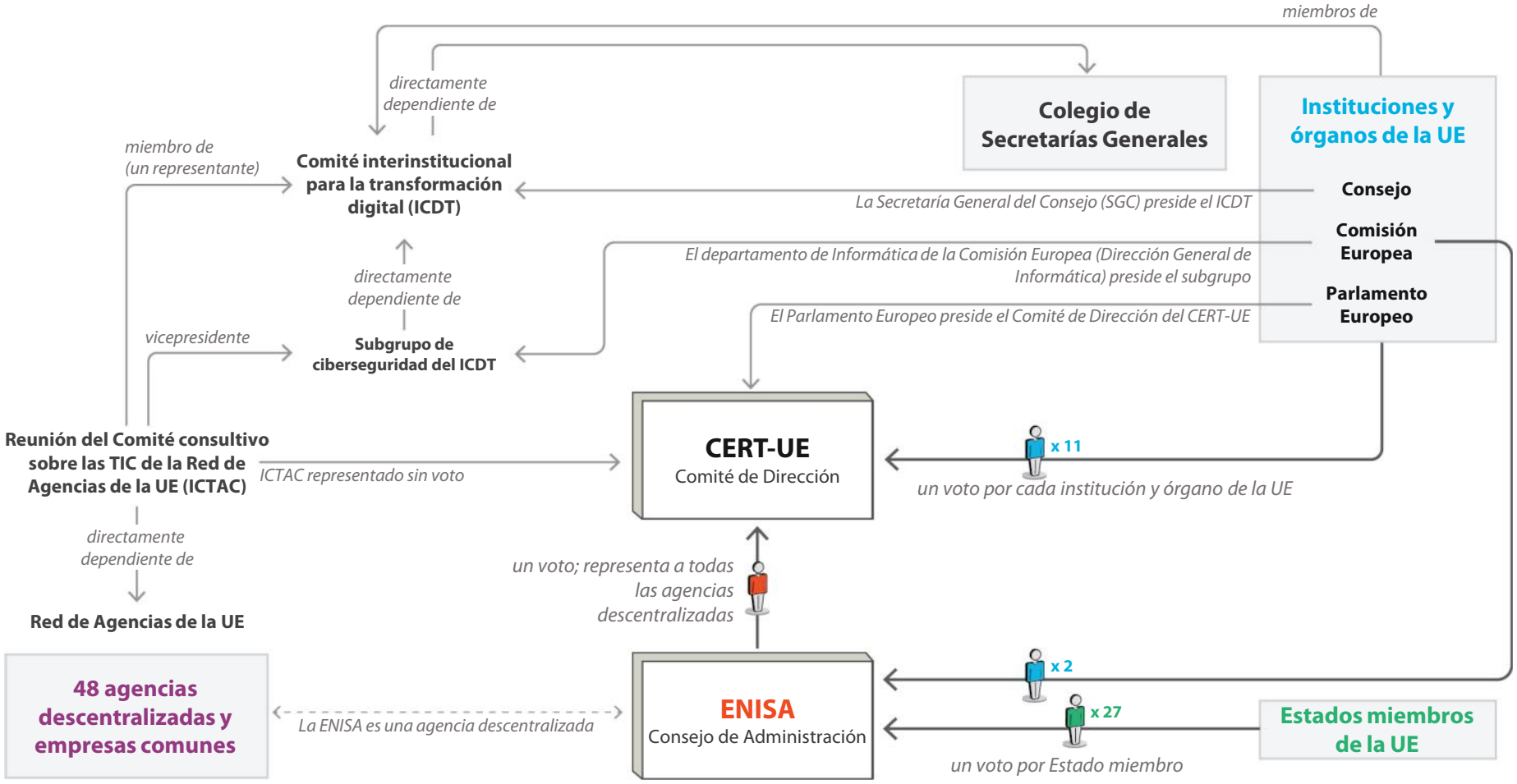
47 Aunque las estructuras de representación son claras, no todas las IOUE consideran suficiente su representación real. Cuando en nuestra encuesta se pedía una opinión sobre la afirmación «Mis necesidades se tienen suficientemente en cuenta en los foros interinstitucionales pertinentes y mi IOUE tiene una representación adecuada en los consejos de toma de decisiones», el 42 % de las IOUE se mostraron en desacuerdo. Algunas de las más pequeñas consideraban que no disponían de recursos suficientes para participar activamente en los foros interinstitucionales.

48 El Comité de Dirección del CERT-UE, su principal órgano decisorio, tampoco es representativa del conjunto de las Partes. El CERT-UE presta servicios a ochenta y siete IOUE y a tres organizaciones distintas de las IOUE. Sin embargo, su Comité de Dirección solo se compone de representantes de los once signatarios del acuerdo interinstitucional (las siete instituciones de la UE más el SEAE, el Comité Económico y Social, el Comité de las Regiones y el Banco Europeo de Inversiones) y de un representante de la ENISA, cada uno de los cuales tiene un voto[26].

49 Más de la mitad de las Partes del CERT-UE son agencias descentralizadas de la UE y empresas conjuntas, que en conjunto cuentan con alrededor de 12 000 empleados. Formalmente, la ENISA representa sus intereses en el Comité de Dirección del CERT-UE. Sin embargo, el mandato de la ENISA de representar a las agencias y empresas comunes de la UE es débil, ya que no fue nombrada ni elegida directamente por ellas. En la práctica, las opiniones de las agencias descentralizadas y las empresas comunes son expresadas en las reuniones del Comité de Dirección por un representante del ICTAC, al que se permite asistir para ayudar a la ENISA en su función de representación de las agencias. A pesar de expresar las opiniones y los intereses de cuarenta y ocho IOUE, el representante del ICTAC no tiene actualmente un puesto formal ni voto en el Comité de Dirección. En abril de 2021, el ICTAC envió al presidente del Comité de Dirección del CERT-UE una solicitud formal de derechos de voto en el Comité. En el momento de redactar este informe, esta solicitud aún no había sido concedida. Véase, en la ***ilustración 6***, una síntesis de la representación de las IOUE en los consejos y comités decisorios.

[26] Cláusula 7 del Acuerdo interinstitucional (ACI) firmado el 20.12.2017.

Ilustración 6 – Gobernanza y representación de la ciberseguridad en los consejos y comités decisorios



Fuente: Tribunal de Cuentas Europeo.

50 La gobernanza interinstitucional en materia de ciberseguridad de las EUIBA está fragmentada y actualmente no existe una entidad concreta que tenga una visión global de la madurez en ciberseguridad de las IOUE, ni autoridad para asumir el liderazgo o para hacer cumplir unas normas comunes vinculantes. Tanto la ENISA como el CERT-UE solo pueden «apoyar» y «ayudar» a las IOUE. Los comités pertinentes no tienen poder de decisión y solo pueden formular recomendaciones a las IOUE. Además, la quinta parte de las IOUE encuestadas tampoco tiene claro dónde deben dirigirse para obtener un servicio, una herramienta o una solución específicos.

Existen memorandos de entendimiento entre los agentes principales, pero hasta la fecha no han producido resultados concretos

51 En mayo de 2018 se firmó un memorando de entendimiento entre la ENISA, el CERT-UE, el Centro Europeo de Ciberdelincuencia de Europol y la Agencia Europea de Defensa (AED). Se centraba en cinco ámbitos de cooperación: intercambio de información, educación y formación, ejercicios de ciberseguridad, cooperación técnica, y asuntos estratégicos y administrativos. Aunque este memorando de entendimiento podría ayudar a evitar duplicaciones gracias a un programa de trabajo común, no tenemos pruebas de que haya dado lugar a resultados concretos y a acciones conjuntas.

52 El Reglamento sobre la Ciberseguridad, que entró en vigor en junio de 2019, preveía la firma de un nuevo acuerdo de cooperación específico entre el CERT-UE y la ENISA. Cabe destacar que finalmente pasaron más de un año y medio hasta que se firmó el memorando de entendimiento, en febrero de 2021; este intenta establecer una cooperación estructurada entre el CERT-UE y la ENISA. Define sus ámbitos de cooperación (desarrollo de capacidades, cooperación operativa, y conocimientos e información) y establece una división aproximada de funciones entre ellos: El CERT-UE dirigirá la asistencia a las IOUE, y la ENISA contribuirá a esta tarea. En el memorando de entendimiento no se definen las disposiciones prácticas, que se especifican en un plan de cooperación anual. El primer plan anual de cooperación para 2021 fue adoptado por el Consejo de Administración de la ENISA en julio de 2021 y por el Comité de Dirección del CERT-UE en septiembre de 2021. Por lo tanto, es demasiado pronto para que nuestra auditoría evalúe si este plan ha producido algún resultado tangible.

53 Dado que los memorandos de entendimiento citados en los apartados ***51*** y ***52*** tienen objetivos y ámbitos de cooperación comunes, como formación, ejercicios o intercambio de información, existe un riesgo de solapamientos y de redundancias.

Todavía no se han aprovechado plenamente las potenciales sinergias a través de la cooperación

Se han realizado avances positivos para lograr sinergias

54 En los programas de trabajo de los comités ICTAC e ICDT CSSG se señalan ámbitos importantes en los que pueden lograrse mejoras de la eficiencia a través de la colaboración. Entre los ejemplos prácticos de iniciativas que han permitido a las IOUE aprovechar sinergias figuran:

- contratos marco interinstitucionales;
- un centro común de recuperación en caso de catástrofe organizado desde 2019 por la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) para las agencias descentralizadas, que permite un ahorro de costes de al menos el 20 % respecto a los precios de mercado (nueve agencias han adoptado esta solución de recuperación en caso de catástrofe);
- acuerdos entre seis empresas comunes ubicadas en el mismo edificio para compartir infraestructuras comunes y un marco común de seguridad informática (desde 2014).

55 Otro ejemplo importante es el «GovSec», un sistema que ayuda a las IOUE a realizar evaluaciones de riesgos para adoptar soluciones en la nube. Según nuestra encuesta, el 75 % de las IOUE ya utilizan algunas plataformas de nube pública, y las demás ya tienen previsto migrar a la nube. Desde 2019, la Comisión ha adoptado un enfoque «primero en la nube», que prevé una oferta segura de servicios híbridos multinube[27]. La Comisión también actúa como intermediario en la nube para todas las IOUE, en el contexto del contrato marco «Cloud II». La gestión de los riesgos para la seguridad y la protección de datos en las plataformas de nube requiere nuevas capacidades y un enfoque diferente frente a la infraestructura informática tradicional *in situ*. La gestión eficaz de los riesgos para la seguridad de la información en la nube es un reto común para las IOUE, y GovSec, un ejemplo de solución que puede responder a las necesidades de varias de ellas, si no de todas.

La colaboración y el intercambio de prácticas entre IOUE siguen siendo óptimos

56 La existencia de comités interinstitucionales no genera sinergias de forma automática, y las IOUE no siempre comparten buenas prácticas, conocimientos especializados, metodologías y balance de experiencias. Además, corresponde a cada

[27] Comisión Europea, The European Commission Cloud Strategy, 2019.

IOUE decidir su grado de implicación en el trabajo del ICDT CSSG. Si bien los miembros del ICDT CSSG asisten a las reuniones, solo pueden contribuir en la medida en que sus obligaciones habituales en las IOUE lo permiten, lo que ya ha ralentizado los avances en la ejecución de las acciones acordadas por algunos grupos de trabajo.

57 Encontramos áreas específicas en las que no existen mecanismos para que las IOUE compartan experiencia e iniciativas. Por ejemplo, en el marco del contrato marco sobre capacidad de defensa de red, las IOUE pueden solicitar un estudio para consolidar los requisitos de ciberseguridad y buscar soluciones. Sin embargo, no existe un archivo de los estudios realizados o solicitados por otras IOUE, por lo que estas pueden solicitar el mismo estudio varias veces. Además, las IOUE no se informan sistemáticamente de que mantienen relaciones contractuales con proveedores específicos ni de que utilizan una solución de software específica. Esta falta de conocimientos puede dar lugar a costes adicionales y a la pérdida de sinergias.

58 Las IOUE tampoco comparten sistemáticamente información sobre los proyectos de ciberseguridad que llevan a cabo, aunque puedan tener repercusiones interinstitucionales. El mandato del ICDT CSSG contiene una disposición para que las IOUE compartan información sobre nuevos proyectos que puedan afectar a la ciberseguridad de otras IOUE o a la protección de la información procedente de ellas. Sin embargo, el ICDT CSSG no está informado de tales proyectos.

59 Cuando se crea una agencia nueva, esta tiene que construir su infraestructura informática y su marco de seguridad informática desde cero. No existe un «catálogo de servicios», una caja de herramientas o directrices/requisitos claros para las agencias nuevas. Consecuencia de ello es una gran heterogeneidad en los entornos informáticos de las IOUE, donde cada organización es libre de adquirir su propio *software*, *hardware*, infraestructura y servicios de forma independiente. Lo mismo ocurre con el marco de seguridad informática, en ausencia de normas y requisitos comunes. Esta situación da lugar a una potencial duplicación de esfuerzos y a un uso ineficiente del dinero de la UE, pero también a una mayor complejidad para el CERT-UE en cuanto al apoyo que debe prestar.

Existen deficiencias prácticas en el intercambio de información delicada

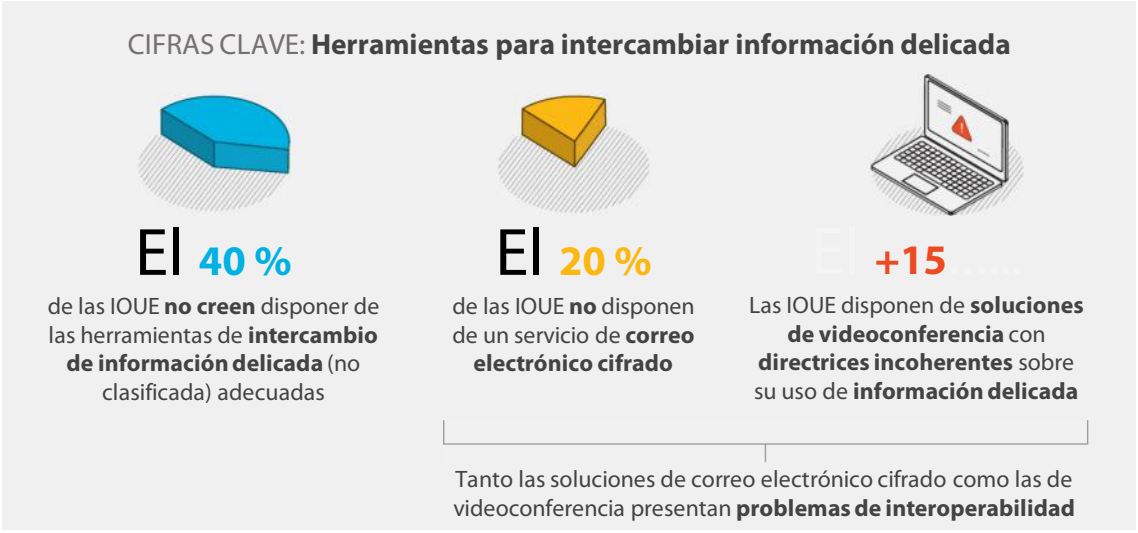
60 Algunas IOUE siguen sin disponer de soluciones adecuadas para intercambiar información delicada no clasificada. Las que sí las tienen, han adoptado en general sus propios productos y sistemas, por lo que la interoperabilidad es un problema. Solo existen plataformas seguras comunes para fines específicos, como las que ofrece el

CERT-UE a todas las Partes para intercambiar información delicada sobre incidentes, amenazas y vulnerabilidades.

61 Por ejemplo, más del 20 % de las IOUE no disponen de un servicio de correo electrónico cifrado. Aquellas que a menudo se enfrentan a problemas de interoperabilidad y certificados no se reconocen mutuamente. El ICTAC y el ICDT llevan años debatiendo opciones para una solución escalable e interoperable, y en 2018 hubo un proyecto piloto. Sin embargo, esta cuestión sigue sin resolverse.

62 Otro problema es la ausencia de marcas comunes para la información delicada no clasificada. Las marcas son categorizaciones que indican a los titulares de información los requisitos de protección específicos de esa información. Difieren entre las IOUE, lo que complica el intercambio y el correcto manejo de la información.

63 En 2020, la pandemia de COVID-19 obligó a las IOUE a adoptar herramientas de comunicación y videoconferencia a gran escala para garantizar la continuidad de las actividades. Hallamos al menos quince soluciones de software de videoconferencia diferentes en uso entre las IOUE. Incluso cuando diferentes IOUE utilizan la misma solución/plataforma, carecen de interoperabilidad. Además, las directrices sobre qué información (en términos de confidencialidad) podría compartirse o debatirse en una plataforma determinada difieren entre las IOUE. Estas cuestiones generan ineficiencias económicas y operativas y pueden crear problemas de seguridad potenciales.



La ENISA y el CERT-UE todavía no han proporcionado a las IOUE todo el apoyo que necesitaban

64 En esta sección examinamos las dos principales entidades encargadas de apoyar a las IOUE en materia de ciberseguridad: la ENISA y el CERT-UE. Evaluamos si el apoyo prestado por ambas entidades ha llegado a las IOUE y responde a sus necesidades, destacando las razones que subyacen a las deficiencias detectadas.

La ENISA es un actor clave en la ciberseguridad de la UE, pero su apoyo solo ha llegado a muy pocas IOUE

65 En junio de 2019, entró en vigor el Reglamento sobre la Ciberseguridad[28], que sustituyó a la anterior base jurídica de la ENISA[29] y otorgó a la Agencia un mandato más sólido. Más concretamente, establece que la ENISA debe apoyar activamente a los Estados miembros y a las IOUE para mejorar la ciberseguridad por medio del desarrollo de la capacidad, la cooperación operativa y el establecimiento de sinergias. En el ámbito del desarrollo de la capacidad, la ENISA tiene ahora el mandato de ayudar a las IOUE «en sus esfuerzos para mejorar la prevención, detección, análisis de ciberamenazas e incidentes (…), en particular a través de un apoyo adecuado al CERT»[30]. La ENISA también debe ayudar a las instituciones de la UE a desarrollar y revisar las estrategias de ciberseguridad de la UE mediante la promoción de su difusión y el seguimiento de los avances en su aplicación.

66 Aunque en el Reglamento sobre la Ciberseguridad se establece claramente que la ENISA deberá apoyar a las IOUE en la mejora de su ciberseguridad, dicha agencia no ha llevado a término ningún plan de acción relativo a su objetivo de contribuir al desarrollo de capacidades de las IOUE (para mayor información, véase el ***recuadro 3***).

---

[28] Las tareas de la ENISA se recogen en el capítulo II (artículos 5 a 12) del Reglamento (UE) 2019/881.

[29] Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo; para conocer las tareas de la ENISA en virtud de este Reglamento, véase el artículo 3.

[30] Artículo 6 del Reglamento (EU) 2019/881.

Recuadro 3

Falta de coherencia entre el objetivo y los resultados de la ENISA con respecto a las IOUE

Algunas de las prioridades trienales de la ENISA recogidas en el programa de trabajo plurianual 2018-2020 en el marco del objetivo 3.2 «Ayudar al desarrollo de la capacidad de las instituciones de la UE» son:

- ofrecer asesoramiento proactivo a las instituciones de la Unión sobre el refuerzo de su seguridad de las redes y de la información (SRI) (determinar las prioridades para las agencias y los órganos de la UE con más necesidades de desarrollo de la capacidad en materia de SRI mediante el establecimiento de interacciones periódicas con ellos (por ejemplo, seminarios anuales) y centrarse en estas prioridades);

- intentar ayudar a las instituciones de la UE en los enfoques del SRI y facilitárselos (establecer asociaciones con el CERT-UE e instituciones con sólidas capacidades en materia de SRI para apoyar sus acciones en el marco de este objetivo)».

En los programas de trabajo de la ENISA para 2018, 2019 y 2020, solo existen dos objetivos operativos (resultados) en el marco del objetivo 3.2:

- Participación en el Comité de Dirección del CERT-UE y representación de las agencias de la UE que utilizan el servicio CERT-UE.

- Cooperación con los órganos pertinentes de la UE sobre iniciativas relativas a la dimensión NIS relacionadas con sus misiones (incluidas EASA, CERT-UE, AED y EC3).

Los objetivos operativos no comprenden ninguna actividad relacionada con el asesoramiento proactivo. Además, el objetivo de determinar las prioridades para las agencias con mayores necesidades no se tradujo en resultados operativos, ya que se sustituyó por el de establecer contacto con las agencias para representar sus necesidades en el Comité de Dirección del CERT-UE.

67 El principal órgano decisorio de la ENISA es su Consejo de Administración, que se compone de un miembro nombrado por cada uno de los veintisiete Estados miembros, y dos nombrados por la Comisión[31] (véase la ***ilustración 6***). Cada miembro tiene un voto y las decisiones se toman por mayoría[32]. En consecuencia, las acciones relativas a los Estados miembros pueden tener mayor prioridad que las relativas a las IOUE. Por

[31] Artículo 14 del Reglamento sobre la Ciberseguridad.

[32] Artículo 18 del Reglamento sobre la Ciberseguridad.

ejemplo, en el programa de trabajo de la ENISA para 2018, el Consejo de Administración decidió, debido a la falta de recursos suficientes, dar prioridad a determinadas actividades y suprimir tres, una de las cuales consistía en apoyar la evaluación de las políticas, los procedimientos y las prácticas existentes en materia de SRI en las instituciones de la UE. Esta actividad tenía por objeto permitir a la ENISA elaborar una visión general de las prácticas y la madurez indicativa en materia de ciberseguridad de las IOUE, como base para futuras acciones específicas.

68 Por consiguiente, la ambición de la ENISA de prestar asistencia proactiva a las IOUE, expresada en sus objetivos estratégicos, no se ha materializado en objetivos operativos o acciones concretas. El apoyo en los ámbitos del desarrollo de capacidades y la cooperación operativa se ha limitado hasta ahora, previa solicitud, a determinadas IOUE.

69 En el Reglamento sobre la Ciberseguridad también se establece que, para ayudar a las IOUE en el desarrollo de la capacidad, la ENISA debe prestar el apoyo adecuado al CERT-UE. En el momento de la auditoría, dicho apoyo se había limitado a unas pocas acciones específicas. Por ejemplo, en 2019, la ENISA llevó a cabo una revisión interpares del CERT-UE, en el contexto de su pertenencia a la red de CSIRT de la UE (establecida por la Directiva SRI).

70 Según las respuestas a nuestra encuesta, la ENISA publica informes y directrices de alta calidad sobre ciberseguridad, algunos de los cuales son utilizados por las IOUE. Sin embargo, no existen directrices específicas dirigidas a las IOUE y a su propio entorno y necesidades. Las IOUE, especialmente las menos avanzadas en ciberseguridad, necesitan orientación práctica no solo sobre «qué» hacer, sino también sobre «cómo» hacerlo. Hasta la fecha, la ENISA y el CERT-UE han facilitado este apoyo de forma limitada y no sistemática.

71 La ENISA ha impartido una serie de cursos de formación sobre ciberseguridad dirigidos a las autoridades de los Estados miembros pero a los que también ha asistido un número limitado de participantes de las IOUE. Solamente proporción dos cursos de autoaprendizaje dirigidos específicamente a las IOUE. La ENISA también ofrece material de formación en línea en su sitio web al que pueden acceder las IOUE, hasta la fecha este ha consistido principalmente en cursos para expertos técnicos del CSIRT, por lo que no han sido útiles para la mayoría de las IOUE.

72 Aparte de la formación, la ENISA puede prestar apoyo a las IOUE mediante ejercicios de ciberseguridad. En octubre de 2020, la ENISA, en cooperación con el CERT-UE, ayudó a realizar un ejercicio de ciberseguridad para el ICTAC, que es el único

ejercicio que la Agencia ha organizado específicamente para participantes de IOUE. Aparte de eso, la ENISA ha ayudado a organizar una serie de ejercicios a petición de algunas IOUE (por ejemplo, eu-LISA, AESM, el Parlamento Europeo y Europol), principalmente para sus partes interesadas en las autoridades de los Estados miembros, con la participación de personal de IOUE.

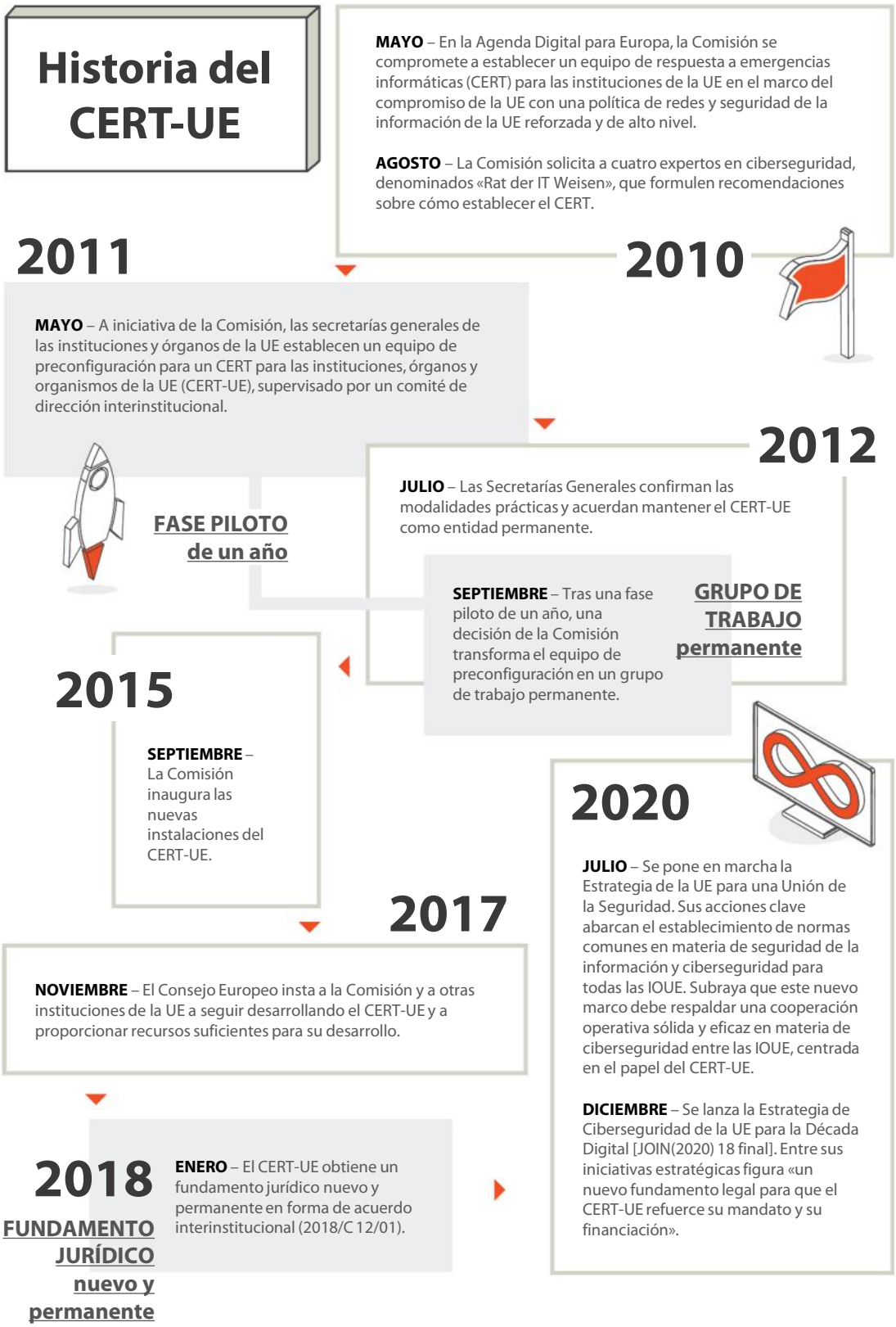
73 El Reglamento sobre la Ciberseguridad también introdujo como nueva función de la ENISA ayudar a las IOUE en sus políticas de divulgación de vulnerabilidades de manera voluntaria. Sin embargo, la ENISA todavía no tiene una visión general de las políticas de divulgación de vulnerabilidades de cada IOUE, y no les ayuda a establecer y aplicar dichas políticas.

El CERT-UE por sus componentes, pero sus medios no están a la altura de los actuales desafíos de ciberseguridad

74 A raíz de una serie de iniciativas (véase la ***ilustración 7***), en septiembre de 2012, en una Decisión de la Comisión[33] se estableció el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE) como grupo de trabajo permanente para las IOUE (véase el apartado ***08***).

[33] Comunicado de prensa de la Comisión Europea: Se ha reforzado la seguridad informática de las instituciones de la UE a raíz del éxito del proyecto piloto.

Ilustración 7 – Historia del CERT-UE



Fuente: Tribunal de Cuentas Europeo.

75 Aunque independiente en sus operaciones, el CERT-UE sigue siendo un grupo de trabajo sin personalidad jurídica. Administrativamente depende de la Comisión Europea (DG Informática), de la que recibe apoyo logístico y administrativo. El objetivo del CERT-UE es reforzar la seguridad de la infraestructura informática de las IOUE mediante la mejora de su capacidad para hacer frente a las ciberamenazas y vulnerabilidades y para prevenir, detectar y responder a los ciberataques. El CERT-UE cuenta con unos cuarenta empleados organizados en equipos de especialistas que se dedican, por ejemplo, a la inteligencia sobre amenazas, el análisis forense digital y la respuesta a incidentes.

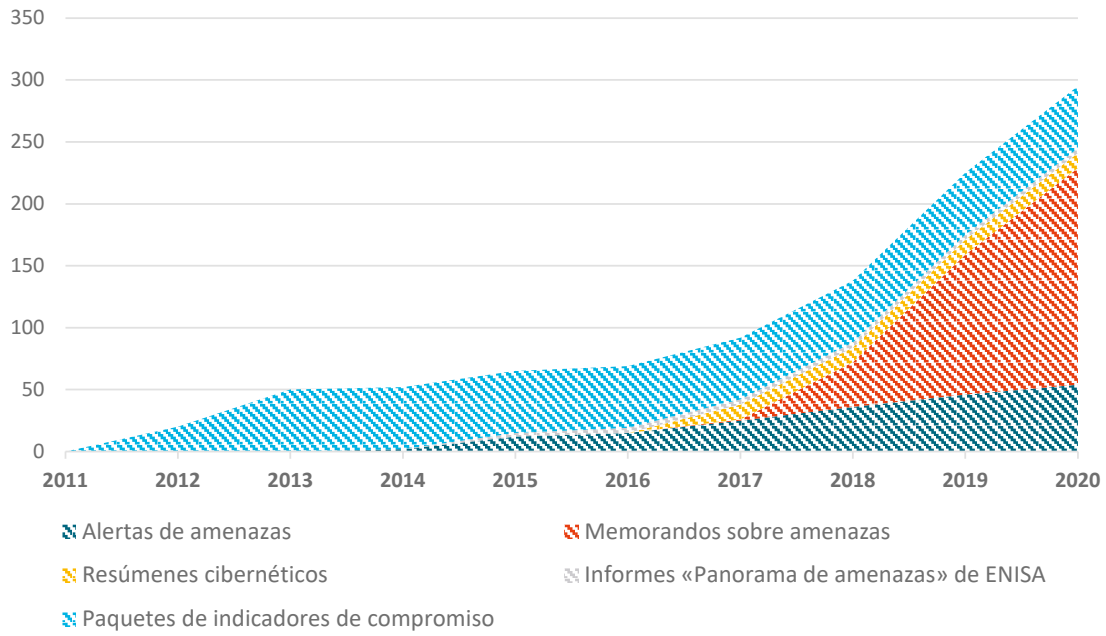
El CERT-UE es un socio apreciado con una carga de trabajo cada vez mayor

76 El CERT-UE solicita comentarios y sugerencias de las Partes a través de talleres trimestrales y reuniones bilaterales anuales y encuestas de satisfacción. Según las encuestas de satisfacción y nuestra propia encuesta, las Partes están muy satisfechas con los servicios prestados por el CERT-UE. La evolución del catálogo de servicios del CERT-UE es prueba de su esfuerzo por adaptarse a las necesidades de las IOUE.

77 Mientras que las grandes IOUE con una importante capacidad interna tienden a utilizar el CERT-UE principalmente como centro de intercambio de información y fuente de información sobre amenazas, las IOUE más pequeñas dependen del CERT-UE para una gama más amplia de servicios, como registros de supervisión, pruebas de penetración, ejercicios de equipo rojo y apoyo para la respuesta ante incidentes. Los servicios del CERT-EU son especialmente valiosos para las IOUE más pequeñas debido a sus conocimientos técnicos internos limitados y a la falta de economías de escala (véanse los apartados ***31*** y ***33***).

78 El CERT-UE ha reforzado sus capacidades y procedimientos en los últimos años en el contexto de un drástico aumento de las amenazas y los incidentes. El número de productos documentales del CERT-EU, especialmente alertas y memorandos de amenazas, registra un crecimiento constante (***ilustración 8***). En 2020, el CERT-UE emitió 171 memorandos sobre amenazas y 53 alertas de amenaza (cantidad muy superior a los 80 memorandos y las 40 alertas que tenía previsto emitir inicialmente).

Ilustración 8 – Aumento de los productos de inteligencia sobre amenazas



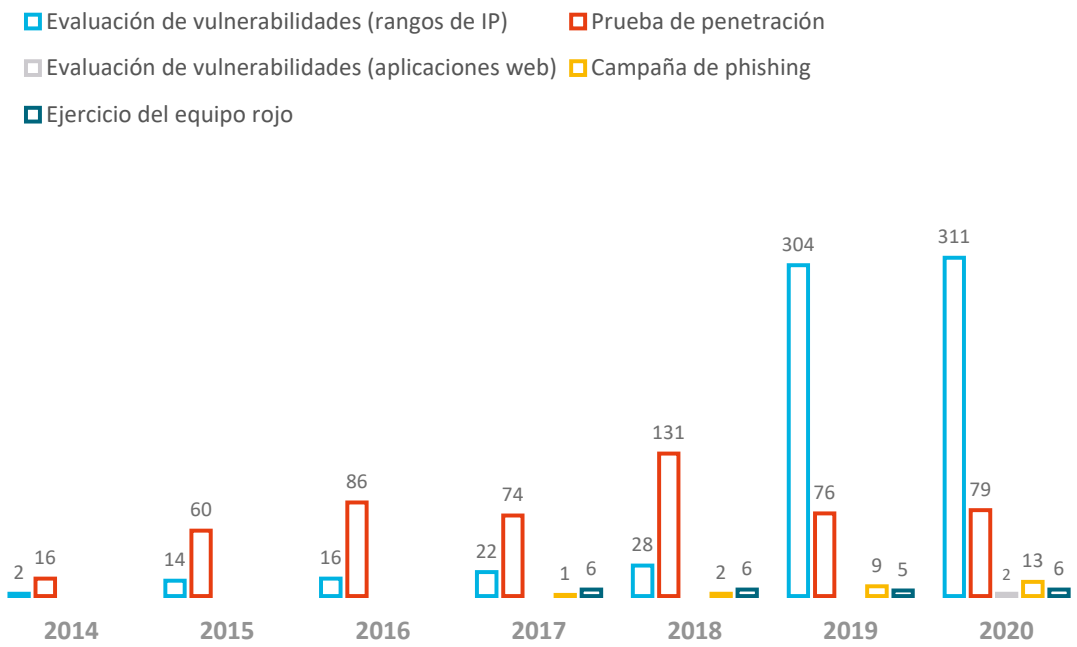
Fuente: Tribunal de Cuentas Europeo, a partir de datos facilitados por el CERT-UE.

79 El CERT-UE también apoya a IOUE en la gestión de ciberincidentes. Mientras que el 52 % de las IOUE cuentan con un equipo de respuesta interno o al menos un coordinador de incidentes, el 48 % restante recurre al CERT-UE u a otros proveedores externos en caso de incidente. Sin embargo, incluso las grandes IOUE con capacidad de respuesta interna pueden solicitar apoyo al CERT-UE para hacer frente a incidentes complejos.

80 El número total de incidentes gestionados por el CERT-UE pasó de 561 en 2019 a 884 en 2020. En concreto, los incidentes significativos han pasado de solo 1 en 2018 a 13 en 2020. En 2021, el número de incidentes significativos ya había alcanzado los 17, frente a los 13 en 2020, que fue un año récord. Estos incidentes significativos suelen ser provocados por amenazas muy sofisticadas. Pueden afectar a varias IOUE, implicar contacto con las autoridades y, por lo general, las partes afectadas y el CERT-UE invierten semanas o meses de trabajo en su erradicación.

81 El CERT-UE es también el principal proveedor de pruebas y evaluaciones proactivas de las ciberdefensas de las IOUE. En la ***ilustración 9*** se presenta un resumen de la actividad del CERT-EU en este ámbito. Además, a partir de 2020, el CERT-UE también realiza análisis de redes externas.

Ilustración 9 – Pruebas y evaluaciones realizadas por el CERT-UE



Fuente: Tribunal de Cuentas Europeo, a partir de datos facilitados por el CERT-UE.

Las Partes no comparten con el CERT-UE la información pertinente a su debido tiempo

82 El ACI[34] establece que las Partes deben notificar al CERT-UE los incidentes de ciberseguridad significativos. Sin embargo, en la práctica, esto no siempre ha sucedido. El ACI no proporciona un mecanismo para exigir la notificación obligatoria y oportuna de incidentes «significativos» de las Partes del CERT-UE. La definición genérica de «incidentes significativos» recogida en el ACI deja a discreción de las IOUE la posibilidad de notificar un incidente. Según la dirección de CERT-UE, algunas Partes no han compartido información sobre incidentes significativos a su debido tiempo, lo que dificulta su función de centro de intercambio de información sobre ciberseguridad y coordinación de la respuesta a incidentes para todas las IOUE. Por ejemplo, una Parte que se enfrentó a una amenaza muy sofisticada no informó al CERT-UE ni solicitó su apoyo. Esto impidió que el ERT-UE recopilara información sobre amenazas que habría resultado útil para apoyar a otras Partes que se enfrentaran a la misma amenaza. Al menos seis IOUE resultaron afectadas por este ataque.

83 Las Partes tampoco han compartido activamente información oportuna con el CERT-UE sobre las ciberamenazas y vulnerabilidades que les afectan, a pesar de que el

[34] Cláusula 3,3 del Acuerdo interinstitucional (ACI) firmado el 20.12.2017.

ACI[35] les exige hacerlo. El equipo de análisis forense digital y respuesta a incidentes de CERT-UE no ha recibido notificaciones sobre vulnerabilidades o deficiencias en los controles descubiertos fuera del contexto de los incidentes que está investigando activamente. Las Partes no comparten proactivamente los resultados pertinentes de las auditorías de seguridad internas o externas.

84 Además, el ACI no obliga a las IOUE a notificar al CERT-UE cambios significativos en su entorno informático y, por consiguiente, las Partes no han informado sistemáticamente al CERT-UE de los cambios pertinentes. Por ejemplo, las IOUE no siempre informan al CERT-UE de los cambios en sus rangos de IP (es decir, la lista de direcciones de Internet de su infraestructura). El CERT-UE necesita rangos de IP actualizados para, por ejemplo, realizar análisis cuando se descubren vulnerabilidades importantes. El hecho de que las IOUE no informen al CERT-UE de tales cambios afecta a su capacidad para apoyarlos. La falta de notificación al CERT-UE también afecta a su capacidad para supervisar los sistemas y genera más trabajo para corregir datos inexactos en las herramientas de supervisión. Según su dirección, el CERT-UE a veces descubre una infraestructura informática hasta entonces desconocida cuando tratan un incidente. Además, aparte de los casos específicos, actualmente el CERT-UE no tiene una visión global de las redes y sistemas informáticos de la comunidad de IOUE.

85 Dado que el ACI carece de un mecanismo de aplicación, las notificaciones de las IOUE al CERT-UE —elemento esencial para crear una comunidad de IOUE de preparación centrada en el CERT-UE— seguirán siendo poco sistemáticas.

Los recursos del CERT-UE son inestables y no están a la altura del nivel de amenaza actual

86 En el ACI[36] se establece que el CERT-UE debe dotarse de financiación y recursos humanos sostenibles garantizando a la vez su rentabilidad y un núcleo adecuado de personal permanente. El activo más importante del CERT-UE es su personal altamente capacitado y especializado. En la ***ilustración 10*** se muestra el cambio en los niveles de dotación de personal del CERT-EU desde su inicio en 2011 hasta hoy.

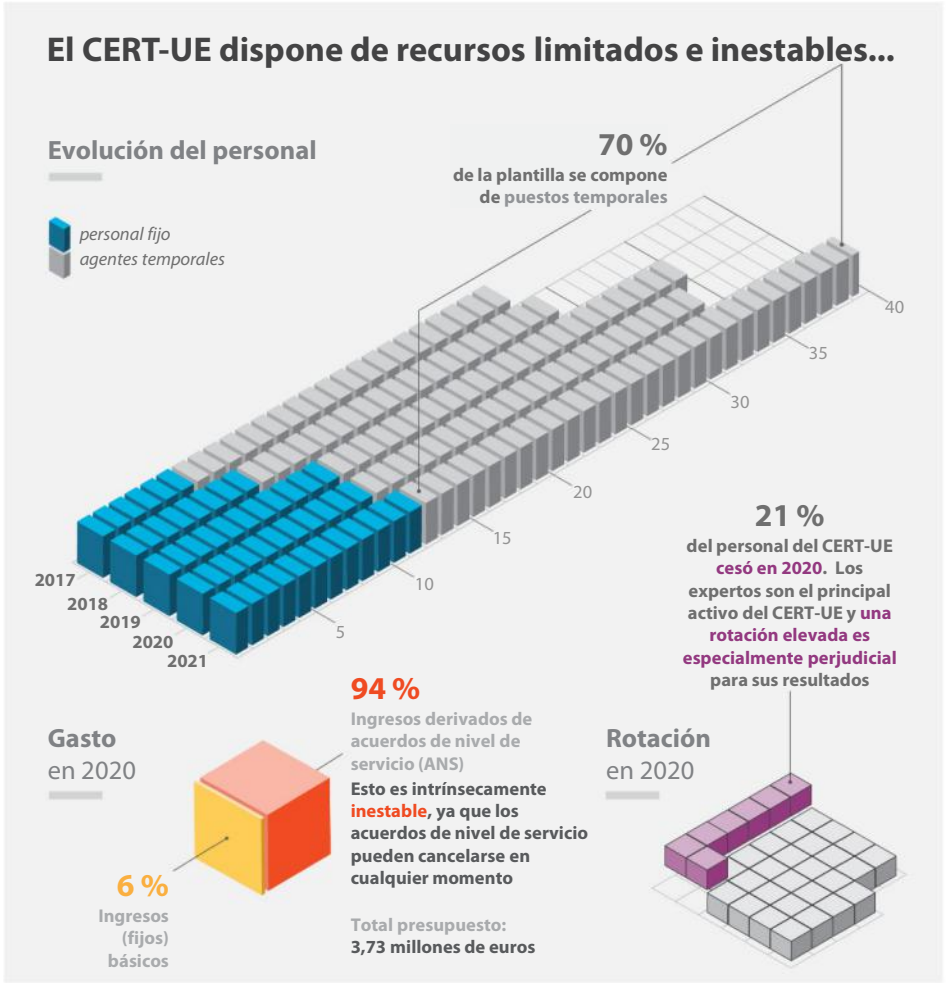
87 Más de dos tercios de los efectivos del CERT-UE tienen contratos temporales. Su salario no es muy competitivo en el mercado de expertos en ciberseguridad y, según la dirección del CERT-UE, cada vez resulta más difícil contratarlos y retenerlos. Cuando los salarios no son lo suficientemente atractivos para los candidatos con mayor

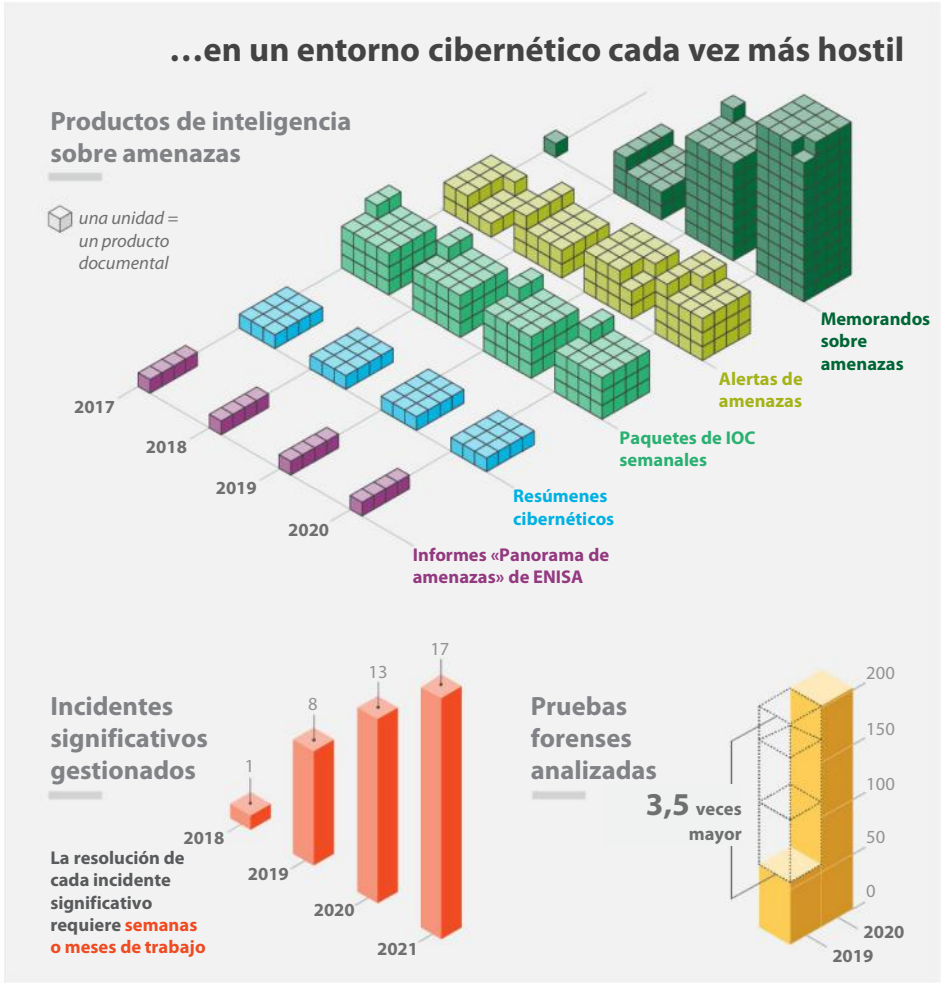
[35] Cláusula 3.2 del Acuerdo interinstitucional (ACI).

[36] Considerando 7 del Acuerdo interinstitucional (ACI).

experiencia, el CERT-UE debe recurrir a la contratación de personal de menor experiencia e invertir tiempo en su formación. Además, los contratos tienen una duración máxima de seis años, lo que significa que el CERT-UE no tiene más opción que dejar que el personal contratado se vaya cuando ya ha acumulado experiencia. La rotación de personal fue especialmente alta en 2020: el 21 % del personal abandonó el CERT-UE y no pudieron cubrirse todas las sustituciones. Respecto a años anteriores, en 2019 abandonó el 9 % de la plantilla y en 2018 el 13 %.

Ilustración 10 – Recursos y desafíos del CERT-UE





Fuente: Tribunal de Cuentas Europeo, a partir de datos del CERT-UE.

88 La dirección del CERT-UE ha subrayado que, en la actualidad, su equipo de análisis forense digital y respuesta a incidentes está desbordado, y el resto de sus equipos no pueden satisfacer la demanda. En consecuencia, el CERT-UE ha tenido que reducir sus actividades: por ejemplo, actualmente no realiza evaluaciones de madurez de las Partes, debido a la falta de recursos. El servicio de «advertencias sobre actividades sospechosas» del CERT-UE empezó a funcionar más tarde de lo previsto, debido de nuevo a la escasez de recursos. Además, varias de las Partes entrevistadas afirmaron que tuvieron que esperar mucho tiempo para acceder a los servicios del CERT-UE.

89 Hasta ahora, las limitaciones de recursos han obligado al CERT-UE a centrarse en particular en la protección de la infraestructura informática *in situ* convencional frente a las principales amenazas de grupos (normalmente respaldados por Estados nación) que entrañan amenazas persistentes avanzadas. Sin embargo, según su dirección, la ampliación del perímetro de TI de las IOUE (que ahora incluye la nube, los dispositivos móviles y las herramientas de teletrabajo) necesita una mayor supervisión y protección, y las amenazas de menor nivel (como la ciberdelincuencia y los programas de secuestro) también requieren más atención.

90 El ACI no prevé que el CERT-UE tenga capacidad operativa las veinticuatro horas al día, los siete días a la semana. El CERT-UE no dispone actualmente de los recursos ni de una estrategia de recursos humanos adecuada para operar fuera del horario laboral de manera permanente y estructurada, a pesar de que los ataques de ciberseguridad no se llevan a cabo en dicho horario. En el caso de las propias IOUE, solo treinta y cinco de las sesenta y cinco encuestadas cuentan con un responsable informático localizable fuera del horario laboral.

91 Para financiar las operaciones del CERT-UE, el Comité de Dirección aprobó en 2012 un modelo de acuerdo de nivel de servicio (ANS). Todas las Partes reciben servicios básicos de forma gratuita y pueden pagar para adquirir servicios ampliados, mediante la firma de un ANS. El presupuesto del CERT-UE para 2020 ascendió a 3 745 000 euros, de los que el 6 % se financió con cargo al presupuesto de la UE y el 94 % con cargo a los ANS. Sin embargo, las Partes son muy heterogéneas: algunas tienen requisitos de seguridad informática maduros, mientras que otros tienen presupuestos de TI modestos y un nivel muy bajo de madurez por lo que se refiere a la ciberseguridad. Por este motivo, los debates sobre los ANS dan lugar a una combinación de requisitos de seguridad elevados para algunas IOUE y una relativa falta de disposición o capacidad para contribuir por parte de otras.

92 Además, los ANS deben renovarse individualmente cada año. Además de ser una carga administrativa, esto genera problemas de flujo de tesorería, ya que el CERT-UE no dispone de fondos procedentes al mismo tiempo de todos los ANS. Además, las agencias pueden rescindir los ANS en cualquier momento. Se corre el riesgo de poner en marcha un círculo vicioso en el que, debido a la pérdida de ingresos, el CERT-UE se vea obligado a reducir sus servicios y no pueda cubrir la demanda, lo que a su vez provocará que otras IOUE rescindan sus ANS y se opten por proveedores privados. Teniendo en cuenta lo anterior, el actual modelo de financiación no es ideal para garantizar un nivel de servicio estable y óptimo.

93 Ante un panorama de ciberamenazas en rápida evolución (véanse los apartados ***06*** y ***80***), el Comité de Dirección del CERT-EU, en su reunión del 19 de febrero de 2020, aprobó una propuesta estratégica para que el CERT-EU ampliara sus servicios de ciberseguridad y desarrollara «capacidades operativas plenas». La propuesta iba acompañada de un análisis de las necesidades de personal y financiación del CERT-UE. Este análisis concluyó que el CERT-UE necesitaría 14 puestos de administrador permanentes adicionales, añadidos gradualmente durante el periodo 2021-2023. El CERT-UE funcionaría entonces a plena capacidad a partir de 2023. Según esta propuesta, en términos de financiación, el CERT-UE tendría que aumentar su presupuesto en 7,6 millones de euros durante el periodo 2021-2023, hasta alcanzar los 11,3 millones de euros en 2024.

94 Sin embargo, pese a que las IOUE apoyan la propuesta estratégica sobre la provisión de recursos adicionales para el CERT-UE, todavía no han llegado a un acuerdo sobre las modalidades prácticas, en primer lugar para el período transitorio de 2021-2023, y, en segundo lugar, a largo plazo, tras la entrada en vigor de la futura normativa sobre ciberseguridad (véase el apartado ***12***).

Conclusiones y recomendaciones

95 Concluimos que la comunidad de instituciones, órganos y organismos de la UE (IOUE) no ha alcanzado un nivel de preparación a la altura de las amenazas. Nuestro trabajo demuestra que las IOUE tienen distintos niveles de madurez en ciberseguridad y, dado que suelen estar interconectadas entre sí y con organizaciones públicas y privadas en los Estados miembros, las deficiencias de ciberseguridad de una IOUE pueden exponer a otras a ciberamenazas.

96 Constatamos que no siempre se aplicaban buenas prácticas, como algunos controles esenciales. Una buena gobernanza de ciberseguridad es esencial para la seguridad de los sistemas de información e informáticos, pero esta aún no aplica en algunas IOUE: en muchos casos, no existen estrategias y planes de seguridad informática o estos no están respaldados por la alta dirección, las políticas de seguridad no siempre se formalizan y las evaluaciones de riesgos no abarcan todo el entorno informático. El gasto en ciberseguridad es desigual, ya que algunas IOUE no gastan lo suficiente en comparación con homólogas de tamaño similar (véanse los apartados ***21*** a ***33***, y ***37*** y ***38***).

97 Los programas de formación y concienciación en materia cibernética son un elemento clave en un marco de ciberseguridad eficaz. Sin embargo, solo el 29 % de las IOUE imparten formación obligatoria sobre ciberseguridad a los responsables de los sistemas informáticos que contienen información delicada, y la formación ofrecida suele ser informal. En los últimos cinco años, el 55 % de las IOUE ha organizado una o varias campañas simuladas de *phishing* (o ejercicios similares). Estos ejercicios son una herramienta importante para formar y concienciar al personal, pero no todas las IOUE los utilizan sistemáticamente (véanse los apartados ***34*** a ***36***). Además, no todas las IOUE disponen de medidas regulares de ciberseguridad sujetas a una garantía independiente (véanse los apartados ***39*** a ***44***).

98 El CERT-UE es un socio muy apreciado por las IOUE a las que presta servicio, pero su capacidad está sobrepasada. Su carga de trabajo, en términos de inteligencia sobre amenazas y gestión de incidentes, ha crecido rápidamente desde 2018. Los ciberincidentes significativos se han multiplicado por diez. Al mismo tiempo, las IOUE no siempre comparten información oportuna sobre incidentes significativos, vulnerabilidades y cambios importantes en su infraestructura informática. Esto menoscaba la eficacia del CERT-UE, ya que impide que alerte a otras IOUE potencialmente afectadas y puede dar lugar a que no se detecten incidentes significativos. Además, los recursos del CERT-UE son inestables y no están a la altura

del nivel actual de amenaza ni de las necesidades de las IOUE. El Comité de Dirección del CERT-UE aprobó en 2020 una propuesta estratégica sobre la provisión de los recursos adicionales que necesita, pero las Partes aún no han alcanzado un acuerdo sobre las modalidades prácticas para la provisión de tales recursos. En consecuencia, los efectivos del CERT-EU no pueden satisfacer la demanda y tienen que reducir las actividades (véanse los apartados ***74*** a ***93***).

Recomendación 1 – Mejorar la preparación en ciberseguridad de las IOUE mediante normas comunes vinculantes y un incremento de los recursos destinados al CERT-UE

La Comisión debería incluir los siguientes principios en su próxima propuesta de Reglamento relativo a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en todas las IOUE:

a) la alta dirección debería asumir la responsabilidad de la gobernanza de la ciberseguridad respaldando las estrategias de ciberseguridad y las políticas de seguridad clave y nombrando a un Responsable principal de Seguridad de los Sistemas de Información independiente (o una función equivalente).

b) Las IOUE deberían disponer de un marco de gestión de riesgos para la seguridad informática que abarque la totalidad de su infraestructura informática y realizar evaluaciones de riesgos periódicas.

c) Las IOUE deberían impartir formación de concienciación sistemática a todo el personal, incluida la dirección.

d) Las IOUE deberían someterse sus ciberdefensas a auditorías y pruebas periódicas. En las auditorías también debería examinarse si los recursos dedicados a la ciberseguridad son suficientes.

e) Las IOUE deberían informar, sin demora, al CERT-UE sobre los incidentes de ciberseguridad significativos, así como sobre los correspondientes cambios y vulnerabilidades de su infraestructura informática.

f) En sus presupuestos, las IOUE deberían incrementar los recursos asignados a al CERT-UE con arreglo a las necesidades identificadas en la propuesta estratégica refrendada por su Comité de Dirección.

g) La normativa debería incluir disposiciones para designar a una entidad que, en representación de todas las IOUE, disponga del mandato y los recursos apropiados para supervisar el cumplimiento de normas comunes sobre ciberseguridad por todas las IOUE y para emitir orientaciones, recomendaciones y llamamientos para la adopción de medidas.

Plazo previsto de aplicación: Primer trimestre de 2023

99 Las IOUE han establecido mecanismos de cooperación en el ámbito de la ciberseguridad, pero hemos observado que no se aprovechan plenamente las posibles

sinergias. Existe una estructura formalizada para el intercambio de información, en la que los agentes y comités desempeñan funciones complementarias. Sin embargo, la participación en los foros interinstitucionales de las IOUE más pequeñas se ve obstaculizada por la limitación de sus recursos, y la representación de las agencias descentralizadas y las empresas conjuntas en el Comité de Dirección del CERT-UE no es óptima. También constatamos que las IOUE no comparten sistemáticamente entre sí información sobre proyectos relacionados con la ciberseguridad, evaluaciones de seguridad y otros contratos de servicios. Esto puede dar lugar a una duplicación de los esfuerzos y a un aumento de los costes. Observamos dificultades operativas en el intercambio de información delicada no clasificada por correo electrónico cifrado o videoconferencia, debido a la falta de interoperabilidad de las soluciones informáticas, las orientaciones contradictorias relativas al permiso para utilizarlas, y la falta de marcadores de información y normas de manipulación comunes (véanse los apartados ***45*** a ***63***).

Recomendación 2 – Promover nuevas sinergias entre las IOUE en determinadas áreas

la Comisión, en el contexto del Comité interinstitucional para la transformación digital, debería promover las siguientes acciones entre las IOUE:

a) adoptar soluciones para la interoperabilidad de los canales de comunicación seguros, desde el correo electrónico cifrado hasta la videoconferencia, y abogar por marcas comunes y normas de tratamiento comunes en relación con la información delicada no clasificada;

b) compartir sistemáticamente información sobre proyectos relacionados con la ciberseguridad que tengan una posible repercusión interinstitucional, evaluaciones de seguridad realizadas al *software* y contratos vigentes con proveedores externos;

c) definir especificaciones para contratos marco y de aprovisionamiento comunes para servicios de ciberseguridad en los que todas las IOUE puedan participar para fomentar economías de escala.

Plazo previsto de aplicación: Cuarto trimestre de 2023

100 La Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el CERT-UE son las dos principales entidades encargadas de apoyar a las IOUE en materia de ciberseguridad. Sin embargo, debido a que los recursos son limitados y a que se ha dado prioridad a otras áreas, no han podido proporcionar a las IOUE todo el apoyo que

necesitan, sobre todo en relación con el desarrollo de capacidades de aquellas que poseen menor experiencia en ciberseguridad (véanse los apartados ***64*** a ***93***).

Recomendación 3 – Reforzar la atención del CERT-UE y la ENISA en las IOUE con menor madurez

El CERT-UE y la ENISA deberían:

a) determinar las áreas prioritarias en las que las IOUE necesitan más apoyo, por ejemplo mediante evaluaciones de madurez;

b) llevar a cabo acciones de desarrollo de la capacidad, de acuerdo con su memorando de entendimiento.

Plazo previsto de aplicación: Cuarto trimestre de 2022

El presente informe ha sido aprobado por la Sala III, presidida por Bettina Jakobsen, Miembro del Tribunal de Cuentas, en Luxemburgo en su reunión del 22 de febrero de 2022.

Por el Tribunal de Cuentas

Klaus-Heiner Lehne
Presidente

Anexos

Anexo I — Lista de IOUE incluidas en la encuesta

Nombre de la IOUE	Tipo
Parlamento Europeo (PE)	Institución (artículo 13, apartado 1, del TUE)
Consejo de la Unión Europea y Consejo Europeo	Institución (artículo 13, apartado 1, del TUE)
Comisión Europea	Institución (artículo 13, apartado 1, del TUE)
Tribunal de Justicia de la Unión Europea (TJUE)	Institución (artículo 13, apartado 1, del TUE)
Banco Central Europeo (BCE)	Institución (artículo 13, apartado 1, del TUE)
Tribunal de Cuentas Europeo	Institución (artículo 13, apartado 1, del TUE)
Servicio Europeo de Acción Exterior (SEAE)	Órgano (artículo 27, apartado 3, del TUE)
Comité Económico y Social Europeo (CESE) y Comité Europeo de las Regiones (CDR)[37]	Órganos (artículo 13, apartado 4, del TUE)
Banco Europeo de Inversiones (BEI)	Órgano (artículo 308 del TFUE)
Autoridad Laboral Europea (ALE)	Agencia descentralizada
Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía (ACER)	Agencia descentralizada
Agencia de Apoyo al ORECE	Agencia descentralizada
Oficina Comunitaria de Variedades Vegetales (OCVV)	Agencia descentralizada
Agencia Europea para la Seguridad y la Salud en el Trabajo (EU-OSHA)	Agencia descentralizada
Agencia Europea de la Guardia de Fronteras y Costas (Frontex)	Agencia descentralizada
Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA)	Agencia descentralizada
Agencia de Asilo de la Unión Europea (AAUE)	Agencia descentralizada
Agencia de la Unión Europea para la Seguridad Aérea (AESA)	Agencia descentralizada
Autoridad Bancaria Europea (ABE)	Agencia descentralizada

[37] El CESE y el CDR cuentan como una IOUE.

Nombre de la IOUE	Tipo
Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC)	Agencia descentralizada
Centro Europeo para el Desarrollo de la Formación Profesional (Cedefop)	Agencia descentralizada
Agencia Europea de Sustancias y Mezclas Químicas (ECHA)	Agencia descentralizada
Agencia Europea de Medio Ambiente (AEMA)	Agencia descentralizada
Agencia Europea de Control de la Pesca (AECP)	Agencia descentralizada
Autoridad Europea de Seguridad Alimentaria (EFSA)	Agencia descentralizada
Fundación Europea para la Mejora de las Condiciones de Vida y de Trabajo (Eurofound)	Agencia descentralizada
Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía [que sustituirá a la: Agencia de la Unión Europea para el Programa Espacial] (EUSPA)	Agencia descentralizada
Instituto Europeo de la Igualdad de Género (EIGE)	Agencia descentralizada
Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ)	Agencia descentralizada
Agencia Europea de Seguridad Marítima (AESM)	Agencia descentralizada
Agencia Europea de Medicamentos (EMA)	Agencia descentralizada
Observatorio Europeo de las Drogas y las Toxicomanías (EMCDDA)	Agencia descentralizada
Agencia de la Unión Europea para la Ciberseguridad (ENISA)	Agencia descentralizada
Agencia de la Unión Europea para la Formación Policial (CEPOL)	Agencia descentralizada
Oficina Europea de Policía (Europol)	Agencia descentralizada
Agencia Ferroviaria de la Unión Europea (AFE)	Agencia descentralizada
Autoridad Europea de Valores y Mercados (ESMA)	Agencia descentralizada
Fundación Europea de Formación (ETF)	Agencia descentralizada
Agencia de los Derechos Fundamentales de la Unión Europea (FRA)	Agencia descentralizada
Oficina de Propiedad Intelectual de la Unión Europea [denominada OAMI hasta el 23 de marzo de 2016](EUIPO)	Agencia descentralizada
Junta Única de Resolución (JUR)	Agencia descentralizada
Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust)	Agencia descentralizada
Centro de Traducción de los Órganos de la Unión Europea (CdT)	Agencia descentralizada
Fiscalía Europea	Agencia descentralizada
Instituto Europeo de Innovación y Tecnología (EIT)	Órgano en el marco de I+i
Empresa Común para la investigación sobre la gestión del tránsito aéreo del Cielo Único Europeo (Empresa Común SESAR)	Empresa Común con arreglo al TFUE

Nombre de la IOUE	Tipo
Empresa Común Componentes y Sistemas Electrónicos para el Liderazgo Europeo (ECSEL)	Empresa Común con arreglo al TFUE
Empresa Común de Pilas de Combustible e Hidrógeno (FCH)	Empresa Común con arreglo al TFUE
Empresa Común para la Iniciativa sobre Medicamentos Innovadores 2 (Empresa Común IMI 2)	Empresa Común con arreglo al TFUE
Empresa Común Clean Sky 2	Empresa Común con arreglo al TFUE
Empresa Común para las Bioindustrias (Empresa Común BBI)	Empresa Común con arreglo al TFUE
Empresa Común Shift2Rail (Empresa Común S2R)	Empresa Común con arreglo al TFUE
Empresa Común de Informática de Alto Rendimiento Europea (Empresa Común EuroHPC)	Empresa Común con arreglo al TFUE
Empresa Común Europea para el ITER y el Desarrollo de la Energía de Fusión (Fusion for Energy)	Empresa Común con arreglo al TFUE
Misión asesora de la Unión Europea para la reforma del sector de la seguridad civil en Ucrania (EUAM Ucrania)	Misión civil (PCSD)
Misión de la Unión Europea de Asistencia y Gestión Integrada de las Fronteras en Libia (EUBAM Libia)	Misión civil (PCSD)
Misión PCSD de la Unión Europea en Níger (EUCAP Sahel Níger)	Misión civil (PCSD)
Misión de Observación de la Unión Europea en Georgia (EUMM Georgia)	Misión civil (PCSD)
Misión de Policía de la Unión Europea para los Territorios Palestinos (EUPOL COPPS)	Misión civil (PCSD)
Misión asesora PCSD de la Unión Europea en la República Centroafricana (EUAM RCA)	Misión civil (PCSD)
Misión asesora de la Unión Europea en apoyo de la reforma del sector de la seguridad en Irak (EUAM Irak)	Misión civil (PCSD)
Misión de asistencia fronteriza de la Unión Europea para el paso fronterizo de Rafah (EU BAM Rafah)	Misión civil (PCSD)
Misión PCSD de la Unión Europea en Mali (EUCAP Sahel Mali)	Misión civil (PCSD)
Misión de la Unión Europea de Desarrollo de las Capacidades en Somalia (EUCAP Somalia)	Misión civil (PCSD)
Misión de la Unión Europea por el Estado de Derecho en Kosovo (EULEX Kosovo)	Misión civil (PCSD)

Anexo II — Información adicional sobre los principales comités interinstitucionales

Comité interinstitucional para la transformación digital (ICDT)

El ICDT es un foro para intercambiar información y fomentar la cooperación en el ámbito de la TI. Se creó en mayo de 2020 para sustituir al antiguo Comité Interinstitutionnel de l'Informatique (CII). El ICDT está compuesto por los responsables de los departamentos informáticos de las IOUE, y cuenta con un subgrupo de ciberseguridad (ICDT CSSG) cuya función es promover la cooperación entre las IOUE en materia de ciberseguridad y servir de foro para el intercambio de información.

El poder decisorio del ICDT se limita a cuestiones que no afectan al modo en que las instituciones cumplen su misión y no afectan a la gobernanza dentro de cada institución. Por lo que se refiere a las decisiones que excedan de sus competencias, el ICDT podrá formular recomendaciones al colegio de secretarías generales de las instituciones y órganos de la UE.

Conforme al mandato del ICDT, sus miembros son representantes de cada institución y órgano de la UE y un representante designado por las agencias de la UE (ICTAC). La Secretaría General del Consejo preside actualmente el ICDT.

Subgrupo de ciberseguridad ICDT (ICDT CSSG)

El ICDT CSSG, en su configuración actual, se estableció en septiembre de 2020 para sustituir al subgrupo de seguridad permanente del antiguo ICI. En comparación con su predecesor, el ICDT CSSG tiene un enfoque más estructurado, ambicioso y orientado a los resultados. Sus actividades las llevan a cabo grupos de trabajo (GT) que se reúnen periódicamente y se centran en cuestiones comunes clave:

- GT1 - Normas comunes, análisis comparativo y madurez
- GT2 - Métodos y herramienta de plataforma compartida y contratos
- GT3 - Seguridad en la nube
- GT4 - Desarrollo del talento en capacidades cibernéticas
- GT5 - Concienciación en materia cibernética
- GT6 - Seguridad de las videoconferencias

De acuerdo con el mandato del CSSG, su secretaría es responsable de supervisar e informar regularmente sobre el progreso de las actividades de los grupos de trabajo.

Presenta informes periódicos al presidente y al vicepresidente del subgrupo de ciberseguridad del ICDT, recabando periódicamente las aportaciones de los coordinadores de los grupos de trabajo. Al final de cada año, el CSSG también debe presentar un informe de actividades resumido.

La Comisión preside actualmente el ICDT CSSG, con un representante del ICTAC como vicepresidente. Aunque el CSSG carece de poder de decisión, puede recomendar decisiones sobre cuestiones pertinentes al ICDT.

Red de Agencias

La Red de Agencias de la UE (EUAN) es una red informal creada por los responsables de agencias de la UE en 2012. La EUAN comprende actualmente 48 empresas comunes y agencias descentralizadas de la UE. Su objetivo es proporcionar una plataforma de intercambio y cooperación para los miembros de la Red en ámbitos de interés común. El Comité Consultivo sobre las TIC (ICTAC) es el subgrupo de la EUAN encargado de promover la cooperación en el ámbito de las TIC, en particular la ciberseguridad.

Comité consultivo sobre las tecnologías de la información y de las comunicaciones (ICTAC)

La ICTAC promueve la cooperación entre las agencias y las empresas conjuntas en el ámbito de las TIC. Su objetivo es encontrar soluciones viables y económicas a problemas comunes, intercambiar información y adoptar posiciones comunes, cuando proceda. Según el mandato del ICTAC, las reuniones generales que reúnen a todos sus miembros se celebran dos veces al año. También se celebran reuniones mensuales periódicas entre los representantes del ICTAC en los grupos de trabajo de la CSSG, el representante de la ICTAC en el CSSG y la «troika» del ICTAC. La Troika está integrada por los presidentes actuales, anteriores y futuros del ICTAC (cada presidente presta servicio durante un periodo de un año). La función de la Troika es apoyar al actual presidente en todos los asuntos relacionados con su función, incluida su sustitución, si las circunstancias así lo requieren.

Siglas y acrónimos

ACI: Acuerdo interinstitucional

ANS: Acuerdo de nivel de servicio

APT: Amenaza persistente avanzada

CERT-UE: Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea

CISO: Chief Information Security Officer

CSA: Cybersecurity Act

CSIRT: Equipo de respuesta a incidentes de seguridad informática

DG Informática: Dirección General de Informática

DG Recursos Humanos y Seguridad: Dirección General de Recursos Humanos y Seguridad

ENISA: Agencia de la Unión Europea para la Ciberseguridad

ETC: Equivalente en tiempo completo

EUAN: Red de Agencias de la Unión Europea

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

ICDT CSSG: Subgrupo de ciberseguridad del Comité interinstitucional para la transformación digital

ICDT: Comité interinstitucional para la transformación digital

ICTAC: Comité consultivo sobre las tecnologías de la información y de las comunicaciones

IOUE: Instituciones, órganos y organismos de la Unión Europea

ISACA: Asociación de Auditoría y Control de Sistemas de Información

ITCB: Consejo de Tecnologías de la Información y Ciberseguridad

MoU: Memorandum of Understanding

SIC: Sistemas de información y comunicaciones

SRI: Seguridad de las redes y de la información

TIC: Tecnologías de la información y de las comunicaciones

Glosario

Amenaza persistente avanzada: Ataque en el que un usuario no autorizado accede a un sistema o red con el fin de robar datos sensibles y permanece allí durante un periodo prolongado.

Ciberespacio: Entorno global en línea en el que las personas, el *software* y los servicios se comunican a través de redes de ordenadores y otros dispositivos conectados.

Ciberespionaje: El acto o la práctica de obtener secretos e información de Internet, redes u ordenadores particulares sin permiso y conocimiento del titular de la información.

Ciberseguridad: Medidas para proteger las redes e infraestructuras informáticas y la información que estas contienen frente a las amenazas externas.

Ejercicio de equipo rojo: Simulación realista de ciberataques utilizando el elemento de sorpresa y técnicas observadas recientemente en el mundo real, centrándose en objetivos específicos a través de múltiples líneas de ataque.

Equipo de respuesta a emergencias informáticas de las IOUE: Centro de intercambio de información y coordinación de la respuesta a incidentes cuyos clientes («Partes») son las instituciones, órganos y organismos de la UE.

Ingeniería social: En seguridad de la información, la manipulación psicológica para engañar a las personas con el fin de que hagan algo o compartan información confidencial.

***Phishing*:** Envío de mensajes de correo electrónico que simulan proceder de una fuente de confianza para engañar a los destinatarios con el fin de que abran vínculos maliciosos o compartan datos personales.

Prueba de penetración: Método para evaluar la seguridad de un sistema informático intentando violar sus salvaguardias de seguridad con las herramientas y técnicas utilizadas habitualmente por los atacantes.

Respuestas de la Comisión

https://www.eca.europa.eu/es/Pages/DocItem.aspx?did=60922

Respuestas del CERT-UE y la ENISA

https://www.eca.europa.eu/es/Pages/DocItem.aspx?did=60922

Plazo

https://www.eca.europa.eu/es/Pages/DocItem.aspx?did=60922

DERECHOS DE AUTOR

PDF	ISBN 978-92-847-7586-6	1977-5687	doi:10.2865/281106	QJ-AB-22-003-ES-N
HTML	ISBN 978-92-847-7578-1	1977-5687	doi:10.2865/40292	QJ-AB-22-003-ES-Q

El número de ciberataques en instituciones, órganos y organismos de la UE (IOUE) está aumentando considerablemente. Dado que las IOUE están estrechamente interconectadas, los puntos débiles de una IOUE pueden exponer a las demás a amenazas de seguridad. Hemos examinado si las IOUE disponen de mecanismos adecuados para protegerse contra las ciberamenazas. Hemos constatado que, en general, el nivel de preparación no es proporcional a las amenazas, y que su grado de madurez con respecto a la ciberseguridad es muy variable. Recomendamos que la Comisión mejore la preparación de las IOUE proponiendo la introducción de normas comunes vinculantes sobre ciberseguridad y un incremento de los recursos del Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE). La Comisión también debería promover una mayor sinergia ente las IOUE, y el CERT-UE y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) debería concentrar su apoyo en las IOUE con menor madurez.

Informe Especial del Tribunal de Cuentas Europeo con arreglo al artículo 287, apartado 4, segundo párrafo, 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/Pages/ContactForm.aspx
Sitio web: eca.europa.eu
Twitter: @EUAuditors