

**Bruselas, 21 de junio de 2022
(OR. en)**

10504/22

**CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689**

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	21 de junio de 2022
A:	Delegaciones
N.º doc. prec.:	9716/22
Asunto:	Conclusiones del Consejo sobre el Informe Especial 05/2022 del Tribunal de Cuentas Europeo titulado «Ciberseguridad de las instituciones, órganos y organismos de la UE: En general, el nivel de preparación no es proporcional a las amenazas» - El Consejo adopta sus Conclusiones en su sesión del 21 de junio de 2022

Adjunto se remite a las delegaciones las Conclusiones del Consejo de referencia, adoptadas por el Consejo en su sesión del 21 de junio de 2022.

CONCLUSIONES DEL CONSEJO**sobre el Informe Especial 05/2022 del Tribunal de Cuentas Europeo
titulado**

«Ciberseguridad de las instituciones, órganos y organismos de la UE: En general, el nivel de preparación no es proporcional a las amenazas»

EL CONSEJO DE LA UNIÓN EUROPEA,

RECORDANDO sus Conclusiones encaminadas a mejorar el estudio de los informes especiales elaborados por el Tribunal de Cuentas en el marco de la aprobación de la gestión presupuestaria¹;

1. TOMA NOTA del Informe Especial 05/2022 del Tribunal de Cuentas Europeo titulado «Ciberseguridad de las instituciones, órganos y organismos de la UE: En general, el nivel de preparación no es proporcional a las amenazas»².
2. SUBRAYA la importancia y la urgencia de reforzar el nivel de ciberseguridad en las instituciones, órganos y organismos de la UE, habida cuenta de la reciente aceleración de la transformación digital dentro de las instituciones, la información sensible que estas procesan, el aumento en número y gravedad de los ataques contra las instituciones, órganos y organismos de la Unión, y el nivel de amenaza que les afecta.
3. RECUERDA las Conclusiones del Consejo Europeo de 20 de junio de 2019³, en las que este invitaba a las instituciones de la UE, junto con los Estados miembros, a elaborar medidas destinadas a reforzar la resiliencia, a mejorar la cultura de seguridad de la UE frente a las amenazas híbridas y las ciberamenazas procedentes de fuera de la UE y a proteger mejor de todo tipo de actividades malintencionadas las redes de información y comunicación de la UE y los procesos decisorios de esta.

¹ 7515/00 + COR 1.

² 8040/22.

³ EUCO 9/19.

4. RECUERDA sus Conclusiones de 10 de diciembre de 2019 sobre las acciones complementarias para aumentar la resiliencia y luchar contra las amenazas híbridas⁴, en las que instaba a las instituciones, órganos y organismos de la UE a que, con el apoyo de los Estados miembros, garantizaran la capacidad de la Unión para proteger su integridad y mejorar la seguridad de las redes de información y comunicación y de los procesos decisorios de la UE frente a actividades malintencionadas de todo tipo, sobre la base de una evaluación exhaustiva de las amenazas. En las Conclusiones se afirmaba que, a tal fin, las instituciones, órganos y organismos, con el apoyo de los Estados miembros, deben desarrollar y aplicar un conjunto completo de medidas para garantizar su seguridad, de conformidad con el mandato del Consejo Europeo de junio de 2019⁵.
5. RECUERDA sus Conclusiones de 22 de marzo de 2021 sobre la Estrategia de Ciberseguridad de la UE para la Década Digital⁶, en las que destacaba que la ciberseguridad es vital para el funcionamiento de la administración y las instituciones públicas, tanto a escala nacional como de la UE, así como para nuestra sociedad y la economía en su conjunto.
6. RECUERDA sus Conclusiones de 23 de mayo de 2022 sobre la elaboración de la posición de la Unión Europea en materia cibernética⁷, en las que se animaba a las instituciones, órganos y organismos de la UE a participar en la elaboración de un inventario de las herramientas existentes para una comunicación segura en el ámbito cibernético, que se habría de debatir en los órganos pertinentes del Consejo y los grupos de cooperación pertinentes, como la red de CSIRT y la red CyCLONe.
7. SUBRAYA la necesidad de abordar el riesgo sistémico que entraña la interconexión entre las instituciones, órganos y organismos de la UE, así como entre estos y las instituciones de los Estados miembros, pese a su independencia institucional y su autonomía administrativa.

⁴ 14972/19.
⁵ EUCO 9/19.
⁶ 6722/21.
⁷ 9364/22.

8. TOMA NOTA de las observaciones del Informe Especial, a saber, que las instituciones, órganos y organismos de la UE no han alcanzado un nivel de preparación en materia cibernética a la altura de las amenazas y tienen distintos niveles de madurez en ciberseguridad. RECONOCE que debe mejorarse el nivel de preparación en materia de ciberseguridad de las instituciones, órganos y organismos de la UE, así como las sinergias entre ellos.
9. Por tanto, ANIMA encarecidamente a las instituciones, órganos y organismos de la UE a que sigan aplicando medidas de gestión de riesgos cibernéticos que garanticen un nivel adecuado de ciberseguridad, tal como se prevé en la propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148, con el fin de mejorar su nivel de preparación.
10. INVITA a las instituciones, órganos y organismos de la UE a que redoblen sus esfuerzos para protegerse de las ciberamenazas y aumenten su cooperación para el establecimiento de normas y especificaciones coherentes, en particular sobre la contratación pública, los proyectos y los servicios relacionados con la ciberseguridad, y a que mejoren la interoperabilidad de sus sistemas informáticos, también con vistas a garantizar la comunicación segura de contenidos no clasificados.
11. INVITA a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y al equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-UE) a que, en el marco de sus competencias, intensifiquen su cooperación a la hora de apoyar a las instituciones, órganos y organismos de la UE en sus iniciativas de ciberseguridad, en particular en lo que respecta al desarrollo de capacidades para aquellas instituciones, órganos y organismos de la UE que muestren un menor nivel de madurez en materia de ciberseguridad.
12. TOMA NOTA de las conclusiones y recomendaciones del Informe Especial, y RECONOCE que debe mejorarse sustancialmente el nivel de preparación en materia de ciberseguridad de las instituciones, órganos y organismos de la UE, así como las sinergias entre ellos. Las instituciones, órganos y organismos de la UE deben contar con un marco global de gestión de riesgos de ciberseguridad, llevar a cabo evaluaciones de riesgos y auditorías periódicas, basadas en una metodología común o conocida y en normas internacionales, y sistematizar la organización de programas de sensibilización y formación en materia de ciberseguridad para el personal.

13. HACE HINCAPIÉ asimismo en que las instituciones, órganos y organismos de la UE deben asignar un presupuesto suficiente que garantice la aplicación de las medidas de protección frente a las ciberamenazas, respetando al mismo tiempo el marco financiero plurianual, y TOMA NOTA de la recomendación del Informe Especial de que debe designarse a una entidad que, en representación de todas las instituciones, órganos y organismos de la UE, disponga del mandato y los recursos apropiados para supervisar el cumplimiento de las normas comunes sobre ciberseguridad.
 14. RECONOCE que el CERT-UE debe ser informado sin demora de los incidentes cibernéticos significativos que ocurran en las instituciones, órganos y organismos de la UE y, a tal fin, debe estar dotado de recursos adecuados, previsibles y adaptados al nivel actual de amenaza y a las necesidades de las instituciones, órganos y organismos de la UE, en particular por lo que respecta al personal, los equipos técnicos y la infraestructura.
 15. OBSERVA que debe reforzarse y sistematizarse la cooperación y el intercambio de información sobre ciberseguridad, así como la interoperabilidad de los canales de comunicación seguros entre las instituciones, órganos y organismos de la Unión. ABOGA por que dicha cooperación e intercambio de información incluya también a las autoridades públicas encargadas de la ciberseguridad en los Estados miembros.
 16. TOMA NOTA de las respuestas de la Comisión, el CERT-UE y la ENISA que acompañan al Informe Especial.
 17. INVITA a la Comisión a que tenga en cuenta las recomendaciones del Informe Especial y muestre ambición en la elaboración de las políticas de ciberseguridad de las instituciones, órganos y organismos de la UE, y a que propugne el establecimiento de mayores sinergias entre ellos.
-