Consejo de la Unión Europea

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

7474/22

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
Asunto:	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.

Adj.: COM(2022) 122 final

COMISIÓN
EUROPEA

Bruselas, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

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}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La presente propuesta establece un marco para garantizar que las instituciones, los órganos y los organismos de la Unión apliquen normas y medidas comunes de ciberseguridad. El objetivo es mejorar la resiliencia y la capacidad de respuesta de todas las entidades en caso de producirse un incidente. La propuesta está en consonancia con las prioridades de la Comisión de adaptar Europa a la era digital y forjar una economía con visión de futuro al servicio de las personas. Además, velar por que la administración pública sea segura y resiliente es una piedra angular de la transformación digital de la sociedad en su conjunto.

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].

La propuesta moderniza el actual marco jurídico del CERT-UE y tiene en cuenta la digitalización de las instituciones, los órganos y los organismos, que ha experimentado cambios y se ha intensificado en los últimos años, así como el panorama, en constante evolución, de las amenazas de ciberseguridad. Ambos fenómenos se han visto amplificados desde el inicio de la crisis de la COVID-19, y el número de incidentes no ha hecho sino aumentar, con ataques cada vez más sofisticados de muy diversas procedencias.

Se propone modificar la denominación del CERT-UE, que pasaría de «Equipo de respuesta a emergencias informáticas» a «Centro de Ciberseguridad» para las instituciones, los órganos y los organismos de la Unión, en sintonía con los cambios observados en los Estados miembros y en otras partes del mundo, donde muchos CERT han pasado a denominarse «Centros de Ciberseguridad»; sin embargo, por ser ya reconocible, se conservaría el nombre abreviado «CERT-UE».

• Coherencia con las disposiciones existentes en la misma política sectorial

La presente propuesta tiene por objeto reforzar, desde el punto de vista de la ciberseguridad, la resiliencia de las instituciones, los órganos y los organismos de la Unión frente a las ciberamenazas, procurando, al mismo tiempo, garantizar la coherencia con la legislación vigente, a saber:

- Directiva (UE) 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Se asegura asimismo la coherencia con la propuesta de Directiva (UE) XXXX/XXXX, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 [propuesta SRI 2].
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento sobre la Ciberseguridad).
- Propuesta de Reglamento (UE) XXXX/XXXX, relativo a la seguridad de la información en las instituciones, los órganos y los organismos de la Unión.
- Recomendación de la Comisión, de 23 de junio de 2021, sobre la creación de una Unidad Cibernética Conjunta.

- Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala.

El anexo de la Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala, establece el plan director de la respuesta coordinada a los incidentes y crisis de ciberseguridad transfronterizos a gran escala.

En su Resolución de 9 de marzo de 2021, el Consejo de la Unión Europea subrayó que la ciberseguridad es vital para el funcionamiento de la administración pública tanto a escala nacional como de la UE, así como para nuestra sociedad y la economía en su conjunto, y destacó tanto la importancia de un marco de seguridad sólido y coherente para proteger a todo el personal, los datos, las redes de comunicación y los sistemas de información de la UE, como la importancia de los procesos decisorios. Para lograrlo, es preciso, en particular, reforzar la resiliencia y mejorar la cultura de seguridad de las instituciones, los órganos y los organismos de la Unión. Además, deben facilitarse suficientes recursos y capacidades, también en el contexto del refuerzo del mandato del CERT-UE.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La base jurídica del presente Reglamento es el artículo 298 del Tratado de Funcionamiento de la Unión Europea («TFUE»), en el que se dispone que, en el cumplimiento de sus funciones, las instituciones, los órganos y los organismos de la Unión se apoyarán en una administración europea abierta, eficaz e independiente. Dentro del respeto al Estatuto y al régimen adoptados con arreglo al artículo 336, el Parlamento Europeo y el Consejo establecerán las disposiciones a tal efecto, mediante Reglamentos adoptados con arreglo al procedimiento legislativo ordinario.

Las tecnologías de la información han proporcionado a las instituciones, los órganos y los organismos de la Unión nuevas vías para ejercer su labor, interactuar con los ciudadanos y mejorar el conjunto de sus actividades. Ahora bien, a medida que evolucionan las tecnologías, también lo hace el panorama de las ciberamenazas. Las instituciones, los órganos y los organismos de la Unión se han convertido en blancos muy atractivos de sofisticados ciberataques. El establecimiento de sistemas y requisitos para garantizar la ciberseguridad parece estar contribuyendo a la eficiencia y la independencia de la administración europea, de tal modo que las instituciones, los órganos y los organismos de la Unión pueden operar de forma más eficiente en el mundo digital al desempeñar sus respectivas misiones.

No obstante, como se explica más adelante, en la sección 3, las actuales disparidades entre las posturas y las estrategias que adoptan las instituciones, los órganos y los organismos de la Unión en el ámbito de la ciberseguridad representan un obstáculo añadido para lograr una administración europea abierta, eficiente e independiente. Sin una estrategia común, las posturas ante la ciberseguridad de las instituciones, los órganos y los organismos de la Unión seguirán evolucionando en direcciones divergentes. Por tanto, la mencionada base jurídica es la apropiada, dado que el objetivo del Reglamento es crear un marco jurídico común para la ciberseguridad en las instituciones, los órganos y los organismos de la Unión.

• Subsidiariedad

El presente Reglamento, 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, entra dentro del ámbito de las competencias exclusivas de la Unión.

- **Proporcionalidad**

Las normas propuestas en el presente Reglamento no exceden de lo necesario para alcanzar los objetivos específicos de manera satisfactoria. Las medidas previstas contribuirán a alcanzar un elevado nivel común de ciberseguridad sin excederse de lo necesario para lograr ese objetivo en vista de los riesgos cada vez más mayores que han de afrontarse.

- **Elección del instrumento**

Se ha elegido un Reglamento, que es directamente aplicable, dado que se considera el instrumento jurídico adecuado para definir y racionalizar las obligaciones impuestas a las instituciones, los órganos y los organismos de la Unión. A fin de introducir mejoras selectivas, un Reglamento es el instrumento jurídico más apropiado.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Evaluaciones *ex ante***

El CERT-UE evaluó las principales ciberamenazas a las que están expuestas, o podrían estar expuestas en un futuro próximo, las instituciones, los órganos y los organismos de la Unión.

El análisis se basó en tres tipos de observaciones:

- intentos de vulnerar la infraestructura informática de las instituciones, los órganos y los organismos de la Unión (si tuvieron éxito, se consideraron incidentes; en caso contrario, se registraron como intentos detectados),
- amenazas detectadas en el entorno de las instituciones, los órganos y los organismos de la Unión (por ejemplo, en sus respectivos sectores, en sus comunidades de partes interesadas o en Europa),
- principales tendencias observadas a escala mundial en relación con las amenazas.

Además, en el análisis se tuvo en cuenta cómo los principales cambios que están teniendo lugar afectan al modo en que las instituciones de la Unión gestionan y usan sus infraestructuras y servicios informáticos. Entre tales cambios cabe citar:

- el incremento del teletrabajo,
- la migración de sistemas a la nube,
- la mayor externalización de servicios informáticos.

Entre 2019 y 2021, se produjo un incremento drástico del número de incidentes importantes[1], orquestados por agentes de amenazas persistentes avanzadas (APT), que afectaron a las instituciones, los órganos y los organismos de la Unión. Solo en el primer semestre de 2021 se registró un número de incidentes importantes equivalente al de todo el año 2020. Esta situación se refleja igualmente en el número de imágenes forenses (copias exactas del contenido de los sistemas o dispositivos afectados) 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.

[1] Por «incidente importante» se entiende todo incidente salvo aquel cuyas consecuencias sean limitadas y del que probablemente ya se tenga una buena comprensión en términos de método o tecnología.

En 2020, el Comité de Dirección del CERT-UE estableció un nuevo objetivo estratégico con miras a que el CERT-UE garantice, para el conjunto de las instituciones, los órganos y los organismos, un exhaustivo nivel de ciberseguridad con el alcance y la amplitud adecuadas y en continua adaptación a las amenazas, ya sean actuales o inminentes, incluidos los ataques contra los dispositivos móviles, los entornos en la nube y los dispositivos del internet de las cosas.

De manera complementaria al análisis de amenazas del CERT-UE, la Comisión evaluó el funcionamiento de la ciberseguridad en veinte instituciones, órganos y organismos de la Unión. Este ejercicio permitió obtener información sobre las prácticas de ciberseguridad establecidas y las capacidades de gestión de la ciberseguridad, con una evaluación comparativa externa de algunos controles técnicos de seguridad.

La evaluación se realizó a partir de cuestionarios a tales instituciones, órganos y organismos de la Unión, datos de dominio público y datos facilitados directamente por las entidades. La información obtenida sobre la situación actual es suficiente para extraer las conclusiones siguientes:

- La madurez de la ciberseguridad, el tamaño de la infraestructura informática y los niveles de capacidad varían considerablemente entre las instituciones, los órganos y los organismos de la Unión evaluados.
- Un buen número de instituciones, órganos y organismos de la Unión disponen, en general, de capacidades maduras de detección y respuesta, pero, en sus capacidades de gobernanza de la ciberseguridad, se observan distintos niveles de gestión integrada de riesgos.
- En general, las instituciones, los órganos y los organismos de la Unión evaluados cuentan con marcos de ciberseguridad (estrategia, política y base normativa) sólidamente establecidos en los ámbitos clave de la ciberseguridad, enumerados en el anexo I del Reglamento; sin embargo, algunas de las entidades presentan un grado deficiente de madurez respecto de la gestión de la continuidad de las actividades, el cumplimiento, la auditoría y la mejora continua.
- Las instituciones, los órganos y los organismos de la Unión evaluados no aplican por igual las medidas técnicas consideradas mejores prácticas.

En resumidas cuentas, el análisis pone de manifiesto que entre la veintena de instituciones, órganos y organismos de la Unión evaluados hay grandes diferencias desde el punto de vista de la gobernanza, la ciberhigiene, la capacidad general y la madurez. Así pues, es fundamental exigir que la totalidad de las instituciones, los órganos y los organismos de la Unión implementen un código básico de medidas de ciberseguridad para acabar con las disparidades en términos de madurez y lograr que alcancen un elevado nivel común de ciberseguridad.

Hasta la fecha, ningún instrumento legislativo de la Unión se ha centrado específicamente en la ciberseguridad de las instituciones, los órganos y los organismos de la Unión ni ha abordado de manera exhaustiva el panorama de las amenazas de ciberseguridad ni los nuevos riesgos informáticos derivados de la digitalización.

- **Consultas con las partes interesadas**

La Comisión ha consultado a las partes interesadas de las instituciones, los órganos y los organismos de la Unión, así como a los representantes de los Estados miembros en el Consejo y a las partes interesadas del Parlamento Europeo. El 25 de junio de 2021, los representantes de los Estados miembros y las partes interesadas pertinentes de las instituciones, los órganos y

los organismos de la Unión participaron en un taller organizado por la Comisión para debatir el contenido de la futura propuesta de Reglamento.

- **Evaluación de impacto**

La presente propuesta afectará a las instituciones, los órganos y los organismos de la Unión. Resulta, pues, innecesaria una evaluación de impacto específica, dado que no se aplicará a los Estados miembros.

- **Derechos fundamentales**

La Unión Europea tiene el compromiso de garantizar un elevado nivel de protección de los derechos fundamentales. Todo intercambio de información con arreglo al presente Reglamento se hará en entornos de confianza, respetando plenamente el derecho a la protección de los datos personales establecido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y la legislación pertinente en materia de protección de datos, en particular el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo.

4. REPERCUSIONES PRESUPUESTARIAS

Los índices de referencia del mercado y distintos estudios[2] señalan que el gasto directo en ciberseguridad viene oscilando entre el 4 y el 7 % del gasto informático agregado de las organizaciones. Ahora bien, el análisis de amenazas realizado por el CERT-UE, en el contexto de la presente propuesta legislativa, indica que, puesto que los organismos internacionales y las organizaciones políticas se enfrentan a mayores riesgos, sería más conveniente fijar el objetivo de destinar a la ciberseguridad el 10 % del gasto informático. Sin embargo, no es posible determinar el coste exacto de los esfuerzos requeridos debido a la ausencia de información detallada sobre el gasto informático de las instituciones, los órganos y los organismos de la Unión y la parte correspondiente al gasto en ciberseguridad.

Si bien es probable, por tanto, que gran parte de las instituciones, los órganos y los organismos de la Unión gasten menos en ciberseguridad de lo que deberían, el presente Reglamento no conllevará, como tal, un aumento de ese gasto corriente. Aun en ausencia del Reglamento, cada entidad tendría que garantizar un nivel adecuado de ciberseguridad. El Reglamento da continuidad a la cooperación previa en el Comité de Dirección del CERT-UE y formaliza un nivel de intercambio de información parcialmente existente en la actualidad. Como se detalla en la ficha financiera legislativa, el CERT-UE, cuyas funciones se amplían, necesitará recursos adicionales, que deben reasignarse de las instituciones, los órganos y los organismos de la Unión que se beneficien de sus servicios.

5. OTROS ELEMENTOS

- **Ejecución y modalidades de seguimiento, evaluación e información**

El Consejo Interinstitucional de Ciberseguridad (CIIC), asistido por el CERT-UE, debe revisar el funcionamiento del presente Reglamento, realizar evaluaciones y presentar a la Comisión un informe con sus conclusiones. Por su parte, la Comisión ha de informar

[2] Fuente: Gartner: «Identifying the Real Information Security Budget», 2016. Ha de tenerse en cuenta igualmente el gasto indirecto en seguridad informática, como en seguridad de las redes —por ejemplo, cortafuegos y antivirus— y responsabilidades de los propietarios de los sistemas —por ejemplo, evaluación de riesgos y realización de controles de seguridad—. Un artículo de 2020 sitúa el gasto en ciberseguridad de las instituciones financieras en torno al 10-11 % del gasto informático [fuente: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com)].

periódicamente al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.

El CERT-UE puede elaborar una propuesta de documento de orientación o de recomendación, que el CIIC podrá decidir adoptar. Un documento de orientación es un tipo de asesoramiento dirigido a la totalidad o a parte de las instituciones, los órganos y los organismos de la Unión, mientras que una recomendación se dirige a instituciones, órganos y organismos de la Unión específicos. Un llamamiento a la acción es un tipo de asesoramiento del CERT-UE en el que se describen medidas urgentes de seguridad que se insta a las instituciones, los órganos y los organismos de la Unión a adoptar en un plazo determinado.

- **Explicación detallada de las disposiciones específicas de la propuesta**

Disposiciones generales

El Reglamento, que establece medidas destinadas a garantizar un elevado nivel común de ciberseguridad, se aplica a las instituciones, los órganos y los organismos de la Unión con el objetivo de que puedan desempeñar sus respectivas misiones de manera abierta, eficiente e independiente. (Artículos 1 a 3 y 23 a 25).

Medidas destinadas a garantizar un elevado nivel común de ciberseguridad

Se impone a las instituciones, los órganos y los organismos de la Unión la obligación de establecer un marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad que asegure una gestión eficaz y prudente de todos los riesgos relacionados con la ciberseguridad. Además, las instituciones, los órganos y los organismos adoptarán un código básico de ciberseguridad que aborde los riesgos detectados en el citado marco, realizarán evaluaciones periódicas de madurez y adoptarán un plan de ciberseguridad. (Artículos 4 a 8).

Consejo Interinstitucional de Ciberseguridad

Se constituye el Consejo Interinstitucional de Ciberseguridad, que será responsable del seguimiento de la ejecución del presente Reglamento por parte de las instituciones, los órganos y los organismos de la Unión, así como de la supervisión de la puesta en ejecución de las prioridades y los objetivos generales por parte del CERT-UE, al que, además, proporcionará una dirección estratégica. (Artículos 9 a 11).

CERT-UE

El CERT-UE contribuirá a reforzar la seguridad del entorno informático del conjunto de las instituciones, los órganos y los organismos de la Unión ofreciéndoles asesoramiento, prestándoles ayuda para prevenir, detectar, mitigar y responder a los incidentes, y proporcionándoles una función de centro de coordinación para el intercambio de información sobre ciberseguridad y la respuesta a incidentes. (Artículos 12 a 17).

Obligaciones de cooperación e información

El Reglamento asegura la cooperación y el intercambio de información entre el CERT-UE y las instituciones, los órganos y los organismos de la Unión con el fin de crear un clima de confianza. A tales efectos, el CERT-UE podrá solicitar a las instituciones, los órganos y los organismos de la Unión que le faciliten la información pertinente e intercambiar con ellos, sin necesidad de obtener el consentimiento de la Parte afectada, información específica sobre incidentes con objeto de facilitar la detección de ciberamenazas o incidentes similares. No obstante, el CERT-UE únicamente podrá intercambiar información específica sobre

incidentes en la que se revele la identidad del objetivo del incidente de ciberseguridad con el consentimiento previo de la Parte afectada.

En particular, las instituciones, los órganos y los organismos de la Unión deberán notificar al CERT-UE las ciberamenazas, las vulnerabilidades y los incidentes importantes sin demora indebida, y en todo caso dentro de las veinticuatro horas siguientes a su constatación. (Artículos 18 a 22).

2022/0085 (COD)

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

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 298,

Visto el Tratado constitutivo de la Comunidad Europea de la Energía Atómica, y en particular su artículo 106 *bis*,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) En la era digital, las tecnologías de la información y la comunicación son una piedra angular para una administración de la Unión abierta, eficiente e independiente. La constante evolución tecnológica y la complejidad e interconexión crecientes de los sistemas digitales amplifican los riesgos relacionados con la ciberseguridad y hacen que la administración de la Unión sea más vulnerable a las ciberamenazas y los incidentes, lo que, en última instancia, supone una amenaza para la continuidad de las actividades de la administración y su capacidad para proteger sus datos. El mayor recurso a los servicios en la nube, el uso extendido de las tecnologías de la información, un alto grado de digitalización, el trabajo a distancia y unas tecnologías y posibilidades de conexión en constante evolución son, hoy en día, características fundamentales de todas las actividades de las entidades de la administración de la Unión; sin embargo, la resiliencia digital aún no se ha desarrollado lo suficiente.

(2) El panorama de las ciberamenazas a las que se enfrentan las instituciones, los órganos y los organismos de la Unión evoluciona constantemente. Las tácticas, las técnicas y los procedimientos empleados por los agentes de riesgo también están en constante evolución, pero los motivos de sus ataques varían poco: desde robar información valiosa no divulgada hasta obtener dinero, manipular la opinión pública o debilitar la infraestructura digital. Los ciberataques de estos agentes se suceden cada vez con mayor frecuencia, y sus campañas, cada vez más sofisticadas y automatizadas, se dirigen contra superficies de ataque expuestas que no dejan de expandirse y aprovechan rápidamente las vulnerabilidades.

(3) Los entornos informáticos de las instituciones, los órganos y los organismos de la Unión se caracterizan por las interdependencias, los flujos de datos integrados y la estrecha colaboración entre sus usuarios. Debido a esa interconexión, toda perturbación, aunque en un primer momento se limite a una institución, un órgano o un organismo de la Unión, puede tener un efecto en cascada más amplio y acabar perjudicando, de manera grave y duradera, al resto. Además, en algunos casos, los entornos informáticos de las instituciones, los órganos o los organismos están

conectados con los de los Estados miembros, de manera que un incidente en una entidad de la Unión puede suponer un riesgo para la ciberseguridad de los entornos informáticos de los Estados miembros y viceversa.

(4) Las instituciones, los órganos y los organismos de la Unión son blancos atractivos y, como tales, se enfrentan a agentes de riesgo altamente cualificados y dotados de amplios recursos, pero también a otro tipo de amenazas. Por otra parte, hay grandes diferencias de una entidad a otra en cuanto al grado de ciberresiliencia y su madurez, así como en cuanto a la capacidad para detectar y responder a actividades informáticas malintencionadas. Así pues, para el funcionamiento de la administración europea, es necesario que las instituciones, los órganos y los organismos de la Unión alcancen un elevado nivel común de ciberseguridad a través de un código básico de ciberseguridad (normas mínimas de ciberseguridad a las que deberán ajustarse tanto las redes y los sistemas de información como sus operadores y usuarios con el fin de minimizar los riesgos relacionados con la ciberseguridad), así como mediante el intercambio de información y la colaboración.

(5) La Directiva [propuesta SRI 2] relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad tiene por objeto reforzar la resiliencia y mejorar las capacidades de respuesta a incidentes de las entidades públicas y privadas, las autoridades y los organismos nacionales competentes y la Unión en su conjunto. Por consiguiente, es imprescindible que las instituciones, los órganos y los organismos de la Unión sigan el mismo camino aplicando normas que sean coherentes con la Directiva [propuesta SRI 2] y reflejen su nivel de ambición.

(6) A fin de alcanzar un elevado nivel común de ciberseguridad, cada institución, órgano y organismo de la Unión debe establecer un marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad que garantice una gestión eficaz y prudente de todos los riesgos relacionados con la ciberseguridad y tome en consideración la gestión de la continuidad de las actividades y de crisis.

(7) Las diferencias entre las instituciones, los órganos y los organismos de la Unión exigen flexibilidad en la ejecución, dado que no hay una solución única válida para todos los casos. Las medidas destinadas a garantizar un elevado nivel común de ciberseguridad no deben prever ninguna obligación que interfiera directamente en el desempeño de la misión o vulnere la autonomía institucional de cada institución, órgano y organismo de la Unión. Así pues, las instituciones, los órganos y los organismos deben establecer sus propios marcos para la gestión, la gobernanza y el control de riesgos en el ámbito de la ciberseguridad y adoptar sus propios códigos básicos y planes de ciberseguridad.

(8) A fin de evitar imponer una carga financiera y administrativa desproporcionada a las instituciones, los órganos y los organismos de la Unión, los requisitos de gestión de riesgos de ciberseguridad han de ser proporcionados en relación con los riesgos que presenten la red y el sistema de información en cuestión, teniendo en cuenta el estado de la técnica de las medidas. Cada institución, órgano y organismo de la Unión ha de proponerse destinar un porcentaje adecuado de su presupuesto informático a la mejora de su nivel de ciberseguridad, con el objetivo de que, a largo plazo, ese porcentaje se sitúe en el 10 %.

(9) Para lograr un elevado nivel común de ciberseguridad es preciso que la ciberseguridad sea supervisada por el más alto nivel de dirección de cada institución, órgano y organismo de la Unión, que deberá aprobar un código básico de ciberseguridad que contemple los riesgos detectados en el marco que han de establecer las distintas

entidades. Incorporar la cultura de la ciberseguridad, esto es, la práctica cotidiana de la ciberseguridad, es una parte integral de un código básico de ciberseguridad para las instituciones, los órganos y los organismos de la Unión.

(10) Las instituciones, los órganos y los organismos de la Unión deben evaluar los riesgos que se derivan de sus relaciones con los proveedores y los prestadores de servicios, en particular de servicios de almacenamiento y tratamiento de datos o de seguridad administrada, y adoptar las medidas adecuadas para encarar esos riesgos. Dichas medidas han de incorporarse al código básico de ciberseguridad y especificarse con más detalle en documentos de orientación o recomendaciones emitidos por el CERT-UE. Al establecer medidas y directrices, es preciso tomar debidamente en consideración la legislación y las políticas pertinentes de la UE, en particular las evaluaciones de riesgos y las recomendaciones del Grupo de Cooperación SRI, como la Evaluación de riesgos coordinada de la UE y el Conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G. Además, podría exigirse la certificación de los productos, servicios y procesos de las TIC pertinentes, en virtud de los esquemas europeos de certificación de la ciberseguridad adoptados con arreglo al artículo 49 del Reglamento (UE) 2019/881.

(11) En mayo de 2011, los secretarios generales de las instituciones y los organismos de la Unión decidieron crear un grupo para la preconfiguración de un equipo de respuesta a emergencias informáticas de las instituciones, los órganos y los organismos de la Unión (CERT-UE) bajo la supervisión de un Comité de Dirección interinstitucional. En julio de 2012, los secretarios generales confirmaron las disposiciones prácticas y, como ejemplo de una cooperación interinstitucional visible en el ámbito de la ciberseguridad, acordaron mantener el CERT-UE con carácter de entidad permanente para seguir ayudando a mejorar el nivel global de seguridad de las tecnologías de la información de las instituciones, los órganos y los organismos de la Unión. En septiembre de 2012, se estableció el CERT-UE, a modo de grupo de trabajo de la Comisión con un mandato interinstitucional. En diciembre de 2017, las instituciones y los organismos de la Unión celebraron un acuerdo interinstitucional sobre la organización y el funcionamiento del CERT-UE[3]. Este acuerdo debe seguir evolucionando en apoyo de la ejecución del presente Reglamento.

(12) Debe modificarse la denominación del CERT-UE, que pasaría de «Equipo de respuesta a emergencias informáticas» a «Centro de Ciberseguridad» para las instituciones, los órganos y los organismos de la Unión, en sintonía con los cambios observados en los Estados miembros y en otras partes del mundo, donde muchos CERT han pasado a denominarse «Centros de Ciberseguridad»; sin embargo, por ser ya reconocible, ha de conservarse el nombre abreviado «CERT-UE».

(13) Muchos ciberataques se inscriben en campañas más amplias dirigidas contra grupos de instituciones, órganos y organismos de la Unión o comunidades de intereses que incluyen a instituciones, órganos y organismos de la Unión. A fin de facilitar la detección proactiva, la respuesta a incidentes o la adopción de medidas de mitigación, las instituciones, los órganos y los organismos de la Unión deben notificar al CERT-UE las ciberamenazas, las vulnerabilidades y los incidentes importantes y transmitir los datos técnicos necesarios para poder detectar, mitigar o responder a ciberamenazas, vulnerabilidades e incidentes similares que afecten a otras instituciones, órganos u organismos de la Unión. Siguiendo el mismo planteamiento previsto en la Directiva

[3] DO C 12 de 13.1.2018, p. 1.

[propuesta SRI 2], cuando una entidad tenga conocimiento de un incidente importante, se le ha de exigir que transmita una notificación inicial al CERT-UE en un plazo de veinticuatro horas. De este modo, el CERT-UE podría difundir la información al resto de instituciones, órganos y organismos de la Unión, así como a los homólogos pertinentes, y ayudar así a proteger los entornos informáticos de la Unión y de sus homólogos frente a incidentes, amenazas y vulnerabilidades similares.

(14) Además de conferir al CERT-UE más funciones y reforzar su papel, es necesario establecer un Consejo Interinstitucional de Ciberseguridad (CIIC), que facilitaría el objetivo de garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión mediante el seguimiento de la ejecución del presente Reglamento por parte de las citadas entidades y la supervisión de la puesta en ejecución de las prioridades y los objetivos generales por parte del CERT-UE, al que proporcionaría igualmente una dirección estratégica. El CIIC debe asegurar la representación de las instituciones y contar con representantes de los órganos y organismos a través de la Red de Agencias de la Unión.

(15) El CERT-UE ha de apoyar la ejecución de las medidas destinadas a garantizar un elevado nivel común de ciberseguridad a través de propuestas de documentos de orientación y recomendaciones dirigidas al Consejo Interinstitucional de Ciberseguridad («CIIC»), o emitiendo llamamientos a la acción. Dichos documentos de orientación y recomendaciones deben ser aprobados por el CIIC. En caso necesario, el CERT-UE ha de emitir llamamientos a la acción en los que se describan las medidas urgentes de seguridad que se insta a las instituciones, los órganos y los organismos de la Unión a adoptar en un plazo determinado.

(16) El CIIC debe hacer un seguimiento del cumplimiento del presente Reglamento y de los documentos de orientación, las recomendaciones y los llamamientos a la acción emitidos por el CERT-UE. Es preciso que el CIIC cuente, para las cuestiones técnicas, con el respaldo de grupos técnicos consultivos, constituidos en función de sus necesidades, que trabajen en estrecha cooperación con el CERT-UE, las instituciones, los órganos y los organismos de la Unión y, en su caso, otras partes interesadas. Cuando sea necesario, el CIIC ha de emitir advertencias no vinculantes y recomendar auditorías.

(17) El CERT-UE debe tener la misión de contribuir a la seguridad del entorno informático de la totalidad de las instituciones, los órganos y los organismos de la Unión. Además, debe ejercer, para las instituciones, los órganos y los organismos de la Unión, la función equivalente a la de coordinador designado a efectos de la divulgación coordinada de vulnerabilidades al Registro Europeo de Vulnerabilidades, según lo dispuesto en el artículo 6 de la Directiva [propuesta SRI 2].

(18) En 2020, el Comité de Dirección del CERT-UE estableció un nuevo objetivo estratégico con miras a que el CERT-UE garantice, para el conjunto de las instituciones, los órganos y los organismos de la Unión, un exhaustivo nivel de ciberseguridad con el alcance y la amplitud adecuadas y en continua adaptación a las amenazas, ya sean actuales o inminentes, incluidos los ataques contra los dispositivos móviles, los entornos en la nube y los dispositivos del internet de las cosas. El objetivo estratégico comprende asimismo la intervención de centros de operaciones de seguridad (SOC) con amplias capacidades para supervisar las redes, así como un seguimiento veinticuatro horas al día, siete días a la semana, en caso de amenaza de gran gravedad. Para las instituciones, los órganos y los organismos de la Unión de mayor tamaño, el CERT-UE ha de prestar apoyo a sus equipos de seguridad

informática, en particular mediante un seguimiento de primera línea veinticuatro horas al día, siete días a la semana. Para las instituciones, los órganos y los organismos de la Unión de menor tamaño y algunos de tamaño mediano, el CERT-UE debe prestar todos los servicios.

(19) El CERT-UE también debe desempeñar la función que se le atribuye en la Directiva [propuesta SRI 2] por lo que respecta a la cooperación y el intercambio de información con la red de equipos de respuesta a incidentes de seguridad informática (CSIRT). Además, en consonancia con la Recomendación (UE) 2017/1584 de la Comisión[4], el CERT-UE ha de cooperar con las partes interesadas pertinentes y coordinar su respuesta. A fin de contribuir a un elevado nivel de ciberseguridad en la Unión, el CERT-UE debe compartir información específica sobre incidentes con sus homólogos nacionales. Asimismo, el CERT-UE ha de colaborar con otros homólogos públicos y privados, incluida la OTAN, previa aprobación del CIIC.

(20) El CERT-UE, en su labor de apoyo a la ciberseguridad operativa, ha de recurrir a los conocimientos especializados de la Agencia de la Unión Europea para la Ciberseguridad, a través de la cooperación estructurada prevista en el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[5]. Cuando proceda, deben establecerse disposiciones específicas entre las dos entidades para definir los aspectos prácticos de dicha cooperación y evitar la duplicación de actividades. El CERT-UE ha de cooperar con la Agencia de la Unión Europea para la Ciberseguridad en lo tocante al análisis de amenazas y compartir con esta periódicamente su informe sobre el panorama de amenazas.

(21) En apoyo de la Unidad Cibernética Conjunta, creada de conformidad con la Recomendación de la Comisión de 23 de junio de 2021[6], el CERT-UE debe cooperar e intercambiar información con las partes interesadas con objeto de fomentar la cooperación operativa y favorecer que las redes existentes desarrollen todo su potencial de protección de la Unión.

(22) El tratamiento de datos personales en virtud del presente Reglamento ha de hacerse de conformidad con la legislación relativa a la protección de datos, en particular el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[7].

(23) El tratamiento de información por el CERT-UE y las instituciones, los órganos y los organismos de la Unión debe ajustarse a las normas establecidas en el Reglamento [propuesta de Reglamento relativo a la seguridad de la información]. Con el fin de garantizar la coordinación en los aspectos relacionados con la seguridad, todo contacto con el CERT-UE iniciado o solicitado por un servicio nacional de seguridad e

---

4 Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (DO L 239 de 19.9.2017, p. 36).

5 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») (DO L 151 de 7.6.2019, p. 15).

6 Recomendación de la Comisión, de 23 de junio de 2021, sobre la creación de una Unidad Cibernética Conjunta [C(2021) 4520].

7 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

inteligencia debe comunicarse sin demora indebida a la Dirección de Seguridad de la Comisión Europea y a la presidencia del CIIC.

(24) Dado que los servicios y las funciones del CERT-UE redundan en interés del conjunto de las instituciones, los órganos y los organismos de la Unión, cada institución, órgano y organismo con gasto informático debe contribuir de manera equitativa a dichos servicios y funciones. La contribución ha de entenderse sin perjuicio de la autonomía presupuestaria de las instituciones, los órganos y los organismos de la Unión.

(25) El CIIC, asistido por el CERT-UE, debe revisar y evaluar la ejecución del presente Reglamento e informar de sus conclusiones a la Comisión. La Comisión, a partir de dichas conclusiones, ha de presentar un informe al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Capítulo I
DISPOSICIONES GENERALES

Artículo 1
Objeto

El presente Reglamento establece:

a) la obligación, para las instituciones, los órganos y los organismos de la Unión, de adoptar un marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad;

b) obligaciones, para las instituciones, los órganos y los organismos de la Unión, en materia de gestión de riesgos de ciberseguridad y comunicación de información;

c) normas sobre la organización y el funcionamiento del Centro de Ciberseguridad para las instituciones, los órganos y los organismos de la Unión (CERT-UE), y sobre la organización y el funcionamiento del Consejo Interinstitucional de Ciberseguridad (CIIC).

Artículo 2
Ámbito de aplicación

El presente Reglamento se aplica a la gestión, la gobernanza y el control de riesgos en el ámbito de la ciberseguridad por parte de la totalidad de las instituciones, los órganos y los organismos de la Unión, así como a la organización y al funcionamiento del CERT-UE y del Consejo Interinstitucional de Ciberseguridad.

Artículo 3
Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «instituciones, órganos y organismos de la Unión»: las instituciones, los órganos y los organismos de la Unión creados por, o constituidos sobre la base de, el Tratado de la Unión Europea, el Tratado de Funcionamiento de la Unión Europea o el Tratado constitutivo de la Comunidad Europea de la Energía Atómica;

2) «redes y sistemas de información»: las redes y los sistemas de información en el sentido del artículo 4, punto 1, de la Directiva [propuesta SRI 2];

3) «seguridad de las redes y los sistemas de información»: la seguridad de las redes y los sistemas de información en el sentido del artículo 4, punto 2, de la Directiva [propuesta SRI 2];

4) «ciberseguridad»: la ciberseguridad en el sentido del artículo 4, punto 3, de la Directiva [propuesta SRI 2];

5) «más alto nivel de dirección»: el cargo directivo, el órgano de gestión o el órgano de coordinación y supervisión al más alto nivel administrativo, habida cuenta de los sistemas de gobernanza de alto nivel de cada institución, órgano u organismo de la Unión;

6) «incidente»: un incidente en el sentido del artículo 4, punto 5, de la Directiva [propuesta SRI 2];

7) «incidente importante»: todo incidente salvo aquel cuyas consecuencias sean limitadas y del que probablemente ya se tenga una buena comprensión en términos de método o tecnología;

8) «ataque a gran escala»: todo incidente que requiera más recursos de los que dispongan la institución, el órgano o el organismo de la Unión afectado y el CERT-UE;

9) «gestión de incidentes»: la gestión de incidentes en el sentido del artículo 4, punto 6, de la Directiva [propuesta SRI 2];

10) «ciberamenaza»: una ciberamenaza en el sentido del artículo 2, punto 8, del Reglamento (UE) 2019/881;

11) «ciberamenaza importante»: toda ciberamenaza en la que existan la intención, la oportunidad y la capacidad de provocar un incidente importante;

12) «vulnerabilidad»: la vulnerabilidad en el sentido del artículo 4, punto 8, de la Directiva [propuesta SRI 2];

13) «vulnerabilidad importante»: toda vulnerabilidad que con probabilidad dará lugar a un incidente importante en caso de aprovecharse;

14) «riesgo de ciberseguridad»: toda circunstancia o hecho razonablemente identificables que puedan ser perjudiciales para la seguridad de las redes y los sistemas de información;

15) «Unidad Cibernética Conjunta»: una plataforma virtual y física de cooperación para las diferentes comunidades de ciberseguridad de la Unión, centrada en la coordinación operativa y técnica contra las ciberamenazas y los incidentes transfronterizos a gran escala en el sentido de la Recomendación de la Comisión de 23 de junio de 2021;

16) «código básico de ciberseguridad»: el conjunto de normas mínimas de ciberseguridad a las que deben ajustarse tanto las redes y los sistemas de información como sus operadores y usuarios a fin de minimizar los riesgos de ciberseguridad.

Capítulo II
MEDIDAS DESTINADAS A GARANTIZAR UN ELEVADO NIVEL COMÚN DE CIBERSEGURIDAD

Artículo 4

Gestión, gobernanza y control de los riesgos

1. Cada institución, órgano y organismo de la Unión, en apoyo de su misión y dentro del ejercicio de su autonomía institucional, establecerá su propio marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad («el marco»). A fin de garantizar la gestión eficaz y prudente de todos los riesgos relacionados con la ciberseguridad, el más alto nivel de dirección de cada entidad supervisará esta labor. El marco deberá estar establecido a más tardar el ... [quince meses después de la entrada en vigor del presente Reglamento].

2. El marco abarcará la totalidad del entorno informático de la institución, el órgano o el organismo de que se trate, con inclusión de cualesquiera entornos informáticos internos, activos externalizados y servicios en entornos de computación en la nube o alojados por terceros, dispositivos móviles, redes corporativas, redes profesionales no conectadas a internet y dispositivos conectados al entorno informático. El marco contemplará la gestión de la continuidad de las actividades y de crisis, así como la seguridad de la cadena de suministro y la gestión de los riesgos humanos que puedan afectar a la ciberseguridad de la institución, el órgano o el organismo de la Unión de que se trate.

3. El más alto nivel de dirección de cada institución, órgano y organismo de la Unión garantizará la supervisión del cumplimiento, por parte de su organización, de las obligaciones relacionadas con la gestión, la gobernanza y el control de riesgos en el ámbito de la ciberseguridad, sin perjuicio de las responsabilidades formales que incumban a otros niveles de dirección en relación con el cumplimiento y la gestión de riesgos en sus respectivos ámbitos de responsabilidad.

4. Cada institución, órgano y organismo de la Unión dispondrá de mecanismos eficaces para asegurar que un porcentaje adecuado de su presupuesto informático se destine a la ciberseguridad.

5. Cada institución, órgano y organismo de la Unión nombrará a su responsable local de ciberseguridad, o a una persona con una función equivalente, que será el punto de contacto único para todos los aspectos relacionados con la ciberseguridad.

Artículo 5

Código básico de ciberseguridad

1. El más alto nivel de dirección de cada institución, órgano y organismo de la Unión aprobará el código básico de ciberseguridad de su propia entidad para abordar los riesgos detectados en el marco a que se refiere el artículo 4, apartado 1. Esto lo hará en apoyo de su misión y dentro del ejercicio de su autonomía institucional. El código básico de ciberseguridad, que deberá estar establecido a más tardar el ... [dieciocho meses después de la entrada en vigor del presente Reglamento], cubrirá los ámbitos enumerados en el anexo I y las medidas enumeradas en el anexo II.

2. La alta dirección de cada institución, órgano y organismo de la Unión asistirá periódicamente a actividades de formación específicas a fin de adquirir los conocimientos y las capacidades suficientes para comprender y evaluar los riesgos de

ciberseguridad y las prácticas de gestión de la ciberseguridad, así como su repercusión en las actividades de la organización.

Artículo 6
Evaluaciones de madurez

Cada institución, órgano y organismo de la Unión realizará, como mínimo cada tres años, una evaluación de la madurez de la ciberseguridad que englobará todos los elementos del entorno informático de la entidad descritos en el artículo 4, teniendo en cuenta, además, cualesquiera documentos de orientación y recomendaciones pertinentes adoptados de conformidad con el artículo 13.

Artículo 7
Planes de ciberseguridad

1. A partir de las conclusiones extraídas de la evaluación de madurez y teniendo en cuenta los activos y los riesgos determinados con arreglo al artículo 4, el más alto nivel de dirección de cada institución, órgano y organismo de la Unión aprobará un plan de ciberseguridad sin demora indebida tras el establecimiento del marco de gestión, gobernanza y control de riesgos y del código básico de ciberseguridad. El objetivo del plan será aumentar el nivel global de ciberseguridad de la entidad de que se trate y contribuir así a alcanzar o consolidar un elevado nivel común de ciberseguridad para el conjunto de las instituciones, los órganos y los organismos de la Unión. A fin de apoyar la misión de la entidad, en el marco de su autonomía institucional, el plan incluirá, como mínimo, los ámbitos enumerados en el anexo I, las medidas enumeradas en el anexo II y medidas de preparación, respuesta y recuperación en caso de incidente, como el seguimiento de la seguridad y los registros secuenciales. El plan se revisará como mínimo cada tres años, tras las evaluaciones de madurez realizadas con arreglo al artículo 6.
2. El plan de ciberseguridad especificará las funciones y responsabilidades del personal a efectos de su ejecución.
3. El plan de ciberseguridad se diseñará teniendo en cuenta cualesquiera documentos de orientación y recomendaciones del CERT-UE que sean de aplicación.

Artículo 8
Ejecución

1. Una vez finalizadas las evaluaciones de madurez, las instituciones, los órganos y los organismos de la Unión las transmitirán al Consejo Interinstitucional de Ciberseguridad. Una vez finalizados los planes de seguridad, las instituciones, los órganos y los organismos de la Unión lo notificarán al Consejo Interinstitucional de Ciberseguridad. Previa solicitud del Consejo Interinstitucional de Seguridad, las entidades facilitarán información sobre aspectos específicos del presente capítulo.
2. Los documentos de orientación y las recomendaciones que se emitan de conformidad con el artículo 13 servirán de apoyo a la ejecución de las disposiciones del presente capítulo.

Capítulo III
CONSEJO INTERINSTITUCIONAL DE CIBERSEGURIDAD

Artículo 9
Consejo Interinstitucional de Ciberseguridad

1. Se crea un Consejo Interinstitucional de Ciberseguridad (CIIC).

2. El CIIC será responsable de:

   a) hacer un seguimiento de la ejecución del presente Reglamento por parte de las instituciones, los órganos y los organismos de la Unión;

   b) supervisar la puesta en ejecución de las prioridades y los objetivos generales por parte del CERT-UE, al que, además, proporcionará una dirección estratégica.

3. El CIIC estará compuesto por tres representantes designados por la Red de Agencias de la Unión (EUAN), a propuesta de su Comité Consultivo para las TIC, que representarán los intereses de los órganos y los organismos que gestionen sus propios entornos informáticos, y un representarte designado por cada uno de los siguientes:

   a) el Parlamento Europeo;

   b) el Consejo de la Unión Europea;

   c) la Comisión Europea;

   d) el Tribunal de Justicia de la Unión Europea;

   e) el Banco Central Europeo;

   f) el Tribunal de Cuentas Europeo;

   g) el Servicio Europeo de Acción Exterior;

   h) el Comité Económico y Social Europeo;

   i) el Comité de las Regiones;

   j) el Banco Europeo de Inversiones;

   k) la Agencia de la Unión Europea para la Ciberseguridad.

   Los miembros podrán estar asistidos por sus suplentes. El presidente o la presidenta podrá invitar a otros representantes de las organizaciones enumeradas o de otras instituciones u otros órganos u organismos de la Unión a asistir a las reuniones del CIIC sin derecho de voto.

4. El CIIC aprobará su reglamento interno.

5. De conformidad con dicho reglamento interno, el CIIC nombrará a su presidente o presidenta, de entre sus miembros, por un período de cuatro años. Su suplente pasará a ser miembro de pleno derecho del CIIC durante el mismo período.

6. El CIIC se reunirá a iniciativa de su presidente o presidenta, a petición del CERT-UE o a petición de cualquiera de sus miembros.

7. Cada miembro del CIIC dispondrá de un voto. Las decisiones del CIIC se adoptarán por mayoría simple, salvo que se disponga otra cosa en el presente Reglamento. El presidente o la presidenta no participará en la votación, salvo que se produzca un empate, en cuyo caso podrá emitir un voto de calidad.

8. El CIIC podrá actuar mediante un procedimiento escrito simplificado, iniciado de conformidad con su reglamento interno. Con arreglo a este procedimiento, la decisión pertinente se considerará aprobada en el plazo establecido por el presidente o la presidenta, salvo oposición de uno de sus miembros.

9. El director o la directora del CERT-UE, o su suplente, participará en las reuniones del CIIC, a menos que este disponga otra cosa.

10. La Comisión prestará servicios de secretaría al CIIC.

11. Los representantes designados por la EUAN, a propuesta del Comité Consultivo para las TIC, transmitirán las decisiones del CIIC a las agencias y las empresas comunes de la Unión. Todo órgano y organismo de la Unión estará autorizado a plantear a los representantes o al presidente o la presidenta del CIIC cualquier cuestión que considere que debe ponerse en conocimiento de este.

12. El CIIC podrá actuar mediante un procedimiento escrito simplificado, iniciado por su presidente o presidenta, con arreglo al cual la decisión pertinente se considerará aprobada en el plazo establecido por el presidente o la presidenta, salvo oposición de uno de sus miembros.

13. El CIIC podrá designar un comité ejecutivo que le asista en el desempeño de su labor, y delegar en este parte de sus funciones y competencias. El CIIC establecerá el reglamento interno del comité ejecutivo, que incluirá sus funciones y competencias y el mandato de sus miembros.

Artículo 10
Funciones del CIIC

En el ejercicio de sus responsabilidades, el CIIC deberá en particular:

a) revisar cualesquiera informes solicitados por el CERT-UE sobre el estado de la ejecución del presente Reglamento por parte de las instituciones, los órganos y los organismos de la Unión;

b) aprobar, sobre la base de una propuesta del director o de la directora de CERT-UE, el programa de trabajo anual del CERT-UE y hacer un seguimiento de su ejecución;

c) aprobar, sobre la base de una propuesta del director o de la directora de CERT-UE, el catálogo de servicios del CERT-UE;

d) aprobar, sobre la base de una propuesta del director o de la directora del CERT-UE, la planificación financiera anual de ingresos y gastos, incluida la dotación de personal, para las actividades del CERT-UE;

e) aprobar, sobre la base de una propuesta del director o de la directora de CERT-UE, las modalidades de los acuerdos de nivel de servicio;

f) examinar y aprobar el informe anual elaborado por el director o la directora del CERT-UE sobre las actividades y la gestión de fondos del CERT-UE;

g) aprobar y hacer un seguimiento de los indicadores clave de rendimiento del CERT-UE definidos sobre la base de una propuesta de su director o directora;

h) aprobar los acuerdos de cooperación, los acuerdos de nivel de servicio o los contratos celebrados entre el CERT-UE y otras entidades con arreglo al artículo 17;

i) establecer los grupos de asesoramiento técnico necesarios para asistir al CIIC en su labor, aprobar su mandato y nombrar a los respectivos presidentes.

Artículo 11
Cumplimiento

El CIIC hará un seguimiento de la ejecución, por parte de las instituciones, los órganos y los organismos de la Unión, del presente Reglamento y de los documentos de orientación, las recomendaciones y los llamamientos a la acción adoptados. Cuando constate que una institución, un órgano o un organismo de la Unión no ha aplicado o ejecutado de manera efectiva el presente Reglamento o los documentos de orientación, las recomendaciones o los llamamientos a la acción emitidos en virtud del presente Reglamento, el CIIC podrá, sin perjuicio de los procedimientos internos de la institución, el órgano o el organismo de la Unión de que se trate:

a) emitir una advertencia; cuando sea necesario en vista de la existencia de un riesgo de ciberseguridad imperioso, el público destinatario de la advertencia se restringirá según corresponda;

b) recomendar al servicio de auditoría interna pertinente que lleve a cabo una auditoría.

Capítulo IV
CERT-UE

Artículo 12
Misión y funciones del CERT-UE

1. La misión del CERT-UE, el Centro de Ciberseguridad interinstitucional y autónomo para el conjunto de las instituciones, los órganos y los organismos de la Unión, será contribuir al refuerzo de la seguridad del entorno informático no clasificado de la totalidad de las instituciones, los órganos y los organismos de la Unión ofreciéndoles asesoramiento sobre ciberseguridad, prestándoles ayuda para prevenir, detectar, mitigar y responder a los incidentes, y proporcionándoles una función de centro de coordinación para el intercambio de información sobre ciberseguridad y la respuesta a incidentes.

2. El CERT-UE desempeñará, para las instituciones, los órganos y los organismos de la Unión, las funciones siguientes:

   a) prestará apoyo a efectos de la ejecución del presente Reglamento y contribuirá a la coordinación de su aplicación a través de las medidas enumeradas en el artículo 13, apartado 1, o de informes especiales solicitados por el CIIC;

   b) prestará apoyo a través de un paquete de servicios de ciberseguridad descritos en su catálogo de servicios («servicios básicos»):

   c) mantendrá una red de homólogos y socios en apoyo de los servicios de acuerdo con lo dispuesto en los artículos 16 y 17;

   d) pondrá en conocimiento del CIIC toda cuestión relacionada con la ejecución del presente Reglamento y de los documentos de orientación, las recomendaciones y los llamamientos a la acción;

   e) informará sobre las ciberamenazas a las que se enfrenten las instituciones, los órganos y los organismos de la Unión y contribuirá al conocimiento situacional de la UE en el ámbito cibernético.

3. El CERT-UE contribuirá a la Unidad Cibernética Conjunta, creada con arreglo a la Recomendación de la Comisión de 23 de junio de 2021, en particular en los ámbitos siguientes:

   a) preparación, coordinación de incidentes, intercambio de información y respuesta a las crisis, en el plano técnico, en asuntos que afecten a las instituciones, los órganos y los organismos de la Unión;

   b) cooperación operativa con la red de equipos de respuesta a incidentes de seguridad (CSIRT), en particular en lo referente a la asistencia mutua, y con la comunidad de ciberseguridad en sentido amplio;

   c) inteligencia sobre ciberamenazas, en particular en lo referente a la conciencia situacional;

   d) cualquier aspecto que requiera los conocimientos técnicos sobre ciberseguridad del CERT-UE.

4. El CERT-UE entablará una cooperación estructurada con la Agencia de la Unión Europea para la Ciberseguridad en relación con el desarrollo de capacidades, la cooperación operativa y los análisis estratégicos a largo plazo de las ciberamenazas, de conformidad con el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo.

5. El CERT-UE podrá prestar los servicios no descritos en su catálogo de servicios («servicios facturables») que se indican a continuación:

   a) servicios de apoyo a la ciberseguridad del entorno informático de las instituciones, los órganos y los organismos de la Unión distintos de los referidos en el apartado 2, en virtud de acuerdos de nivel de servicio y en función de los recursos disponibles;

   b) servicios de apoyo a las operaciones o los proyectos de ciberseguridad de las instituciones, los órganos y los organismos de la Unión, distintos de los destinados a proteger sus entornos informáticos, en virtud de acuerdos escritos y con la aprobación previa del CIIC;

   c) servicios de apoyo a la seguridad del entorno informático de organizaciones distintas de las instituciones, los órganos y los organismos de la Unión que cooperen estrechamente con estos, por ejemplo, mediante la asignación de funciones o responsabilidades con arreglo al Derecho de la Unión, en virtud de acuerdos escritos y con la aprobación previa del CIIC.

6. El CERT-UE podrá organizar ejercicios de ciberseguridad o recomendar la participación en ejercicios en curso, en estrecha cooperación, cuando proceda, con la Agencia de la Unión Europea para la Ciberseguridad, con objeto de someter a prueba el nivel de ciberseguridad de las instituciones, los órganos y los organismos de la Unión.

7. El CERT-UE podrá prestar asistencia a las instituciones, los órganos y los organismos de la Unión en relación con incidentes en entornos informáticos clasificados si la Parte afectada lo solicita expresamente.

Artículo 13

Documentos de orientación, recomendaciones y llamamientos a la acción

1. En apoyo de la ejecución del presente Reglamento, el CERT-UE:

a) emitirá llamamientos a la acción, en los que se describirán determinadas medidas urgentes de seguridad que se insta a las instituciones, los órganos y los organismos de la Unión a adoptar en un plazo específico;

b) propondrá al CIIC documentos de orientación dirigidos a la totalidad o a un subconjunto de las instituciones, los órganos y los organismos de la Unión;

c) propondrá al CIIC recomendaciones dirigidas a instituciones, órganos y organismos de la Unión específicos.

2. Los documentos de orientación y las recomendaciones podrán incluir:

a) las modalidades de la gestión de riesgos de ciberseguridad y los códigos básicos de ciberseguridad, o mejoras al respecto;

b) las modalidades de las evaluaciones de madurez y los planes de ciberseguridad; y

c) en su caso, el uso de tecnologías, arquitecturas y mejores prácticas comunes con miras a la interoperabilidad y el establecimiento de normas comunes en el sentido del artículo 4, punto 10, de la Directiva [propuesta SRI 2].

3. El CIIC podrá adoptar documentos de orientación o recomendaciones a propuesta del CERT-UE.

4. El CIIC podrá dar instrucciones al CERT-UE para que emita, retire o modifique una propuesta de documento de orientación o de recomendación o un llamamiento a la acción.

Artículo 14
Dirección del CERT-UE

El director o la directora del CERT-UE presentará periódicamente informes al CIIC y a su presidente o presidenta sobre el desempeño, la planificación financiera, los ingresos, la ejecución del presupuesto, los acuerdos de nivel de servicio y los acuerdos escritos celebrados, la cooperación con homólogos y socios, y las misiones realizadas por el personal del CERT-UE, incluidos los informes a que se refiere el artículo 10, apartado 1.

Artículo 15
Aspectos financieros y de personal

1. La Comisión, tras obtener la aprobación por unanimidad del CIIC, nombrará al director o a la directora del CERT-UE. Se consultará al CIIC en todas las fases del procedimiento antes del nombramiento del director o de la directora del CERT-UE, en particular sobre la redacción de las convocatorias de vacante, el examen de las candidaturas y la designación de los comités de selección para el puesto.

2. En la aplicación de los procedimientos administrativos y financieros, el presidente o la presidenta del CERT-UE actuará bajo la autoridad de la Comisión.

3. Las funciones y actividades del CERT-UE, con inclusión de los servicios que preste en virtud del artículo 12, apartados 2, 3, 4 y 6, y el artículo 13, apartado 1, a las instituciones, los órganos y los organismos de la Unión financiados con cargo a la rúbrica del marco financiero plurianual dedicada a la administración pública europea, se financiarán mediante una línea presupuestaria específica del presupuesto de la Comisión. Los puestos reservados al CERT-UE se detallarán en una nota a pie de página de la plantilla de personal de la Comisión.

4. Las instituciones, los órganos y los organismos de la Unión distintos de los mencionados en el apartado 3 efectuarán una contribución financiera anual al CERT-UE para cubrir los servicios prestados por este de conformidad con dicho apartado 3. Las respectivas contribuciones se basarán en orientaciones del CIIC y serán acordadas entre cada entidad y el CERT-UE en acuerdos de nivel de servicio. Las contribuciones representarán una parte equitativa y proporcional del coste total de los servicios prestados. Se consignarán en la línea presupuestaria específica a que se refiere el apartado 3 como ingresos afectados, de conformidad con lo previsto en el artículo 21, apartado 3, letra c), del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo[8].

5. Los costes de las funciones definidas en el artículo 12, apartado 5, se recuperarán de las instituciones, los órganos y los organismos de la Unión que reciban los servicios del CERT-UE. Los ingresos se asignarán a las líneas presupuestarias con las que se cubran los costes.

Artículo 16

Cooperación del CERT-UE con sus homólogos de los Estados miembros

1. El CERT-UE cooperará e intercambiará información con sus homólogos nacionales de los Estados miembros, incluidos los CERT, los centros nacionales de ciberseguridad, los CSIRT y los puntos de contacto únicos a que se refiere el artículo 8 de la Directiva [propuesta SRI 2], en lo concerniente a ciberamenazas, vulnerabilidades e incidentes, posibles contramedidas y cualesquiera cuestiones pertinentes para la mejora de la protección del entorno informático de las instituciones, los órganos y los organismos de la Unión, en particular a través de la red de CSIRT a que se refiere el artículo 13 de la Directiva [propuesta SRI 2].

2. El CERT-UE podrá, sin necesidad de obtener el consentimiento de la Parte afectada, intercambiar información específica sobre incidentes con sus homólogos nacionales de los Estados miembros con objeto de facilitar la detección de ciberamenazas o incidentes similares. No obstante, el CERT-UE únicamente podrá intercambiar información específica sobre incidentes en la que se revele la identidad del objetivo del incidente de ciberseguridad con el consentimiento previo de la Parte afectada.

Artículo 17

Cooperación del CERT-UE con homólogos no pertenecientes a los Estados miembros

1. El CERT-UE podrá cooperar con homólogos no pertenecientes a los Estados miembros, en particular los de sectores específicos, en lo tocante a herramientas y métodos tales como técnicas, tácticas, procedimientos y mejores prácticas, y en lo tocante a las ciberamenazas y las vulnerabilidades. A los efectos de la cooperación con dichos homólogos, en particular cuando se trate de homólogos no pertenecientes a la UE que cooperen con homólogos nacionales de los Estados miembros, el CERT-UE solicitará la aprobación previa del CIIC.

---

[8] Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión, por el que se modifican los Reglamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 y (UE) n.º 283/2014 y la Decisión n.º 541/2014/UE y por el que se deroga el Reglamento (UE, Euratom) n.º 966/2012 (DO L 193 de 30.7.2018, p. 1).

2. El CERT-UE podrá cooperar con otros socios, como entidades comerciales, organizaciones internacionales, entidades nacionales no pertenecientes a la Unión Europea o expertos individuales, con el fin de recopilar información sobre ciberamenazas, vulnerabilidades y posibles contramedidas generales y específicas. A los efectos de una cooperación más amplia con dichos socios, el CERT-UE solicitará la aprobación previa del CIIC.

3. El CERT-UE podrá, con el consentimiento de la Parte afectada por un incidente, facilitar información relacionada con el incidente a socios que puedan contribuir a su análisis.

Capítulo V
OBLIGACIONES DE COOPERACIÓN E INFORMACIÓN

Artículo 18
Tratamiento de la información

1. El CERT-UE y las instituciones, los órganos y los organismos de la Unión respetarán la obligación de secreto profesional de conformidad con el artículo 339 del Tratado de Funcionamiento de la Unión Europea u otros marcos equivalentes aplicables.

2. Toda solicitud de acceso público a los documentos que obren en poder del CERT-UE se atendrá a las disposiciones del Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo[9], y en particular a la obligación, prevista en dicho Reglamento, de consultar a la institución, el órgano o el organismo de la Unión pertinente cuando la solicitud se refiera a sus documentos.

3. El tratamiento de datos personales con arreglo al presente Reglamento estará sujeto al Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo.

4. El tratamiento de información por el CERT-UE y sus instituciones, órganos y organismos de la Unión se hará de conformidad con las normas establecidas en la [propuesta de Reglamento relativo a la seguridad de la información].

5. Todo contacto con el CERT-UE iniciado o solicitado por un servicio nacional de seguridad e inteligencia se comunicará sin demora indebida a la Dirección de Seguridad de la Comisión y al presidente o a la presidenta del CIIC.

Artículo 19
Obligaciones de intercambio de información

1. Con miras a coordinar la gestión de vulnerabilidades y la respuesta a incidentes, el CERT-UE podrá solicitar a las instituciones, los órganos y los organismos de la Unión que le faciliten información acerca de sus respectivos inventarios de sistemas informáticos que sea pertinente para el desempeño de su labor. La institución, el órgano o el organismo objeto de la solicitud transmitirá sin demora indebida la información solicitada, así como toda actualización posterior de la información.

2. Las instituciones, los órganos y los organismos de la Unión facilitarán al CERT-UE, previa solicitud y sin demora indebida, información digital creada mediante el uso de

[9] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

los dispositivos electrónicos implicados en sus respectivos incidentes. El CERT-UE podrá aclarar con más detalle el tipo de información digital que necesita a efectos del conocimiento situacional y la respuesta a incidentes.

3. El CERT-UE únicamente podrá intercambiar información específica sobre incidentes en la que se revele la identidad de la institución, el órgano o el organismo de la Unión afectados por el incidente con el consentimiento de la entidad afectada. El CERT-UE únicamente podrá intercambiar información específica sobre incidentes en la que se revele la identidad del objetivo del incidente de ciberseguridad con el consentimiento previo de la entidad afectada por el incidente.

4. Las obligaciones de intercambio de información no se aplicarán a la información clasificada de la UE (ICUE) ni a la información que una institución, un órgano o un organismo de la Unión haya recibido de un servicio de seguridad o de inteligencia de un Estado miembro con la condición explícita de que no se comparta con el CERT-UE.

Artículo 20
Obligaciones de notificación

1. Las instituciones, los órganos y los organismos de la Unión transmitirán al CERT-UE una notificación inicial de las ciberamenazas, las vulnerabilidades y los incidentes importantes sin demora indebida, y en todo caso dentro de las veinticuatro horas siguientes a su constatación.

   En casos debidamente justificados y previo acuerdo del CERT-UE, la institución, el órgano o el organismo de la Unión de que se trate podrá incumplir el plazo establecido en el párrafo anterior.

2. Adicionalmente, las instituciones, los órganos y los organismos de la Unión notificarán al CERT-UE, sin demora indebida, los detalles técnicos pertinentes sobre las ciberamenazas, las vulnerabilidades y los incidentes que faciliten la detección, la respuesta a incidentes o la adopción de medidas de mitigación. La notificación incluirá, si se dispone de ella, la información siguiente:

   a) indicadores de compromiso pertinentes;

   b) mecanismos de detección pertinentes;

   c) posibles consecuencias;

   d) medidas de mitigación pertinentes.

3. El CERT-UE presentará mensualmente a la ENISA un informe resumido que contendrá datos anonimizados y agregados sobre las ciberamenazas, las vulnerabilidades y los incidentes importantes notificados de conformidad con el apartado 1.

4. El CIIC podrá publicar documentos de orientación o recomendaciones sobre las modalidades y el contenido de las notificaciones. El CERT-UE difundirá los detalles técnicos pertinentes a fin de facilitar la detección proactiva, la respuesta a incidentes o la adopción de medidas de mitigación por parte de las instituciones, los órganos y los organismos de la Unión.

5. Las obligaciones de notificación no serán aplicables a la ICUE ni a la información que una institución, un órgano o un organismo de la Unión haya recibido de un

servicio de seguridad o de inteligencia de un Estado miembro con la condición explícita de que no se comparta con el CERT-UE.

Artículo 21

Coordinación de la respuesta a incidentes y cooperación en caso de incidentes importantes

1. En el ejercicio de su función de centro de intercambio de información sobre ciberseguridad y coordinación de la respuesta a incidentes, el CERT-UE facilitará el intercambio de información sobre ciberamenazas, vulnerabilidades e incidentes entre:

   a) las instituciones, los órganos y los organismos de la Unión;

   b) los homólogos a que se refieren los artículos 16 y 17.

2. El CERT-UE facilitará la coordinación de la respuesta a incidentes entre las instituciones, los órganos y los organismos de la Unión, con inclusión de lo siguiente:

   a) contribución a una comunicación externa congruente;

   b) asistencia mutua;

   c) uso óptimo de los recursos operativos;

   d) coordinación con otros mecanismos de respuesta a las crisis a escala de la Unión.

3. El CERT-UE apoyará a las instituciones, los órganos y los organismos de la Unión en lo que respecta al conocimiento situacional en materia de ciberamenazas, vulnerabilidades e incidentes.

4. El CIIC publicará orientaciones sobre la coordinación de la respuesta a incidentes y la cooperación en caso de incidentes importantes. Cuando se sospeche que un incidente es de carácter delictivo, el CERT-UE ofrecerá asesoramiento sobre el modo de notificar el incidente a las autoridades policiales.

Artículo 22

Ataques a gran escala

1. El CERT-UE coordinará la respuesta de las instituciones, los órganos y los organismos de la Unión a los ataques a gran escala. Llevará un inventario de los conocimientos técnicos necesarios para la respuesta a incidentes en el caso de que se produzcan tales ataques.

2. Las instituciones, los órganos y los organismos de la Unión contribuirán al inventario de conocimientos técnicos facilitando una lista, que actualizarán anualmente, en la que figuren los expertos disponibles en sus respectivas organizaciones junto con una descripción detallada de las capacidades técnicas específicas de cada uno de ellos.

3. Previa aprobación de la institución, el órgano o el organismo de la Unión de que se trate, el CERT-UE también podrá recurrir a los expertos de la lista referida en el apartado 2 para contribuir a la respuesta a un ataque a gran escala en un Estado miembro, en consonancia con los procedimientos operativos de la Unidad Cibernética Conjunta.

Capítulo VI
DISPOSICIONES FINALES

Artículo 23
Reasignación presupuestaria inicial

La Comisión propondrá la reasignación a su presupuesto de personal y recursos financieros de las instituciones, los órganos y los organismos de la Unión pertinentes. La reasignación será efectiva al mismo tiempo que el primer presupuesto adoptado tras la entrada en vigor del presente Reglamento.

Artículo 24
Revisión

1. El CIIC, asistido por el CERT-UE, informará periódicamente a la Comisión acerca de la ejecución del presente Reglamento. El CIIC podrá asimismo formular recomendaciones a la Comisión para que proponga las modificaciones necesarias del presente Reglamento.
2. La Comisión informará de la ejecución del presente Reglamento al Parlamento Europeo y al Consejo a más tardar transcurridos cuarenta y ocho meses desde la entrada en vigor del presente Reglamento, y posteriormente cada tres años.
3. La Comisión evaluará el funcionamiento del presente Reglamento e informará de sus conclusiones al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones al menos cinco años después de la entrada en vigor.

Artículo 25
Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente / La Presidenta	*El Presidente / La Presidenta*

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Ámbito(s) político(s) afectado(s)

1.3. La propuesta/iniciativa se refiere a:

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultado(s) e incidencia esperados

1.4.4. Indicadores de resultados

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado de la aplicación de la iniciativa

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de reasignación

1.6. Duración e incidencia financiera de la propuesta/iniciativa

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del modo / de los modos de gestión, el/los mecanismo(s) de aplicación de la financiación, las modalidades de pago y la estrategia de control propuestos

2.2.2. Información relativa a los riesgos establecidos y al sistema / a los sistemas de control interno establecidos para atenuarlos

2.2.3. Estimación y justificación de la relación coste/beneficio de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados»), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia financiera estimada de la propuesta en los créditos

3.2.1. Resumen de la incidencia estimada en los créditos de operaciones

3.2.2. Resultados estimados financiados con créditos de operaciones

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

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

1.2. Ámbito(s) político(s) afectado(s)

Administración pública europea

La propuesta atañe a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión.

1.3. La propuesta/iniciativa se refiere a:

☑una acción nueva

☐ una acción nueva a raíz de un proyecto piloto / una acción preparatoria[10]

☐ la prolongación de una acción existente

☑ una fusión o reorientación de una o más acciones hacia otra / una nueva acción

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

– Establecer un marco para garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión.

– Proporcionar una nueva base jurídica para el CERT-UE a fin de reforzar su mandato y su financiación.

1.4.2. Objetivo(s) específico(s)

(1) Establecer la obligación, para las instituciones, los órganos y los organismos de la Unión, de adoptar un marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad.

(2) Establecer la obligación, para las instituciones, los órganos y los organismos de la Unión, de informar de su marco de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad, así como de los incidentes de ciberseguridad.

(3) Establecer normas sobre la organización y el funcionamiento del Centro de Ciberseguridad para las instituciones, los órganos y los organismos de la Unión (CERT-UE), y sobre la organización y el funcionamiento del Consejo Interinstitucional de Ciberseguridad (CIIC).

(4) Contribuir a la Unidad Cibernética Conjunta.

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

[10] Tal como se contempla en el artículo 58, apartado 2, letra a) o b), del Reglamento Financiero.

– Marcos internos de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad, códigos básicos de ciberseguridad, evaluaciones periódicas de madurez y planes de ciberseguridad en las instituciones, los órganos y los organismos de la Unión.

– Mejora de la resiliencia en materia de ciberseguridad y las capacidades de respuesta a incidentes de las instituciones, los órganos y los organismos de la Unión.

– Modernización del CERT-UE.

– Contribución a la Unidad Cibernética Conjunta.

1.4.4. Indicadores de resultados

Especifíquense los indicadores que permiten realizar el seguimiento de los avances y logros.

– Las instituciones, los órganos y los organismos de la Unión establecen sus marcos y códigos básicos, realizan evaluaciones periódicas de madurez y aplican sus planes de ciberseguridad.

– Mejora la gestión de los incidentes.

– La alta dirección de las instituciones, los órganos y los organismos de la Unión adquiere mayor conciencia de los riesgos de ciberseguridad.

– Se nivela el gasto en seguridad de las TIC como porcentaje del gasto global en las TIC.

– Se refuerza el liderazgo del CIIC y del CERT-UE.

– Se da un mayor intercambio de información entre las instituciones, los órganos y los organismos de la Unión y con los organismos y las partes interesadas pertinentes de la UE.

– Hay una mayor cooperación en el ámbito de la ciberseguridad con los organismos y las partes interesadas pertinentes de la UE, a través del CERT-UE y la ENISA.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado de la aplicación de la iniciativa.

El objetivo de la propuesta es dotar a las instituciones, los órganos y los organismos de la Unión de mayor ciberresiliencia, reducir las disparidades entre estas entidades en cuanto a su resiliencia, y mejorar el nivel de conciencia situacional conjunta y la capacidad colectiva de preparación y respuesta.

La propuesta es plenamente coherente con otras iniciativas conexas, y en particular con 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 [propuesta SRI 2].

La propuesta es una parte esencial de la Estrategia de la UE para una Unión de la Seguridad y de la Estrategia de Ciberseguridad de la UE para la Década Digital.

De acuerdo con la programación, la Comisión Europea propondría el Reglamento en octubre de 2021, el Parlamento Europeo y el Consejo lo adoptarían en 2022, y las disposiciones serían aplicables a partir de la entrada en vigor del Reglamento. Está

previsto que las repercusiones financieras y de recursos humanos expuestas en la presente ficha financiera legislativa comiencen en 2023. Aunque ya se inició un período preparatorio en 2021, las actividades preparatorias de 2021 y 2022 quedan fuera de las repercusiones financieras de la propuesta.

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

Motivos para actuar a nivel europeo (*ex ante*):

Entre 2019 y 2021, se produjo un incremento drástico del número de incidentes importantes, orquestados por agentes de amenazas persistentes avanzadas, que afectaron a las instituciones, los órganos y los organismos de la Unión. Solo en el primer semestre de 2021 se registró un número de incidentes importantes equivalente al de todo el año 2020. Esta situación se refleja igualmente en el número de imágenes forenses (copias exactas del contenido de los sistemas o dispositivos afectados) 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.

El nivel de madurez de la ciberseguridad varía sustancialmente de una entidad a otra[11]. El presente Reglamento garantiza que la totalidad de las instituciones, los órganos y los organismos de la Unión implementen un código básico de medidas de seguridad y cooperen entre sí con miras al funcionamiento abierto y eficiente de la administración de la Unión.

Los sistemas que deben preservarse se inscriben en el ámbito de la autonomía de las instituciones, los órganos y los organismos de la Unión, que son los responsables de su administración; los Estados miembros no podrían llevar a cabo las medidas propuestas.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La Directiva SRI es el primer instrumento horizontal del mercado interior destinado a mejorar la resiliencia de las redes y los sistemas de la Unión frente a los riesgos de ciberseguridad. Desde su entrada en vigor en 2016, ha contribuido notablemente a elevar el nivel común de ciberseguridad de los Estados miembros. Con la propuesta de Directiva SRI 2 se pretende mejorar las medidas introducidas.

El objetivo del Reglamento es establecer medidas similares para las instituciones, los órganos y los organismos de la Unión.

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

La propuesta está en consonancia con el marco financiero plurianual y es una parte esencial de la Estrategia de la UE para una Unión de la Seguridad y de la Estrategia de Ciberseguridad de la UE para la Década Digital.

[11] Referencia: [Informe especial del TCE sobre la ciberseguridad en las instituciones, los órganos y los organismos de la Unión].

La propuesta prevé que se apliquen medidas a las instituciones, los órganos y los organismos de la Unión con el fin de garantizar un elevado nivel común de ciberseguridad. La propuesta es acorde con 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 [propuesta SRI 2].

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de reasignación

La gestión de las funciones del CERT-UE exige perfiles específicos y una carga de trabajo adicional que no puede asumirse sin el aumento de los recursos humanos y financieros.

1.6. Duración e incidencia financiera de la propuesta/iniciativa

☐ **duración limitada**

– ☐ en vigor desde [el] [DD.MM]AAAA hasta [el] [DD.MM]AAAA

– ☐ incidencia financiera desde AAAA hasta AAAA para los créditos de compromiso y desde AAAA hasta AAAA para los créditos de pago.

☑ **duración ilimitada**

– Está previsto que la incidencia financiera comience con el primer presupuesto adoptado tras la entrada en vigor del Reglamento. Durante el primer año, considerado de transición, tendría lugar una reasignación de recursos de las instituciones y los principales organismos de la Unión a la Comisión; esta y otras (re)asignaciones de recursos se llevarán a cabo en el marco de los presupuestos anuales. Si el Reglamento se adopta en 2022, el ejercicio de 2023 será el período transitorio, y en 2024 se alcanzará la plena operatividad.

1.7. Modo(s) de gestión previsto(s)[12]

☑ **Gestión directa** por la Comisión y cada institución, órgano y organismo de la Unión

– ☑ por sus servicios, incluido su personal en las Delegaciones de la Unión;

– ☐ por las agencias ejecutivas.

☐ **Gestión compartida** con los Estados miembros

☐ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

– ☐ terceros países o los organismos que estos hayan designado;

– ☐ organizaciones internacionales y sus agencias (especifíquense);

– ☐ el BEI y el Fondo Europeo de Inversiones;

– ☐ los organismos a que se hace referencia en los artículos 70 y 71 del Reglamento Financiero;

– ☐ organismos de Derecho público;

– ☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que cuenten con garantías financieras suficientes;

– ☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que cuenten con garantías financieras suficientes;

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la PESC, de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

– *Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.*

Observaciones

[12] Los detalles de los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

A los efectos de los procedimientos administrativos y financieros, el CERT-UE actuará bajo la autoridad de la Comisión.

Recursos adicionales derivados del proyecto de Reglamento:

La ejecución de los artículos 12 y 13 del proyecto de Reglamento conlleva la ampliación del catálogo de servicios con servicios básicos adicionales. Cuando se alcance la plena operatividad, serán necesarios los siguientes recursos adicionales (hasta el final del MFP a finales de 2027): 21 EJC y 14,05 millones EUR.

El desglose de los recursos adicionales con cargo al presupuesto para las diferentes funciones es el siguiente:

(a) Para el desempeño de las funciones en apoyo de las instituciones, los órganos y los organismos de la Unión que se detallan en el artículo 12, apartado 2, letras a), b), c) y e): 13,75 EJC y 11,275 millones EUR.

(b) Para el desempeño de las funciones que se detallan en el artículo 12, apartado 3 (contribución a la Unidad Cibernética Conjunta): 2 EJC y 381 000 EUR.

(c) Para el desempeño de las funciones que se detallan en el artículo 12, apartado 4 (cooperación estructurada con la ENISA): 0,25 EJC y 236 000 EUR.

(d) Para el desempeño de las funciones que se detallan en el artículo 12, apartado 6 (ejercicios de ciberseguridad): 0,25 EJC y 79 000 EUR.

(e) Para el desempeño de las funciones que se detallan en el artículo 12, apartado 2, letra d), y en el artículo 13 (análisis e informes sobre la ejecución del Reglamento, preparación de documentos de orientación, recomendaciones y llamamientos a la acción): 3,75 EJC y 2,079 millones EUR.

(f) Para el desempeño de las funciones de apoyo a la Secretaría del Consejo Interinstitucional de Ciberseguridad (CIIC): 1 EJC.

Resumen de los recursos actuales y transición a la plena operatividad:

En septiembre de 2021, el CERT-UE funcionó con los recursos siguientes:

- puestos permanentes y en comisión de servicios: 14 EJC,

- agentes contractuales financiados en virtud de acuerdos de nivel de servicio: 24 EJC,

- total: 38 EJC.

El presupuesto del CERT-UE en 2020 fue de 250 000 EUR con cargo al presupuesto de la Comisión y 3,5 millones EUR a través de ingresos afectados procedentes de acuerdos de nivel de servicio. Total: 3,75 millones EUR. Este fue el presupuesto total del CERT-UE, con el que se cubrieron las actividades de formación, el *hardware*, el *software*, las misiones, la labor de apoyo, los agentes contractuales y las conferencias.

Una vez que el Reglamento entre en vigor, se prevé que los recursos futuros del CERT-UE sean los siguientes:

- puestos permanentes: 34 EJC,

- agentes contractuales: 15 EJC,

- total: 49 EJC, es decir, un incremento neto de 11 EJC.

Con el cambio en la proporción entre puestos permanentes y agentes contractuales se trata de salvar el escollo que representa la contratación y la retención de profesionales de alto nivel en el ámbito de la ciberseguridad, dada su escasez en el mercado laboral.

Además, se requerirá 1 agente contractual EJC en la Dirección General de Informática de la Comisión para apoyar al CIIC (Consejo Interinstitucional de Ciberseguridad).

En total, la ejecución del Reglamento requerirá 21 EJC (20 EJC para el CERT-UE y 1 para la Dirección General de Informática de la Comisión). Estas necesidades adicionales se compensarán con una reducción paralela de 9 agentes contractuales EJC en el CERT-UE, anteriormente financiados mediante ingresos afectados procedentes de acuerdos de nivel de servicio.

El presupuesto de recursos no humanos del CERT-UE en 2024, después del período transitorio, cubrirá las funciones enumeradas en las letras a) a e) y, de acuerdo con las previsiones, se financiará como sigue:

- 8,921 millones EUR anuales procedentes de las instituciones de la Unión financiadas con cargo a la rúbrica 7 del presupuesto de la Unión,

- 2,459 millones EUR procedentes de las instituciones, los órganos y los organismos de la Unión financiados con cargo a las rúbricas 1 a 6 del presupuesto de la Unión,

- 2,670 millones EUR procedentes de las instituciones, los órganos y los organismos de la Unión autofinanciados.

- Presupuesto total del CERT-UE: 14,05 millones EUR.

Las funciones enumeradas en el artículo 12, apartado 5, no se describen en el catálogo de servicios, pues se trata de servicios facturables. Son servicios accesorios que representan importes relativamente bajos y en su mayoría revisten carácter temporal. Los costes de estos servicios se recuperarán de los beneficiarios mediante acuerdos de nivel de servicio o acuerdos escritos.

Con respecto a las contribuciones al personal del CERT-UE: las instituciones y los principales organismos de la Unión aportarán una parte equitativa que será proporcional a la parte respectiva de puestos permanentes AD de la organización. Queda por ver si el BCE y el BEI también podrán contribuir de manera equitativa mediante el envío de personal permanente en comisión de servicios.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones.

La Comisión, asistida por el CIIC y el CERT-UE, revisará periódicamente el funcionamiento del Reglamento y presentará un informe al Parlamento Europeo y al Consejo por primera vez dentro de los cuarenta y ocho meses siguientes a la entrada en vigor del Reglamento y posteriormente cada tres años.

Los datos utilizados para las revisiones procederían principalmente del CIIC y del CERT-UE. Además, en caso necesario, podrían utilizarse herramientas específicas de recopilación de datos, por ejemplo, encuestas a las instituciones, los órganos y los organismos de la Unión, la ENISA o la red de CSIRT.

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del modo / de los modos de gestión, el/los mecanismo(s) de aplicación de la financiación, las modalidades de pago y la estrategia de control propuestos

Cada institución, órgano y organismo de la Unión gestionará las acciones derivadas del Reglamento de conformidad con sus normas y reglamentos pertinentes.

La gestión administrativa y financiera de las actividades del CERT-UE se integra en la administración de la Comisión y, por tanto, se ajusta a sus mecanismos de gestión y ejecución, modalidades de pago y controles aplicables.

El auditor interno de la Comisión ejerce, con respecto al CERT-UE, las mismas facultades que tiene atribuidas en relación con los servicios de la Comisión.

2.2.2. Información relativa a los riesgos establecidos y al sistema / a los sistemas de control interno establecidos para atenuarlos

Los riesgos son muy bajos, dado que el CERT-UE ya está adscrito administrativamente a la Dirección General de Informática como grupo de trabajo de la Comisión, y el CIIC se inspira en el actual Comité de Dirección del CERT-UE. Por lo tanto, el ecosistema para la gestión financiera y el control interno ya está establecido.

2.2.3. Estimación y justificación de la relación coste/beneficio de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados»), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

Los procedimientos para la contratación pública, la gestión financiera y el control ya están establecidos y han sido sobradamente probados. La relación coste-eficacia de los controles y los niveles de riesgo de error corresponden a los de cada institución, órgano u organismo de la Unión y a los de la Comisión por lo que respecta a las actividades del CERT-UE.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas, por ejemplo, la estrategia contra el fraude.

Se aplican a las actividades del CERT-UE la gestión financiera y los sistemas de control interno de la Comisión.

Para la lucha contra el fraude, la corrupción y otros actos ilícitos, se aplican sin restricción las disposiciones del Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo, de 11 de septiembre de 2013, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF).

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

- Líneas presupuestarias existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND[13].	de países de la AELC[14]	de países candidatos [15]	de terceros países	en el sentido del artículo 21, apartado 2, letra b), del Reglamento Financiero
1 a 6	Líneas presupuestarias que cubren las contribuciones de la Unión a las agencias y los organismos descentralizados	CD	NO	NO	NO	NO
7	Líneas presupuestarias que cubren las remuneraciones del personal, los gastos informáticos y otros gastos administrativos en las distintas secciones del presupuesto de la UE	CND	NO	NO	NO	NO

- Nuevas líneas presupuestarias solicitadas

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND	de países de la AELC	de países candidatos	de terceros países	en el sentido del artículo 21, apartado 2, letra b), del Reglamento Financiero
	Ninguna		SÍ/NO	SÍ/NO	SÍ/NO	SÍ/NO

[13] CD = créditos disociados / CND = créditos no disociados.
[14] AELC: Asociación Europea de Libre Comercio.
[15] Países candidatos y, cuando proceda, países candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia financiera estimada de la propuesta en los créditos

3.2.1. Resumen de la incidencia estimada en los créditos de operaciones

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

– ☑ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	1 a 6	Rúbricas que cubren las contribuciones a las agencias y los organismos descentralizados

DG: Varias			Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
○ Créditos operativos								
Líneas presupuestarias que cubren las contribuciones de la Unión a las agencias descentralizadas (xx 10 xx xx)[16]	Compromisos	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagos	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[17]								
Línea presupuestaria		(3)						
TOTAL de los créditos en el caso de la DG: Varias	Compromisos	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Pagos	=2a+2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Según la nomenclatura presupuestaria oficial.

[17] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

○ TOTAL de los créditos de operaciones	Compromisos	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagos	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)						
TOTAL de los créditos para las RÚBRICAS 1 a 6 del marco financiero plurianual	Compromisos	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Pagos	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Si la propuesta/iniciativa afecta a más de una rúbrica operativa, repetir la sección anterior:

○ TOTAL de los créditos de operaciones (todas las rúbricas operativas)	Compromisos	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagos	(5)	2,459	2,459	2,459	2,459	2,459	12,293
TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos (todas las rúbricas operativas)		(6)						
TOTAL de los créditos para las RÚBRICAS 1 a 6 del marco financiero plurianual (Importe de referencia)	Compromisos	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Pagos	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Rúbrica del marco financiero plurianual	7	«Gastos administrativos»

Esta sección debe rellenarse mediante «los datos presupuestarios de carácter administrativo» introducidos primeramente en el anexo de la ficha de financiación legislativa (anexo V de las normas internas), que se carga en DECIDE a efectos de consulta entre servicios.

En millones EUR (al tercer decimal)

		Año **2023**	Año **2024**	Año **2025**	Año **2026**	**Año 2027**	**TOTAL**
DG: DIGIT (CERT-UE)							
○ Recursos humanos		1,184	2,126	2,754	3,225	3,225	12,514
○ Otros gastos administrativos		7,938	8,921	8,921	8,921	8,921	43,622
TOTAL DG DIGIT (CERT-UE)	Créditos	9,122	11,047	11,675	12,146	12,146	56,136

TOTAL de los créditos para la RÚBRICA 7 del marco financiero plurianual	(Total compromisos = Total pagos)	9,122	11,047	11,675	12,146	12,146	**56,136**

En millones EUR (al tercer decimal)

		Año 2023	Año 2024	Año 2025	Año 2026	Año 2027	**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 7 del marco financiero plurianual (*)	Compromisos	11,581	13,506	14,134	14,605	14,605	68,429
	Pagos	11,581	13,506	14,134	14,605	14,605	68,429

(*) Las contribuciones de las instituciones, los órganos y los organismos de la Unión autofinanciados se estiman en 2,670 millones EUR al año (total para los cinco años: 13,350 millones EUR). Las contribuciones constituirán ingresos afectados para el CERT-UE. Los cuadros anteriores solo incluyen la incidencia total estimada en el presupuesto de la Unión, pero no dichas contribuciones.

3.2.2. Resultados estimados financiados con créditos de operaciones

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados			Año **N**		Año **N+1**		Año **N+2**		Año **N+3**		Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)						**TOTAL**	
	RESULTADOS																	
⇩	Tipo[18]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º total	Coste total
OBJETIVO ESPECÍFICO N.º 1[19]…																		
- Resultado																		
- Resultado																		
- Resultado																		
Subtotal del objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2 ...																		
- Resultado																		
Subtotal del objetivo específico n.º 2																		
TOTALES																		

[18] Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[19] Tal como se describe en el punto 1.4.2. «Objetivo(s) específico(s)…»

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

– ☐ La propuesta/iniciativa no exige la utilización de créditos de carácter administrativo

– ☑ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año 2023	Año 2024	Año 2025	Año 2026	Año 2027	**TOTAL**
RÚBRICA 7 del marco financiero plurianual						
Recursos humanos						
Personal permanente (grado AD)	1,099	2,041	2,669	3,14	3,14	12,089
Agentes contractuales	0,085	0,085	0,085	0,085	0,085	0,425
Otros gastos administrativos	7,938	8,921	8,921	8,921	8,921	43,622
Subtotal para la RÚBRICA 7 del marco financiero plurianual	9,122	11,047	11,675	12,146	12,146	56,136

Al margen de la RÚBRICA 7[20] del marco financiero plurianual						
Recursos humanos						
Otros gastos de naturaleza administrativa						
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual						

TOTAL	9,122	11,047	11,675	12,146	12,146	56,136

Los créditos necesarios para recursos humanos y otros gastos de carácter administrativo se cubrirán mediante créditos de la DG ya asignados a la gestión de la acción o reasignados dentro de la DG, que se complementarán, en caso necesario, con

[20] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

3.2.3.1. Necesidades estimadas de recursos humanos

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos.

– ☑ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en equivalencia a tiempo completo

		Año 2023	Año 2024	Año 2025	Año 2026	Año 2027		
Empleos de plantilla (funcionarios y personal temporal)								
20 01 02 01 (Sede y oficinas de Representación de la Comisión)		7	13	17	20	20		
20 01 02 03 (Delegaciones)								
01 01 01 01 (Investigación indirecta)								
01 01 01 11 (Investigación directa)								
Otras líneas presupuestarias (especifíquense)								
Personal externo (en unidades de equivalente a jornada completa: EJC)[21]								
20 02 01 (AC, ENCS e INT de la «dotación global»)		1	1	1	1	1		
20 02 03 (AC, AL, ENCS, INT y JPD en las delegaciones)								
XX 01 xx **yy zz** [22]	- en la sede							
	- en las delegaciones							
01 01 01 02 (AC, ENCS e INT: Investigación Indirecta)								
01 01 01 12 (AC, ENCS e INT: Investigación directa)								
Otras líneas presupuestarias (especifíquense)								
TOTAL		**8**	**14**	**18**	**21**	**21**		

XX es la política o título en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben efectuarse:

Funcionarios y personal temporal	Los funcionarios llevarán a cabo las tareas y las actividades del CERT-UE de conformidad con el Reglamento, en particular los capítulos IV y V.
Personal externo	El agente contractual asistirá a las funciones de secretaría del Consejo Interinstitucional de Ciberseguridad.

[21] AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de agencia; JPD = joven profesional en delegación.

[22] Sublímite para el personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

3.2.4. Compatibilidad con el marco financiero plurianual vigente

La propuesta/iniciativa:

– ☑ puede ser financiada en su totalidad mediante una redistribución dentro de la rúbrica correspondiente del marco financiero plurianual (MFP).

Explíquese la reprogramación requerida, precisando las líneas presupuestarias afectadas y los importes correspondientes. Facilítese un cuadro de Excel en el caso de que se lleve a cabo una reprogramación importante.

– ☐ requiere el uso de los márgenes no asignados con cargo a la rúbrica pertinente del MFP o el uso de los instrumentos especiales tal como se define en el Reglamento del MFP.

Explíquese lo que se requiere, precisando las rúbricas y las líneas presupuestarias afectadas, los importes correspondientes y los instrumentos propuestos que van a usarse.

– ☐ requiere una revisión del MFP.

Explíquese lo que se requiere, precisando las rúbricas y las líneas presupuestarias afectadas y los importes correspondientes.

3.2.5. Contribución de terceros

La propuesta/iniciativa:

– ☑ no prevé la cofinanciación por terceros[23]

– ☐ prevé la cofinanciación por terceros que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año **N**[24]	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			Total
Especifíquese el organismo de cofinanciación								
TOTAL créditos cofinanciados								

[23] No se han estimado los ingresos afectados procedentes de la prestación esporádica de servicios a organizaciones que no sean Partes, prevista en el artículo 12, apartado 5, letra c), dado que se espera que sean marginales.

[24] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de aplicación previsto (por ejemplo: 2021). Igual para los años siguientes.

3.3. Incidencia estimada en los ingresos

– ☑ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

– ☐ en los recursos propios

– ☐ en otros ingresos

– indíquese si los ingresos se asignan a las líneas de gasto ☐

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio actual	Impacto de la propuesta/iniciativa[25]						
		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo …….								

En el caso de los ingresos afectados, especifíquense la línea o las líneas presupuestarias de gasto en la(s) que repercutan.

Otras observaciones (por ejemplo, método/fórmula utilizados para calcular la incidencia en los ingresos o cualquier otra información).

[25] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos tras la deducción del 20 % de los gastos de recaudación.