



Respuestas del presidente del Comité de Dirección del CERT-UE, el CERT-UE y la ENISA al informe especial del Tribunal de Cuentas Europeo sobre la ciberseguridad de las instituciones, organismos y agencias de la UE.

1. Resumen ejecutivo

A la luz de la permanente evolución que se constata en el panorama de las ciberamenazas, la ciberseguridad ha adquirido la mayor y más crítica importancia para las Instituciones, Organismos y Agencias de la Unión Europea (EUIBA), que durante los últimos años han sido objeto de ciberataques cada vez más sofisticados. En el marco de sus respectivos mandatos, tanto ENISA como el CERT-UE pueden proporcionar un valioso apoyo a las EUIBA en materia de ciberseguridad a diferentes niveles. La propuesta de Reglamento de la Comisión Europea relativo a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, organismos y agencias de la UE constituye un instrumento esencial en este contexto, un instrumento que cuenta con un firme apoyo desde ENISA, el CERT-UE y el presidente del Comité de Dirección del CERT-UE.

Con este fin, ENISA, el CERT-UE y el presidente del Comité de Dirección del CERT-UE acogen con agrado el informe especial del Tribunal de Cuentas Europeo sobre la ciberseguridad de las instituciones, organismos y agencias de la UE, que llega en un momento muy oportuno para abordar los niveles de capacidad de respuesta de las EUIBA en su conjunto. El informe señala claramente el papel central que corresponde a ENISA y al CERT-UE en este ámbito. También subraya la necesidad de destinar recursos adicionales y adoptar acciones concretas específicamente orientadas a mejorar la situación de las EUIBA en materia de ciberseguridad.

Entendido esto, ENISA, el CERT-UE y el presidente del Comité de Dirección del CERT-UE expresan su apoyo a las principales observaciones y recomendaciones del informe, que se encuentran en consonancia con las propuestas legislativas de la Comisión Europea en los ámbitos de la ciberseguridad y de la seguridad de la información para las EUIBA.

Los comentarios que figuran en la siguiente sección tienen como objetivo proporcionar algunas aclaraciones adicionales a determinados ámbitos del informe, en concreto a lo referido al trabajo pertinente ya realizados por ENISA y por el CERT-UE, así como las acciones que tienen previsto emprender ENISA y el CERT-UE, especialmente en el ámbito del



desarrollo de capacidades para las EUIBA. En relación con las recomendaciones, ENISA y CERT-UE aceptan la Recomendación 3 (Incrementar el grado de atención prestado por el CERT-UE y ENISA a las EUIBA menos maduras), específicamente dirigida a estas dos entidades.

2. Observaciones principales

ENISA y el CERT-UE apoyan las principales observaciones formuladas por el Tribunal de Cuentas. Dicho esto, a continuación se facilitan algunas aclaraciones adicionales, especialmente en relación a las acciones en vigor llevadas a cabo por ENISA y por el CERT-UE, así como los planes ya establecidos para futuras actividades.

Apartado 49

En relación con la solicitud formal enviada por la ICTAC al presidente del Comité de Dirección del CERT-UE en relación con los derechos de voto en el seno del comité, queremos aclarar lo siguiente:

Dados los considerables costes indirectos que la revisión de la IIA actual habría supuesto, y dado que en los trabajos en curso relacionados con el «Reglamento relativo a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, organismos y agencias de la Unión» ya se había abordado la representación de las agencias descentralizadas, se acordó resolver formalmente el asunto, en una perspectiva a largo plazo, mediante la regulación. Hasta entonces, tal como confirmó el presidente, las prácticas actuales se mantendrán y se seguirá animando a los representantes de ICTAC a que den a conocer sus puntos de vista y que estos sean tenidos en cuenta, en la medida de lo posible y con toda equidad.

Apartado 66

A finales de 2021, ENISA instauró un plan de acción para los ciberejercicios, que incluyen específicamente a las EUIBA. En el primer trimestre de 2022 se establecerá un plan de acción pertinente para las formaciones impartidas a las EUIBA.

Casilla 3

Aunque no se mencionasen explícitamente como resultados operativos, ENISA ha estado facilitando apoyo operativo y de cooperación a diversas EUIBA en base a sus solicitudes. Por



ejemplo, en 2018, en virtud del Objetivo 2.2. Apoyo a la implementación de la política de la Unión Europea:

- El Banco Central Europeo solicitó apoyo para el desarrollo del sistema de pruebas "red team" de EUROSystem
- La Agencia de Seguridad Aérea de la Unión Europea solicitó apoyo para desarrollar los objetivos del Centro Europeo de Ciberseguridad en la aviación, incrementar la concienciación en materia de ciberseguridad y para la aplicación sectorial de la Directiva NIS.
- La Agencia Ferroviaria de la Unión Europea solicitó apoyo en la aplicación de la Directiva NIS al sector ferroviario, en particular, apoyo en el desarrollo de un centro de intercambio y análisis de información sectorial (ISAC) para los gestores de infraestructuras y las empresas ferroviarias, así como capacitación (organización de sesiones de formación y concienciación).
- La ENISA apoyó a la 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) en sus esfuerzos por potenciar su capacidad en el ámbito de la ciberseguridad y la continuidad de sus operaciones. En particular, la ENISA facilitó su experiencia en la organización de ejercicios y el desarrollo de escenarios, así como el suministro del entorno completo ENISA-CEP (Cyber Exercise Platform) de la a eu-LISA con el objetivo de organizar un ejercicio de capacidad de respuesta para uno de los sistemas informáticos vitales de la Unión Europea.

Además de esto, ENISA, desde 2019, se ha implicado activamente con las EUIBA (por ejemplo, AFE, AESM, EASA, ACER) en apoyo de la Directiva NIS, en relación con la creación de conocimientos específicos del sector y actividades de concienciación en materia de ciberseguridad, así como en iniciativas sectoriales relacionadas con políticas de ciberseguridad.

Apartado 71

ENISA desarrolló en 2021 y publicará en 2022 una formación especializada sobre «Cómo crear un programa de concienciación y utilizar ejercicios teóricos de simulación» orientada



específicamente a las EUIBA. En el contexto de su cooperación estructurada, ENISA y el CERT-UE también facilitarán formaciones conjuntas a las EUIBA en 2022.

Apartado 72

Debe tenerse en cuenta que los ejercicios de ciberseguridad de la ENISA son muy ambiciosos y cuentan con un vasto público destinatario, incluidas también las EUIBA. Este enfoque se corresponde también a abordar a las necesidades de las EUIBA, ya que para ellas los ejercicios con los representantes de los Estados miembros pueden reportar grandes beneficios. Conviene observar que ENISA ha venido implicando desde 2016 al personal técnico de las EUIBA en los Ejercicios Cyber Europe, bajo la dirección del CERT-UE, que es el organismo encargado de planificar esta circunscripción. Como continuación de estos esfuerzos, ENISA planea en su Estrategia para el Ejercicio 2022, al amparo de las actividades de desarrollo de capacidades, la promoción de un nuevo producto que se facilitará con el apoyo del CERT-UE, y que facilitará oportunidades a las EUIBA para obtener formación en Ejercicios de Autoevaluación.

3. Conclusiones y recomendaciones

ENISA y CERT-UE aceptan la Recomendación 3 (Incrementar el grado de atención prestado por el CERT-UE y la ENISA a las EUIBA menos maduras), específicamente dirigida a estas dos entidades.