Consejo de la Unión Europea

Bruselas, 22 de marzo de 2022
(OR. en)

7474/22
ADD 3

Expediente interinstitucional: 2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	22 de marzo de 2022
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	SWD(2022) 68 final
Asunto:	DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN RESUMEN DE LA EVALUACIÓN DE IMPACTO que acompaña al documento Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión

Adjunto se remite a las Delegaciones el documento – SWD(2022) 68 final.

Adj.: SWD(2022) 68 final

COMISIÓN
EUROPEA

Bruselas, 22.3.2022
SWD(2022) 68 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DE LA EVALUACIÓN DE IMPACTO

que acompaña al documento

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Introducción

En 2020 se produjo un incremento del número de incidentes importantes, orquestados por agentes de riesgo de amenazas persistentes avanzadas (APT), que afectaron a las instituciones, los órganos y los organismos de la Unión. Esta situación se refleja igualmente en el número de imágenes forenses analizadas por el CERT-UE en 2020, que triplicó la cifra de 2019, mientras que el número de incidentes importantes se multiplicó por más de diez desde 2018.

Sin embargo, las instituciones, los órganos y los organismos de la Unión presentan en algunos casos unos niveles de capacidades de ciberseguridad y de gasto en seguridad informática llamativamente desiguales, lo que da lugar a grandes divergencias en cuanto al grado de madurez de la ciberseguridad. Por otra parte, el análisis del panorama de las amenazas y las estadísticas de incidentes de seguridad informática muestran que la exposición cibernética de las instituciones, los órganos y los organismos de la Unión no hará sino aumentar.

2. Objetivos

Las deficiencias detectadas llevan, en última instancia, a un nivel insuficiente de ciberresiliencia en las instituciones, los órganos y los organismos de la Unión, a la fragmentación de los recursos destinados a la seguridad informática y al desequilibrio entre las posturas adoptadas respecto de la seguridad informática.

El objetivo del instrumento jurídico sería disponer medidas que garanticen un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión. Gracias a ello, se promovería y aseguraría que la madurez de la ciberseguridad vaya a la par de la digitalización galopante de las instituciones, los órganos y los organismos de la Unión.

3. Consejo Interinstitucional de Ciberseguridad y marco de ciberseguridad

La propuesta de un Consejo Interinstitucional de Ciberseguridad y un marco de ciberseguridad permitirá, por una parte, introducir medidas que garanticen un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión, facilitando así la armonización en torno a un marco que aborde las amenazas de ciberseguridad del conjunto de las instituciones, los órganos y los organismos de la Unión, y, por otra parte, establecer tanto una actividad de seguimiento como la comunicación de información a dicho Consejo Interinstitucional de Ciberseguridad.

La propuesta moderniza la misión y las funciones del CERT-UE teniendo en cuenta la digitalización de las instituciones, los órganos y los organismos de la Unión, que ha experimentado cambios y se ha intensificado en los últimos años, así como el panorama, en constante evolución, de las amenazas de ciberseguridad.

No hay repercusiones directas ni consecuencias presupuestarias para los Estados miembros ni para los ciudadanos de la UE.

La base jurídica del Reglamento es el artículo 298 del Tratado de Funcionamiento de la Unión Europea, en el que se prevé que, en el cumplimiento de sus funciones, las instituciones, los órganos y los organismos de la Unión se apoyen en una administración europea abierta, eficaz e independiente.

La presente propuesta se basa en la Estrategia de la UE para una Unión de la Seguridad [COM(2020) 605 final] y en la Estrategia de Ciberseguridad de la UE para la Década Digital [JOIN(2020) 18 final].

4. Conclusión

El Consejo Interinstitucional de Ciberseguridad y el marco de ciberseguridad permiten lograr la mayoría de los objetivos perseguidos de una manera relativamente eficaz, eficiente y coherente con otras políticas de la Unión, con el máximo apoyo de las partes interesadas. La solución seleccionada es la más viable, habida cuenta de los límites jurídicos imperantes a los que estamos sujetos y de que un enfoque único para todos los casos no permitiría responder debidamente a la actual situación de las instituciones, los órganos y los organismos de la Unión, que presentan distintos grados de madurez y se enfrentan a diferentes riesgos y complejidades desde el punto de vista tecnológico.