Consejo de la Unión Europea

Bruselas, 29 de marzo de 2022
(OR. en)

7670/22
ADD 7

Expediente interinstitucional: 2022/0084(COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

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) 65 final
Asunto:	DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN RESUMEN DEL INFORME DEL ANÁLISIS DE IMPACTO que acompaña al documento Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la seguridad de la información en las instituciones, órganos y organismos de la Unión

Adjunto se remite a las Delegaciones el documento – SWD(2022) 65 final.

Adj.: SWD(2022) 65 final

COMISIÓN
EUROPEA

Bruselas, 22.3.2022
SWD(2022) 65 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DEL INFORME DEL ANÁLISIS DE IMPACTO

que acompaña al documento

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la seguridad de la información en las instituciones, órganos y organismos de la Unión

{COM(2022) 119 final} - {SWD(2022) 66 final}

Ficha resumen

Análisis de impacto sobre la seguridad de la información en las instituciones, órganos y organismos de la Unión

A. Contexto político

La Agenda Estratégica del Consejo Europeo para 2019-2024 insta a las instituciones a proteger las redes de información y comunicación de la UE y sus procesos de toma de decisiones frente a actividades malintencionadas de todo tipo, incluidas las amenazas cibernéticas e híbridas. En consecuencia, el Consejo de Asuntos Generales de diciembre de 2019 concluyó que las instituciones y órganos de la UE debían desarrollar y aplicar un conjunto completo de medidas para garantizar la seguridad de su información.

En julio de 2020, la Comisión adoptó su Estrategia de la UE para una Unión de la Seguridad, en virtud de la cual se comprometió a complementar los esfuerzos nacionales en el ámbito de la seguridad. Como parte de esta estrategia, la Comisión propuso crear un conjunto mínimo de normas sobre seguridad de la información y ciberseguridad en todas las instituciones y órganos de la Unión.

B. Definición del problema

Los principales problemas son los siguientes: i) la diferencia significativa entre el nivel de seguridad de las instituciones y órganos de la Unión en función de sus normas internas de seguridad de la información; ii) la falta de coordinación entre las instituciones y órganos de la Unión en el desempeño de sus tareas de seguridad.

Las instituciones y órganos de la Unión tienen actualmente sus propias normas de seguridad de la información o no las han adoptado en absoluto. La fragmentación del marco jurídico aplicable dio lugar a diferentes categorías de información no clasificada, marcas e instrucciones de tratamiento diferentes en todos los ámbitos. En lo que respecta a la información clasificada de la UE, la interoperabilidad de los sistemas pertinentes sigue siendo limitada, lo que impide una transferencia fluida de información entre instituciones y órganos y con los Estados miembros.

Esta situación aumenta el riesgo de que haya atacantes que puedan violar la seguridad en el eslabón más débil y lo utilicen como punto de partida para nuevos ataques contra otras instituciones u órganos.

C. Objetivos

El objetivo general de la iniciativa es crear normas de seguridad de la información para todas las instituciones y órganos de la Unión con el fin de garantizar una protección reforzada y coherente contra las cambiantes amenazas a su información.

El objetivo general se traduce en cuatro objetivos específicos:

- Establecer categorías armonizadas y exhaustivas de información
- Identificar lagunas en materia de seguridad y aplicar las medidas necesarias
- Establecer una cooperación fluida en materia de seguridad de la información entre las instituciones y órganos de la Unión
- Modernizar las políticas de seguridad de la información, teniendo en cuenta la transformación

digital y el teletrabajo

D. Opiniones de las distintas partes interesadas

Las partes interesadas consultadas (instituciones y órganos de la Unión, autoridades nacionales de seguridad de los Estados miembros y expertos en investigación del CCI) coincidieron en la necesidad de unas normas comunes de seguridad de la información para todas las instituciones y órganos de la Unión, centrándose en los siguientes puntos:

- Deben tenerse en cuenta la diversidad y el diferente entorno de gestión de cada institución y órgano de la Unión y deben permitirse soluciones locales
- Aunque la mayoría de las instituciones y órganos están dispuestos a cooperar con sus homólogos en el seno de órganos comunes a efectos de la seguridad de la información, no están dispuestos a delegar sus poderes de toma de decisiones
- El proyecto de Reglamento debe elaborarse respetando el Acuerdo intergubernamental[1] de los Estados miembros sobre la protección de la información clasificada

E. Impacto de la propuesta

Beneficios

Al crear una base de referencia para las normas de seguridad de la información en todas las instituciones y órganos de la Unión, el proyecto de Reglamento aumentará los niveles generales de seguridad de la información, reduciendo al mismo tiempo las discrepancias actuales. También debería contribuir a eliminar los posibles eslabones débiles, protegiendo al mismo tiempo la información compartida en el seno de la Administración europea.

Desde el punto de vista de la eficiencia, el proyecto de Reglamento debería mejorar el desempeño coordinado de las tareas comunes de seguridad de la información (por ejemplo, habilitaciones, acreditación de sistemas de comunicación e información) y a la creación de órganos de gobernanza comunes (por ejemplo, el Grupo de Coordinación Interinstitucional o los subgrupos técnicos).

Repercusiones económicas

En el caso de las instituciones y órganos de la Unión, se espera que los esfuerzos necesarios para aplicar la nueva legislación se vean compensados por el aumento de la eficiencia, mientras que los costes adicionales pueden cubrirse con los actuales programas de mejora de la seguridad de la información de cada organización. A largo plazo, se beneficiarán de un enfoque coherente a la hora de hacer frente a la constante evolución de las amenazas a la seguridad de la información.

La Comisión Europea se encargaría de la secretaría permanente del Grupo de Coordinación Interinstitucional y asignaría recursos humanos para esta tarea (un funcionario AD y un funcionario AST).

No se esperan repercusiones económicas en las Administraciones de los Estados miembros ni en el sector privado.

[1] Acuerdo entre los Estados miembros de la Unión Europea, reunidos en el seno del Consejo, sobre la protección de la información clasificada intercambiada en interés de la Unión Europea (2011/C202/05).

F. Seguimiento
Futura revisión de la política
Se llevará a cabo una evaluación completa cada cinco años desde la fecha de aplicación con el fin de evaluar el impacto y la aplicación del proyecto de Reglamento. La Comisión presentará al Parlamento Europeo y al Consejo un informe con sus conclusiones.