Consejo de la Unión Europea

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

7474/22
ADD 1

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

PROPUESTA

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.:	COM(2022) 122 final - Annexes
Asunto:	ANEXOS de la 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 – COM(2022) 122 final - Annexes.

Adj.: COM(2022) 122 final - Annexes

COMISIÓN
EUROPEA

Bruselas, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANEXOS

de la

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ANEXO I

El código básico de ciberseguridad cubrirá los ámbitos siguientes:

1) política de ciberseguridad, incluidos los objetivos y las prioridades en relación con la seguridad de las redes y los sistemas de información, en particular por lo que respecta al uso de servicios de computación en la nube [en el sentido del artículo 4, apartado 19, de la Directiva (propuesta SRI 2)] y las disposiciones técnicas para facilitar el teletrabajo;

2) organización de la ciberseguridad, incluida la determinación de funciones y responsabilidades;

3) gestión de activos, incluidos un inventario de los activos informáticos y un trazado de la red informática;

4) control de acceso;

5) seguridad de las operaciones;

6) seguridad de las comunicaciones;

7) adquisición, desarrollo y mantenimiento de sistemas;

8) relaciones con los proveedores;

9) gestión de incidentes, incluidas estrategias tales como el seguimiento de la seguridad y el registro secuencial para mejorar la preparación, la respuesta y la recuperación en caso de incidente y la cooperación con el CERT-UE;

10) gestión de la continuidad de las actividades y gestión de crisis; y

11) programas de educación, sensibilización y formación en materia de ciberseguridad.

ANEXO II

Las instituciones, los órganos y los organismos de la Unión integrarán en sus códigos básicos de ciberseguridad y planes de ciberseguridad, como mínimo, las medidas específicas de ciberseguridad que se indican a continuación, habida cuenta de los documentos de orientación y las recomendaciones del CIIC:

1) acciones concretas para avanzar hacia una arquitectura de confianza cero (esto es, un modelo de seguridad, un conjunto de principios de diseño de sistemas y una estrategia coordinada de ciberseguridad y gestión de sistemas basados en el reconocimiento de la existencia de amenazas tanto dentro como fuera de los límites tradicionales de las redes);

2) adopción de la autenticación multifactor como norma en la totalidad de las redes y los sistemas de información;

3) garantía de la seguridad de la cadena de suministro de *software* mediante criterios para el desarrollo seguro de *software* y la evaluación;

4) introducción de mejoras en las normas de contratación pública con miras a garantizar un elevado nivel común de ciberseguridad a través de:

   a) eliminación de los obstáculos contractuales que limitan la comunicación de información al CERT-UE, por parte de los proveedores de servicios informáticos, acerca de incidentes, vulnerabilidades y ciberamenazas;

   b) obligación contractual de informar de los incidentes, las vulnerabilidades y las ciberamenazas, así como de disponer de capacidades adecuadas de respuesta a incidentes y seguimiento de incidentes.