UNIÓN EUROPEA

EL PARLAMENTO EUROPEO **EL CONSEJO**

Estrasburgo, 13 de diciembre de 2023
(OR. en)

2022/0085 (COD)
LEX 2289

PE-CONS 57/1/23
REV 1

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

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

REGLAMENTO (UE, Euratom) 2023/…
DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 13 de diciembre de 2023

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[1],

[1] Posición del Parlamento Europeo de 21 de noviembre de 2023 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 8 de diciembre de 2023.

Considerando lo siguiente:

(1) En la era digital, las tecnologías de la información y la comunicación son una piedra angular de una administración europea 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 las entidades de la Unión sean más vulnerables a las ciberamenazas y los incidentes, lo que supone una amenaza para la continuidad de sus actividades y la capacidad de proteger sus datos. Aunque el mayor uso de servicios en la nube, el uso extendido de las tecnologías de la información y de las comunicaciones (TIC), el alto grado de digitalización, el trabajo a distancia y las tecnologías y posibilidades de conexión en constante evolución son características fundamentales de todas las actividades de las entidades de la Unión, la resiliencia digital aún no se ha desarrollado lo suficiente.

(2) El panorama de las ciberamenazas a las que se enfrentan las entidades de la Unión evoluciona constantemente. Las tácticas, las técnicas y los procedimientos empleados por los agentes de la amenaza también están en constante evolución, pero los principales 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 de TIC de las entidades 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 sola entidad 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, ciertos entornos de TIC de las entidades de la Unión están conectados con los entornos de TIC 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 de TIC de los Estados miembros y viceversa. El intercambio de información sobre incidentes concretos puede facilitar la detección de ciberamenazas o incidentes similares que afecten a los Estados miembros.

(4) Las entidades de la Unión son objetivos atractivos que se enfrentan a agentes de amenaza 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 madurez y ciberresiliencia, así como en cuanto a la capacidad de detectar y responder a actividades cibernéticas maliciosas. Así pues, el funcionamiento de las entidades de la Unión requiere que estas alcancen un elevado nivel común de ciberseguridad mediante la aplicación de medidas de ciberseguridad que guarden proporción con los riesgos de ciberseguridad identificados, así como mediante el intercambio de información y la colaboración.

(5) La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[1] tiene por objeto mejorar la ciberresiliencia y las capacidades de respuesta a incidentes de las entidades públicas y privadas, las autoridades y los organismos competentes y la Unión en su conjunto. Por consiguiente, es necesario garantizar que las entidades de la Unión actúen de modo homogéneo, para lo que se deben adoptar normas que sean coherentes con la Directiva (UE) 2022/2555 y que reflejen su nivel de ambición.

(6) A fin de alcanzar un elevado nivel común de ciberseguridad, es necesario que cada entidad de la Unión establezca un marco interno de gestión, gobernanza y control de riesgos en materia de ciberseguridad (en lo sucesivo, «marco») que garantice una gestión eficaz y prudente de todos los riesgos de ciberseguridad y tenga en cuenta la gestión de las crisis y la continuidad de las actividades. El marco debe establecer políticas en materia de ciberseguridad, que incluyan prioridades y objetivos, para la seguridad de los sistemas de redes y de información que constituyan la totalidad del entorno de TIC no clasificado. El marco debe basarse en un enfoque que contemple todos los riesgos y tenga por objetivo proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a sucesos como robos, incendios, inundaciones, fallos en las telecomunicaciones o en el suministro de electricidad, acceso físico no autorizado o daños a la información que posee una entidad de la Unión y a las instalaciones de tratamiento de información de la entidad, o frente a cualquier tipo de injerencia en esa información y esas instalaciones, que puedan poner en peligro la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos almacenados, transmitidos, tratados o accesibles a través de los sistemas de redes y de información.

---

[1] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80).

(7) A fin de gestionar los riesgos de ciberseguridad identificados en el marco, cada entidad de la Unión debe tomar medidas técnicas, operativas y organizativas adecuadas y proporcionadas. Dichas medidas deben abordar los ámbitos y las medidas de gestión de riesgos de ciberseguridad que se contemplan en el presente Reglamento, para reforzar la ciberseguridad de cada una de las entidades de la Unión.

(8) Cada entidad de la Unión debe reflejar en un plan de ciberseguridad los activos y los riesgos para la ciberseguridad determinados en el marco, así como las conclusiones derivadas de las evaluaciones periódicas de madurez de la ciberseguridad. El plan de ciberseguridad debe incluir las medidas adoptadas para la gestión de los riesgos de ciberseguridad.

(9) Dado que garantizar la ciberseguridad es un proceso continuo, debe revisarse periódicamente la eficacia y la idoneidad de todas las medidas adoptadas en virtud del presente Reglamento a la luz de la evolución de los riesgos de ciberseguridad, los activos y la madurez de la ciberseguridad de las entidades de la Unión. El marco debe revisarse periódicamente y al menos cada cuatro años, mientras que el plan de ciberseguridad debe revisarse cada dos años, o con más frecuencia de ser necesario, tras las evaluaciones de madurez de la ciberseguridad o tras cualquier revisión sustancial del marco.

(10) Las medidas de gestión de riesgos de ciberseguridad establecidas por las entidades de la Unión deben incluir políticas destinadas, en la medida de lo posible, a dar transparencia al código fuente, teniendo en cuenta las salvaguardias de los derechos de terceros o de entidades de la Unión. Dichas políticas deben guardar proporción con el riesgo de ciberseguridad y tener por objeto facilitar el análisis de las ciberamenazas, sin crear obligaciones de divulgación o derechos de acceso a los códigos de terceros más allá de las condiciones contractuales aplicables.

(11) Las herramientas y aplicaciones de ciberseguridad de código abierto pueden contribuir a un mayor grado de apertura. Unos estándares abiertos facilitan la interoperabilidad entre herramientas de seguridad, contribuyendo así a la seguridad de las partes interesadas. Las herramientas y aplicaciones de ciberseguridad de código abierto pueden suponer un impulso a la amplia comunidad de desarrolladores, permitiendo la diversificación de los proveedores. El código abierto puede propiciar un proceso de verificación más transparente de las herramientas relacionadas con la ciberseguridad y un proceso de detección de vulnerabilidades a cargo de la comunidad. Por consiguiente, las entidades de la Unión deben poder promover el uso de software de código abierto estándares abiertos aplicando políticas relativas al uso de datos abiertos y de código abierto como parte de la estrategia de seguridad a través de la transparencia.

(12) Las diferencias entre las entidades de la Unión exigen flexibilidad en la aplicación del presente Reglamento. Las medidas destinadas a garantizar un elevado nivel común de ciberseguridad previstas en el presente Reglamento no deben imponer ninguna obligación que interfiera directamente en el desempeño de la misión o vulnere la autonomía institucional de cada entidad de la Unión. Así pues, dichas entidades deben establecer sus propios marcos y adoptar sus propias medidas de gestión de riesgos de ciberseguridad y planes de ciberseguridad. Al aplicar dichas medidas, deben tenerse debidamente en cuenta las sinergias existentes entre las entidades de la Unión, con el fin de gestionar adecuadamente los recursos y optimizar los costes. También debe prestarse la debida atención para que las medidas no afecten negativamente a la eficiencia del intercambio de información y de la cooperación entre las entidades de la Unión y entre estas y sus homólogos de los Estados miembros.

(13) Con el fin de optimizar el uso de los recursos, el presente Reglamento debe prever la posibilidad de que dos o más entidades de la Unión con estructuras similares cooperen en la realización de las evaluaciones de madurez de la ciberseguridad de sus respectivas entidades.

(14) Para evitar imponer una carga financiera y administrativa desproporcionada a las entidades de la Unión, los requisitos de gestión de riesgos de ciberseguridad han de guardar proporción con los riesgos de ciberseguridad que presenten para los sistemas de redes y de información en cuestión, teniendo en cuenta el grado de progreso de dichas medidas. Cada entidad de la Unión ha de proponerse destinar un porcentaje adecuado de su presupuesto de TIC a la mejora de su nivel de ciberseguridad. A más largo plazo, debe perseguirse un objetivo indicativo que se sitúe en al menos el 10 %. La evaluación de madurez de la ciberseguridad debe valorar si el gasto de la entidad de la Unión en ciberseguridad guarda proporción con los riesgos de ciberseguridad que afronta. Sin perjuicio de las normas relativas al presupuesto anual de la Unión contenidas en los Tratados, en su propuesta sobre el primer presupuesto anual que se haya de adoptar tras la entrada en vigor del presente Reglamento, la Comisión debe tener en cuenta las obligaciones derivadas del presente Reglamento a la hora de evaluar las necesidades presupuestarias y de personal de las entidades de la Unión que se desprendan de sus estimaciones de gastos.

(15) Para lograr un elevado nivel común de ciberseguridad es preciso que la ciberseguridad sea supervisada por el más alto nivel de dirección de cada entidad de la Unión. El más alto nivel de dirección de la entidad de la Unión debe ser responsable de la aplicación del presente Reglamento, lo que incluye el establecimiento del marco, la adopción de medidas de gestión de riesgos de ciberseguridad y la aprobación del plan de ciberseguridad. Fomentar la cultura de la ciberseguridad, esto es, la práctica cotidiana de la ciberseguridad, es una parte integral del marco y de las medidas correspondientes de gestión de riesgos de ciberseguridad en todas las entidades de la Unión.

(16) La seguridad de los sistemas de redes y de información que manejan información clasificada de la Unión (ICUE) es esencial. Las entidades de la Unión que manejan ICUE están obligadas a aplicar los marcos normativos exhaustivos establecidos para proteger dicha información, incluidos procedimientos específicos de gobernanza, estrategia y gestión de riesgos. Es preciso que los sistemas de redes y de información que manejan ICUE cumplan normas de seguridad más estrictas que los sistemas de redes y de información no clasificados, de modo que los sistemas de redes y de información que manejan ICUE sean más resilientes a las ciberamenazas e incidentes. Por consiguiente, aun reconociendo la necesidad de un marco común a este respecto, el presente Reglamento no debe aplicarse a los sistemas de redes y de información que manejan ICUE. No obstante, si una entidad de la Unión lo solicita explícitamente, el Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE (CERT-EU, por sus siglas en inglés) debe poder prestar asistencia a dicha entidad de la Unión en relación con los incidentes en entornos de TIC clasificados.

(17) Las entidades de la Unión deben evaluar los riesgos de ciberseguridad que se derivan de sus relaciones con los proveedores y los prestadores de servicios, incluidos los proveedores de servicios de almacenamiento y tratamiento de datos o de servicios de seguridad gestionados, y adoptar las medidas adecuadas para hacer frente a esos riesgos. Las medidas de ciberseguridad han de especificarse con más detalle en directrices o recomendaciones emitidas por el CERT-EU. Al establecer medidas y directrices, es preciso tomar debidamente en consideración el estado de la tecnología y, en su caso, las normas técnicas europeas e internacionales pertinentes, así como el Derecho y las políticas pertinentes de la Unión, incluidas las evaluaciones de riesgos de ciberseguridad y las recomendaciones del Grupo de Cooperación establecido en virtud del artículo 14 de la Directiva (UE) 2022/2555, como la evaluación de riesgos coordinada de la UE de la ciberseguridad de las redes 5G y el conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G. Además, teniendo en cuenta el panorama de ciberamenazas y la importancia de fortalecer la ciberresiliencia de las entidades de la Unión, podría exigirse la certificación de los productos, servicios y procesos de las TIC pertinentes en el marco de los esquemas europeos específicos de certificación de la ciberseguridad adoptados en virtud del artículo 49 del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[1].

[1] 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).

(18) En mayo de 2011, los secretarios generales de las instituciones, órganos y organismos de la Unión decidieron crear un grupo para la preconfiguración de un equipo de CERT-EU, 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-EU 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-EU, a modo de grupo de trabajo de la Comisión con un mandato interinstitucional. En diciembre de 2017, las instituciones, los órganos y los organismos de la Unión celebraron un acuerdo interinstitucional sobre la organización y el funcionamiento del CERT-EU[1]. El presente Reglamento debe disponer un conjunto exhaustivo de normas sobre la organización, el funcionamiento y la actividad del CERT-EU. Lo dispuesto en el presente Reglamento prevalece sobre lo dispuesto en el acuerdo interinstitucional sobre la organización y el funcionamiento del CERT-EU celebrado en diciembre de 2017.

(19) Debe modificarse la denominación del CERT-EU, que pasaría a llamarse Servicio de Ciberseguridad de las instituciones, órganos y organismos de la Unión, pero, por ser ya reconocible, ha de conservarse el nombre abreviado CERT-EU.

---

[1] Acuerdo entre el Parlamento Europeo, el Consejo Europeo, el Consejo de la Unión Europea, la Comisión Europea, el Tribunal de Justicia de la Unión Europea, el Banco Central Europeo, el Tribunal de Cuentas Europeo, el Servicio Europeo de Acción Exterior, el Comité Económico y Social Europeo, el Comité Europeo de las Regiones y el Banco Europeo de Inversiones sobre la organización y el funcionamiento del Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE (CERT-UE) (DO C 12 de 13.1.2018, p. 1).

(20) Además de atribuir al CERT-EU más tareas y ampliar sus funciones, el presente Reglamento crea el Consejo Interinstitucional de Ciberseguridad (CIIC) a fin de facilitar un elevado nivel común de ciberseguridad en las entidades de la Unión. El CIIC debe desempeñar un papel exclusivo en el seguimiento y apoyo de la aplicación del presente Reglamento por parte de las entidades de la Unión, así como en la supervisión del cumplimiento de las prioridades y los objetivos generales del CERT-EU, al que debe marcar su dirección estratégica. Por consiguiente, el CIIC debe garantizar la representación de las instituciones de la Unión y contar con representantes de los órganos y organismos de la Unión a través de la Red de Agencias de la UE (EUAN, por sus siglas en inglés). La organización y el funcionamiento del CIIC deben regirse asimismo por un reglamento interno, en el que se pueden incluir disposiciones más detalladas sobre la periodicidad de las reuniones del CIIC, incluidos encuentros anuales a nivel político en los que la presencia de representantes del más alto nivel de dirección de cada miembro del CIIC permita al CIIC mantener debates sobre la estrategia y marcar la orientación estratégica del CIIC. Además, el CIIC debe tener la posibilidad de crear un comité ejecutivo que lo asista en el desempeño de su labor, y de delegar en él parte de sus funciones y facultades, especialmente en lo que atañe a las funciones que requieren conocimientos especializados de sus miembros, como, por ejemplo, la aprobación del catálogo de servicios y sus actualizaciones, las modalidades de los acuerdos de nivel de servicio, las evaluaciones de documentos e informes presentados por las entidades de la Unión al CIIC en virtud del presente Reglamento o las funciones relacionadas con la preparación de decisiones sobre las medidas de cumplimiento emitidas por el CIIC o con el seguimiento de su aplicación. El CIIC debe establecer el reglamento interno del comité ejecutivo, que ha de incluir sus funciones y facultades.

(21) El objetivo del CIIC es apoyar a las entidades de la Unión para reforzar sus respectivas posturas de ciberseguridad mediante la aplicación del presente Reglamento. Con el fin de apoyar a las entidades de la Unión, el CIIC debe orientar al director del CERT-EU, adoptar una estrategia plurianual para aumentar el nivel de ciberseguridad en las entidades de la Unión, establecer la metodología y otros aspectos de las revisiones inter pares voluntarias y facilitar la creación de un grupo informal de responsables locales de ciberseguridad, con el apoyo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés), al objeto de intercambiar mejores prácticas e información en relación con la aplicación del presente Reglamento.

(22) A fin de lograr un elevado nivel de ciberseguridad en todas las entidades de la Unión, los intereses de los órganos y organismos de la Unión que gestionan su propio entorno de TIC deben estar representados en el CIIC por tres representantes designados por la EUAN. La seguridad del tratamiento de datos personales y, por tanto, también su ciberseguridad, es una piedra angular de la protección de datos. Habida cuenta de las sinergias entre la protección de datos y la ciberseguridad, el Supervisor Europeo de Protección de Datos debe estar representado en el CIIC en su calidad de entidad de la Unión sujeta al presente Reglamento, con conocimientos específicos en el ámbito de la protección de datos, incluida la seguridad de las redes de comunicaciones electrónicas. Dada la importancia de la innovación y la competitividad en la ciberseguridad, el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad debe estar representado en el CIIC. Habida cuenta del papel de la ENISA como centro de conocimientos especializados en ciberseguridad y del apoyo que presta, así como de la importancia de la ciberseguridad de las infraestructuras y los servicios espaciales de la Unión, la ENISA y la Agencia de la Unión Europea para el Programa Espacial deben estar representadas en el CIIC. Habida cuenta de las funciones encomendadas al CERT-EU con arreglo al presente Reglamento, el presidente del CIIC debe invitar al director del CERT-EU a todas las reuniones del CIIC, excepto cuando el CIIC debata cuestiones directamente relacionadas con el director del CERT-EU.

(23) El CIIC debe hacer un seguimiento del cumplimiento del presente Reglamento y de la aplicación de las directrices, las recomendaciones y los llamamientos a la acción. Es preciso que el CIIC cuente, para las cuestiones técnicas, con el respaldo de grupos técnicos consultivos, constituidos como el CIIC considere adecuado. Dichos grupos técnicos consultivos deben trabajaren estrecha cooperación con el CERT-EU, las entidades de la Unión y, en su caso, otras partes interesadas.

(24) Cuando el CIIC constate que una entidad de la Unión no ha aplicado efectivamente el presente Reglamento, incluidas las directrices, las recomendaciones o los llamamientos a la acción emitidos en virtud del presente Reglamento, el CIIC debe tener la posibilidad, sin perjuicio de los procedimientos internos de la entidad de la Unión de que se trate, de adoptar medidas de cumplimiento. El CIIC debe aplicar las medidas de cumplimiento de forma progresiva, es decir, debe adoptar primero la medida menos severa, a saber, un dictamen motivado, y, solo en caso necesario, medidas cada vez más severas, hasta culminar con la medida más severa, que sería recomendar la suspensión temporal de los flujos de datos hacia la entidad de la Unión de que se trate. Dicha recomendación solo debe aplicarse en casos excepcionales de incumplimiento prolongado, deliberado, reiterado o grave del presente Reglamento por parte de la entidad de la Unión de que se trate.

(25) El dictamen motivado representa la medida de cumplimiento menos severa para abordar las lagunas observadas en la aplicación del presente Reglamento. El CIIC debe estar facultado para dar seguimiento al dictamen motivado con orientaciones que ayuden a la entidad de la Unión a garantizar que su marco, las medidas de gestión de riesgos de ciberseguridad, el plan de ciberseguridad y sus notificaciones cumplan lo dispuesto en el presente Reglamento, y posteriormente con una advertencia para que se subsanen en un plazo concreto las deficiencias detectadas de la entidad de la Unión. Si las deficiencias señaladas en la advertencia no se han subsanado suficientemente, el CIIC debe poder emitir una notificación motivada.

(26) El CIIC debe poder recomendar que una entidad de la Unión se someta a una auditoría. Con este fin, la entidad de la Unión debe tener la posibilidad de recurrir a su propio servicio de auditoría interna. El CIIC también debe poder solicitar que la auditoría sea realizada por un servicio de auditoría de un tercero, que puede pertenecer a un proveedor de servicios del sector privado determinado de mutuo acuerdo.

(27) En casos excepcionales de incumplimiento prolongado, deliberado, reiterado o grave del presente Reglamento por parte de una entidad de la Unión, el CIIC debe estar facultado para recomendar, como último recurso, a todos los Estados miembros y entidades de la Unión la suspensión temporal de los flujos de datos a dicha entidad de la Unión hasta que esta ponga fin al incumplimiento. Esa recomendación debe comunicarse a través de canales de comunicación adecuados y seguros.

(28) A fin de garantizar la correcta aplicación del presente Reglamento, el CIIC, si considera que un incumplimiento continuado del presente Reglamento por parte de una entidad de la Unión ha sido causada directamente por las acciones u omisiones de un miembro de su personal, incluso al más alto nivel de dirección, debe solicitar a la entidad de la Unión de que se trate que adopte las medidas oportunas, e incluso solicitar que considere la posibilidad de adoptar medidas disciplinarias de conformidad con las normas y procedimientos previstos en el Estatuto de los funcionarios de la Unión Europea y régimen aplicable a los otros agentes de la Unión Europea, establecido en el Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo[1] (en lo sucesivo, «Estatuto de los funcionarios») y cualesquiera otras normas y procedimientos aplicables.

(29) El CERT-EU debe contribuir a la seguridad del entorno de TIC de la totalidad de las entidades de la Unión. A la hora de valorar si ofrece asesoramiento o contribuciones de carácter técnico sobre cuestiones estratégicas pertinentes a petición de una entidad de la Unión, el CERT-EU debe asegurarse de que ello no impida el desempeño del resto de las tareas que se le asignan en virtud del presente Reglamento. El CERT-EU debe ejercer, respecto de las entidades de la Unión, la función equivalente a la de coordinador designado a efectos de la divulgación coordinada de las vulnerabilidades según lo dispuesto en el artículo 12, apartado 1, de la Directiva (UE) 2022/2555.

---

[1] Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo, de 29 de febrero de 1968, por el que se establece el Estatuto de los funcionarios de las Comunidades Europeas y el régimen aplicable a los otros agentes de estas Comunidades y por el que se establecen medidas específicas aplicables temporalmente a los funcionarios de la Comisión (DO L 56 de 4.3.1968, p. 1).

(30) El CERT-EU ha de apoyar la aplicación de las medidas destinadas a garantizar un elevado nivel común de ciberseguridad por medio de propuestas de directrices y recomendaciones dirigidas al CIIC o emitiendo llamamientos a la acción. EL CIIC debe aprobar dichas directrices y recomendaciones. En caso necesario, el CERT-EU ha de emitir llamamientos a la acción en los que se describan las medidas urgentes de seguridad que se insta a adoptar a las entidades de la Unión en un plazo determinado. El CIIC debe poder dar instrucciones al CERT-EU para que emita, retire o modifique una propuesta de directrices o de recomendación o un llamamiento a la acción.

(31) El CERT-EU también debe desempeñar la función que se le atribuye en la Directiva (UE) 2022/2555 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, por sus siglas en inglés), establecida en virtud del artículo 15 de dicha Directiva. Además, en consonancia con la Recomendación (UE) 2017/1584 de la Comisión[1], el CERT-EU ha de cooperar con las partes interesadas pertinentes y coordinar con ellas una respuesta. A fin de contribuir a un elevado nivel de ciberseguridad en la Unión, el CERT-EU debe compartir información específica sobre incidentes con sus homólogos de los Estados miembros. Asimismo, el CERT-EU ha de colaborar con otros homólogos públicos y privados, incluida la Organización del Tratado del Atlántico Norte, previa aprobación del CIIC.

---

1 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).

(32) El CERT-EU, en su labor de apoyo a la ciberseguridad operativa, debe usar los conocimientos especializados disponibles de la ENISA por medio de la cooperación estructurada prevista en el Reglamento (UE) 2019/881. 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-EU ha de cooperar con la ENISA en el análisis de ciberamenazas y compartir con esta periódicamente su informe sobre el panorama de amenazas.

(33) El CERT-EU debe poder cooperar e intercambiar información con las comunidades pertinentes en materia de ciberseguridad dentro de la Unión y sus Estados miembros para fomentar la cooperación operativa y favorecer que las redes existentes desarrollen todo su potencial de protección de la Unión.

(34) Dado que los servicios y las funciones del CERT-EU redundan en interés de las entidades de la Unión, cada entidad con gasto de TIC debe contribuir de manera equitativa a dichos servicios y funciones. La contribución ha de entenderse sin perjuicio de la autonomía presupuestaria de las entidades de la Unión.

(35) Muchos ciberataques se inscriben en campañas más amplias dirigidas contra grupos de entidades de la Unión o comunidades de intereses que incluyen a entidades de la Unión. A fin de facilitar la detección proactiva, la respuesta a incidentes o la adopción de medidas paliativas y la recuperación en caso de incidente, las entidades de la Unión deben notificar al CERT-EU los incidentes, las ciberamenazas, las vulnerabilidades y los cuasiincidentes y transmitir los datos técnicos necesarios para poder detectar, mitigar o responder a ciberamenazas, vulnerabilidades y cuasiincidentes que afecten a otras entidades de la Unión. Siguiendo el mismo planteamiento de la Directiva (UE) 2022/2555, se ha de exigir a las entidades de la Unión que transmitan una alerta temprana al CERT-EU en un plazo de veinticuatro horas desde el momento en que tengan conocimiento de un incidente significativo. Tal intercambio de información debería permitir al CERT-EU difundir la información al resto de entidades de la Unión, así como a los homólogos pertinentes, y ayudar así a proteger los entornos de TIC de las entidades de la Unión y de sus homólogos frente a incidentes similares.

(36) El presente Reglamento establece un planteamiento en varias etapas con respecto a la notificación de información sobre incidentes significativos con el fin de lograr el equilibrio idóneo entre, por un lado, una notificación ágil que ayude a reducir la posible propagación de incidentes significativos y permita a las entidades de la Unión buscar asistencia y, por otro, una notificación minuciosa que extraiga lecciones valiosas de cada incidente concreto y mejore con el tiempo la ciberresiliencia de entidades concretas de la Unión y contribuya a reforzar su nivel general de ciberseguridad. En este sentido, el presente Reglamento debe incluir la notificación de incidentes que, a partir de una evaluación inicial realizada por la entidad de la Unión de que se trate, podrían provocar perturbaciones operativas graves o pérdidas económicas graves a la entidad de la Unión de que se trate o podrían afectar a otras personas físicas o jurídicas causándoles perjuicios materiales o inmateriales considerables. La evaluación inicial debe tener en cuenta, entre otros aspectos, los sistemas de redes y de información afectados y, en particular, su importancia para el funcionamiento de la entidad de la Unión, la gravedad y las características técnicas de la ciberamenaza, así como las vulnerabilidades subyacentes que se estén aprovechando y la experiencia de la entidad de la Unión con incidentes similares. Indicadores como en qué medida se ve afectado el funcionamiento de la entidad de la Unión, cuánto dura un incidente o cuántas personas físicas o jurídicas se ven afectadas, podrían ser importantes a la hora de determinar si la perturbación operativa es grave.

(37) Dada la interconexión de la infraestructura y los sistemas de redes y de información de la entidad de la Unión de que se trate y del Estado miembro donde esté ubicada, resulta crucial que se informe sin demora indebida a ese Estado miembro de todo incidente significativo ocurrido en dicha entidad de la Unión. A tal efecto, la entidad de la Unión afectada debe informar a los homólogos pertinentes del Estado miembro designados o establecidos en virtud de los artículos 8 y 10 de la Directiva (UE) 2022/2555 de la aparición de un incidente significativo sobre el que está notificando al CERT-EU. Cuando el CERT-EU tenga conocimiento de un incidente significativo que acaezca en algún Estado miembro, debe notificarlo al homólogo pertinente de ese Estado miembro.

(38) Debe establecerse un mecanismo que garantice el intercambio efectivo de información, la coordinación y la cooperación entre las entidades de la Unión en caso de incidentes graves, que incluya una clara identificación de las funciones y las responsabilidades de las entidades de la Unión participantes. Con arreglo a lo que disponga el plan de gestión de cibercrisis, el representante de la Comisión en el CIIC debe ser el punto de contacto para facilitar la puesta a disposición, por parte del CIIC, de información pertinente sobre incidentes graves con la Red europea de organizaciones de enlace nacionales para las crisis de ciberseguridad (EU-CyCLONe, por sus siglas en inglés) con el fin de contribuir al conocimiento común de la situación. La función del representante de la Comisión en el CIIC como punto de contacto debe entenderse sin perjuicio de la función autónoma y diferenciada de la Comisión dentro de EU-CyCLONe en virtud del artículo 16, apartado 2, de la Directiva (UE) 2022/2555.

(39) El Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[1] es de aplicación al tratamiento de datos personales llevado a cabo en el marco del presente Reglamento. El tratamiento de datos personales podría producirse en relación con las medidas adoptadas en el contexto de la gestión de riesgos de ciberseguridad, la gestión de vulnerabilidades e incidentes, el intercambio de información sobre incidentes, ciberamenazas y vulnerabilidades, y la coordinación y cooperación en la respuesta a incidentes. Tales medidas podrían requerir el tratamiento de determinadas categorías de datos personales, como las direcciones IP, los localizadores uniformes de recursos (URL), los nombres de dominio, las direcciones de correo electrónico, las funciones organizativas del interesado, los sellos de tiempo, el asunto de los correos electrónicos o los nombres de archivo. Todas las medidas adoptadas en virtud del presente Reglamento deben cumplir el marco de protección de datos y privacidad, y las entidades de la Unión, el CERT-EU y, en su caso, el CIIC, deben adoptar todas las salvaguardias técnicas y organizativas pertinentes para garantizar que se puedan exigir responsabilidades en relación con dicho cumplimiento.

(40) De conformidad con el artículo 5, apartado 1, letra b), del Reglamento (UE) 2018/1725, el presente Reglamento establece la base jurídica para el tratamiento de datos personales por las entidades de la Unión, el CERT-EU y, en su caso, el CIIC, a efectos del desempeño de sus funciones y el cumplimiento de sus obligaciones con arreglo al presente Reglamento. El CERT-EU puede actuar como encargado del tratamiento o responsable del tratamiento atendiendo a las funciones que desempeñe en virtud del Reglamento (UE) 2018/1725.

---

[1] 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).

(41) En determinados casos, a efectos del cumplimiento de sus obligaciones con arreglo al presente Reglamento a fin de lograr un elevado nivel de ciberseguridad y, en particular, en el contexto de la gestión de vulnerabilidades e incidentes, puede ser necesario que las entidades de la Unión y el CERT-EU traten las categorías especiales de datos personales a que se refiere el artículo 10, apartado 1, del Reglamento (UE) 2018/1725. El presente Reglamento establece la base jurídica para el tratamiento de categorías especiales de datos personales por las entidades de la Unión y el CERT-EU de conformidad con el artículo 10, apartado 2, letra g), del Reglamento (UE) 2018/1725. El tratamiento de categorías especiales de datos personales con arreglo al presente Reglamento debe ser estrictamente proporcional al objetivo perseguido. Con arreglo a las condiciones establecidas en el artículo 10, apartado 2, letra g), del Reglamento (UE) 2018/1725, las entidades de la Unión y el CERT-EU solo deben poder tratar dichos datos en la medida necesaria y cuando así se disponga expresamente en el presente Reglamento. Al tratar categorías especiales de datos personales, las entidades de la Unión y el CERT-EU deben respetar el contenido esencial del derecho a la protección de datos y establecer medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses de los interesados.

(42) En virtud del artículo 33 del Reglamento (UE) 2018/1725, las entidades de la Unión y el CERT-EU, teniendo en cuenta el estado de la tecnología, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel adecuado de seguridad de los datos personales, como el derecho de acceso restringido en función del principio de la necesidad de conocer, la aplicación de los principios de registro de auditoría, la adopción de una cadena de custodia, la conservación de datos en reposo en un entorno controlado y auditable, procedimientos operativos normalizados y medidas de protección de la privacidad, como la seudonimización o el cifrado. Dichas medidas no deben aplicarse de manera que afecten a los fines de gestión de incidentes y a la integridad de las pruebas. Cuando una entidad de la Unión o el CERT-EU transfiera datos personales relacionados con un incidente, incluidas categorías especiales de datos personales, a un homólogo o socio a efectos del presente Reglamento, dichas transferencias deben cumplir lo dispuesto en el Reglamento (UE) 2018/1725. Cuando se transfieran categorías especiales de datos personales a un tercero, las entidades de la Unión y el CERT-EU deben asegurarse de que el tercero aplique medidas relativas a la protección de datos personales de un nivel equivalente al del Reglamento (UE) 2018/1725.

(43) Los datos personales tratados a efectos del presente Reglamento solo deben conservarse durante el tiempo que sea necesario de conformidad con el Reglamento (UE) 2018/1725. Las entidades de la Unión y, en su caso, el CERT-EU en calidad de responsable del tratamiento deben establecer períodos de conservación que se limiten a lo necesario para alcanzar los fines especificados. En particular, en el caso de datos personales recogidos para la gestión de incidentes, las entidades de la Unión y el CERT-EU deben diferenciar entre los datos personales recogidos para la detección de una ciberamenaza en sus entornos de TIC a fin de prevenir un incidente y los datos personales recogidos para mitigar un incidente, darle respuesta y recuperarse de él. Para la detección de una ciberamenaza es importante tener en cuenta el tiempo en que un agente de amenaza puede permanecer en un sistema sin ser detectado. Para la mitigación, la respuesta y la recuperación en caso de incidente es importante tener en cuenta si los datos personales son necesarios para investigar y gestionar un incidente recurrente o un incidente de naturaleza similar cuando pueda demostrarse una correlación.

(44) El manejo de información por el CERT-EU y las entidades de la Unión debe ajustarse a las normas aplicables a la seguridad de la información. La inclusión de la seguridad de los recursos humanos como medida de gestión de riesgos de ciberseguridad también debe atenerse a las normas aplicables.

(45) A efectos del intercambio de información, se usan marcas visibles para indicar que los destinatarios de la información deben aplicar límites al intercambio de esta, basándose, en particular, en acuerdos de confidencialidad o acuerdos informales de confidencialidad, como el protocolo TLP (del inglés «traffic light protocol») para el intercambio de información u otras indicaciones claras por parte de la fuente. El protocolo TLP debe entenderse como un medio para facilitar información sobre cualquier limitación de la difusión ulterior de la información. Se utiliza en casi todos los CSIRT y en algunos centros de intercambio y análisis de la información.

(46) El presente Reglamento debe evaluarse de forma periódica a la luz de las futuras negociaciones de marcos financieros plurianuales que permitan la adopción de nuevas decisiones en relación con el funcionamiento y la función institucional del CERT-EU, incluida la posible constitución del CERT-EU como organismo de la Unión.

(47) El CIIC, asistido por el CERT-EU, debe revisar y evaluar la aplicación 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. Dicho informe, con la contribución del CIIC, debe evaluar la conveniencia de incluir los sistemas de redes y de información que manejen ICUE en el ámbito de aplicación del presente Reglamento, en particular cuando no existan normas de seguridad de la información comunes a las entidades de la Unión.

(48) De acuerdo con el principio de proporcionalidad, para alcanzar el objetivo fundamental de lograr un elevado nivel común de ciberseguridad es necesario y conveniente regular la ciberseguridad de las entidades de la Unión. El presente Reglamento no excede de lo necesario para alcanzar el objetivo perseguido, de conformidad con lo dispuesto en el artículo 5, apartado 4, del Tratado de la Unión Europea.

(49) El presente Reglamento refleja las grandes diferencias de tamaño y capacidad entre las entidades de la Unión, también por lo que se refiere a los recursos financieros y humanos.

(50) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725, emitió su dictamen el 17 de mayo de 2022[1].

HAN ADOPTADO EL PRESENTE REGLAMENTO:

[1] DO C 258 de 5.7.2022, p. 10.

Capítulo I
Disposiciones generales

Artículo 1

Objetivo

El presente Reglamento establece medidas destinadas a lograr un elevado nivel común de ciberseguridad dentro de las entidades de la Unión en relación con:

a) el establecimiento por cada entidad de la Unión de un marco interno de gestión, gobernanza y control de riesgos en materia de ciberseguridad en virtud del artículo 6;

b) la gestión, la notificación y el intercambio de información en materia de riesgos de ciberseguridad;

c) la organización, el funcionamiento y la actividad del Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10, así como la organización, el funcionamiento y la actividad del Servicio de Ciberseguridad para las instituciones, los órganos y los organismos de la Unión (CERT-EU por sus siglas en inglés);

d) el seguimiento de la aplicación del presente Reglamento.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento se aplica a las entidades de la Unión, al Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10 y al CERT-EU.

2. El presente Reglamento se aplica sin perjuicio de la autonomía institucional prevista en los Tratados.

3. Con la excepción del artículo 13, apartado 8, el presente Reglamento no se aplica a los sistemas de redes y de información para el manejo de información clasificada de la UE (ICUE).

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «entidades de la Unión»: las instituciones, los órganos y los organismos de la Unión creados o constituidos en virtud del Tratado de la Unión Europea, el Tratado de Funcionamiento de la Unión Europea (TFUE) o el Tratado constitutivo de la Comunidad Europea de la Energía Atómica;

2) «sistemas de redes y de información»: los sistemas de redes y de información según se definen en el artículo 6, punto 1, de la Directiva (UE) 2022/2555;

3) «seguridad de los sistemas de redes y de información»: la seguridad de los sistemas de redes y de información según se define en el artículo 6, punto 2, de la Directiva (UE) 2022/2555;

4) «ciberseguridad»: la ciberseguridad según se define en el artículo 2, punto 1, del Reglamento (UE) 2019/881;

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, responsable del funcionamiento de una entidad de la Unión, y que tenga encomendada la adopción o autorización de decisiones con arreglo a los sistemas de gobernanza de alto nivel de dicha entidad de la Unión, sin perjuicio de las responsabilidades formales de otros niveles de gestión respecto al cumplimiento y a la gestión de riesgos de ciberseguridad en sus respectivas áreas de responsabilidad;

6) «cuasiincidente»: un cuasiincidente según se define en el artículo 6, punto 5, de la Directiva (UE) 2022/2555;

7) «incidente»: un incidente según se define en el artículo 6, punto 6, de la Directiva (UE) 2022/2555;

8) «incidente grave»: un incidente que cause perturbaciones que superen la capacidad de una entidad de la Unión o del CERT-EU para responder a él o que afecte significativamente a dos entidades de la Unión como mínimo;

9) «incidente de ciberseguridad a gran escala»: un incidente de ciberseguridad a gran escala según se define en el artículo 6, punto 7, de la Directiva (UE) 2022/2555;

10) «gestión de incidentes»: la gestión de incidentes según se define en el artículo 6, punto 8, de la Directiva (UE) 2022/2555;

11) «ciberamenaza»: una ciberamenaza según se define en el artículo 2, punto 8, del Reglamento (UE) 2019/881;

12) «ciberamenaza significativa»: una ciberamenaza significativa según se define en el artículo 6, punto 11, de la Directiva (UE) 2022/2555;

13) «vulnerabilidad»: una vulnerabilidad según se define en el artículo 6, punto 15, de la Directiva (UE) 2022/2555;

14) «riesgo de ciberseguridad»: un riesgo según se define en el artículo 6, punto 9, de la Directiva (UE) 2022/2555;

15) «servicio de computación en nube»: un servicio de computación en nube según se define en el artículo 6, punto 30, de la Directiva (UE) 2022/2555.

Artículo 4

Tratamiento de datos personales

1. El tratamiento de datos personales con arreglo al presente Reglamento por parte del CERT-EU, del Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10 y de las entidades de la Unión se llevará a cabo de conformidad con el Reglamento (UE) 2018/1725.

2. Cuando desempeñen funciones o cumplan obligaciones en virtud del presente Reglamento, el CERT-EU, el Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10 y las entidades de la Unión únicamente tratarán e intercambiarán datos personales en la medida necesaria y con el único fin de desempeñar dichas funciones o cumplir dichas obligaciones.

3. El tratamiento de las categorías especiales de datos personales a que se refiere el artículo 10, apartado 1, del Reglamento (UE) 2018/1725 se considerará necesario por razón de un interés público esencial de conformidad con el artículo 10, apartado 2, letra g), de dicho Reglamento. Dichos datos solo podrán tratarse en la medida necesaria para la aplicación de las medidas de gestión de riesgos de ciberseguridad a que se refieren los artículos 6 y 8 del presente Reglamento, para la prestación de servicios por el CERT-EU en virtud del artículo 13 del presente Reglamento, para el intercambio de información específica sobre incidentes en virtud del artículo 17, apartado 3, y del artículo 18, apartado 3, del presente Reglamento, para el intercambio de información en virtud del artículo 20 del presente Reglamento, para las obligaciones de notificación del artículo 21 del presente Reglamento, para la coordinación de la respuesta a incidentes y la cooperación en caso de incidentes en virtud del artículo 22 del presente Reglamento y para la gestión de incidentes graves en virtud del artículo 23 del presente Reglamento. Las entidades de la Unión y el CERT-EU, cuando actúen como responsables del tratamiento de datos, aplicarán medidas técnicas para impedir el tratamiento de categorías especiales de datos personales para otros fines y establecerán medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses de los interesados.

Capítulo II
Medidas destinadas a garantizar un elevado nivel común de ciberseguridad

Artículo 5

Aplicación de medidas

1. A más tardar el … [*ocho meses a partir de la fecha de entrada en vigor del presente Reglamento*], el Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10, previa consulta a la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) y tras recibir orientaciones del CERT-EU, emitirá directrices para las entidades de la Unión con el fin de llevar a cabo una revisión inicial de la ciberseguridad y establecer el marco interno de gestión, gobernanza y control de riesgos de ciberseguridad en virtud del artículo 6, llevar a cabo evaluaciones de madurez de la ciberseguridad en virtud del artículo 7, adoptar medidas de gestión de riesgos de ciberseguridad en virtud del artículo 8 y adoptar el plan de ciberseguridad en virtud del artículo 9.

2. Al aplicar los artículos 6 a 9, las entidades de la Unión tendrán en cuenta las directrices a que se refiere el apartado 1 del presente artículo, así como las directrices y recomendaciones pertinentes adoptadas en virtud de los artículos 11 y 14.

Artículo 6

Marco de gestión, gobernanza y control de riesgos de ciberseguridad

1. A más tardar el … [*quince meses a partir de la fecha de entrada en vigor del presente Reglamento*], cada entidad de la Unión, tras llevar a cabo un análisis inicial de la ciberseguridad, que puede consistir en una auditoría, establecerá un marco interno de gestión, gobernanza y control de riesgos de ciberseguridad (en lo sucesivo, «marco»). El más alto nivel de dirección de la entidad de la Unión supervisará y será responsable del establecimiento del marco.

2. El marco abarcará la totalidad del entorno de TIC no clasificado de la entidad de la Unión de que se trate, incluidos cualquier entorno local de TIC, de red tecnológica operativa, 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 a dichos entornos (en lo sucesivo, «entorno de TIC»). El marco se basará en un planteamiento que contemple todas las amenazas.

3. El marco garantizará un elevado nivel de ciberseguridad. El marco establecerá políticas internas de ciberseguridad, incluidos objetivos y prioridades, para la seguridad de los sistemas de redes y de información, y las funciones y responsabilidades del personal de la entidad de la Unión encargado de garantizar la aplicación efectiva del presente Reglamento. El marco incluirá asimismo mecanismos para medir la eficacia de la aplicación.

4. El marco se revisará de forma periódica, a la luz de la evolución de los riesgos de ciberseguridad, y, como mínimo, cada cuatro años. Cuando proceda y previa solicitud del Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10, el marco de una entidad de la Unión se actualizará basándose en las orientaciones del CERT-EU relativas a los incidentes detectados o las posibles deficiencias constatadas en la aplicación del presente Reglamento.

5. El más alto nivel de dirección de cada entidad de la Unión será responsable de la aplicación del presente Reglamento y supervisará el cumplimiento de sus obligaciones relacionadas con el marco.

6. Cuando proceda, y sin perjuicio de su responsabilidad en la aplicación del presente Reglamento, el más alto nivel de dirección de cada entidad de la Unión podrá delegar obligaciones específicas en virtud del presente Reglamento en altos funcionarios en el sentido del artículo 29, apartado 2, del Estatuto de los funcionarios, u otros funcionarios de nivel equivalente, dentro de la entidad de la Unión de que se trate. Independientemente de dicha delegación, el más alto nivel de dirección podrá ser considerado responsable de las infracciones del presente Reglamento en que incurra la entidad de la Unión de que se trate.

7. Cada entidad de la Unión dispondrá de mecanismos eficaces para asegurar que un porcentaje adecuado de su presupuesto de TIC se destine a la ciberseguridad. Al fijar ese porcentaje se tendrá debidamente en cuenta el marco.

8. Cada entidad de la Unión designará 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. El responsable local de ciberseguridad facilitará la aplicación del presente Reglamento e informará directamente al más alto nivel de dirección de manera periódica sobre el estado de la aplicación. Sin perjuicio de que el responsable local de ciberseguridad sea el punto de contacto en cada entidad de la Unión, la entidad de la Unión podrá delegar determinadas funciones del responsable local de ciberseguridad relativas a la aplicación del presente Reglamento en el CERT-EU mediante un acuerdo de nivel de servicio celebrado entre dicha entidad de la Unión y el CERT-EU, o se podrán compartir esas funciones entre varias entidades de la Unión. Cuando dichas funciones se deleguen en el CERT-EU, el Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10 decidirá si la prestación de ese servicio formará parte de los servicios básicos del CERT-EU, teniendo en cuenta los recursos humanos y financieros de la entidad de la Unión de que se trate. Cada entidad de la Unión comunicará al CERT-EU sin demora indebida quién haya sido designado responsable local de ciberseguridad y cualquier cambio posterior a este respecto.

El CERT-EU elaborará y actualizará una lista de los responsables locales de ciberseguridad designados.

9. Los altos funcionarios en el sentido del artículo 29, apartado 2, del Estatuto de los funcionarios, u otros funcionarios de nivel equivalente, de cada entidad de la Unión, así como todo el personal pertinente encargado de aplicar las medidas de gestión de riesgos de ciberseguridad y de cumplir las obligaciones establecidas en el presente Reglamento, recibirán periódicamente formación específica a fin de adquirir los conocimientos y las capacidades suficientes para comprender y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en las actividades de la entidad de la Unión.

Artículo 7

Evaluaciones de la madurez de la ciberseguridad

1. A más tardar el … [*dieciocho meses a partir de la fecha de entrada en vigor del presente Reglamento*], y posteriormente al menos cada dos años, cada entidad de la Unión realizará una evaluación de la madurez de ciberseguridad que englobará todos los elementos de su entorno de TIC.

2. Las evaluaciones de la madurez de la ciberseguridad se realizarán, cuando proceda, con la asistencia de un tercero especializado.

3. Las entidades de la Unión con estructuras similares podrán cooperar en la realización de las evaluaciones de la madurez de la ciberseguridad de sus respectivas entidades.

4. Previa solicitud del Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10 y con el consentimiento expreso de la entidad de la Unión de que se trate, los resultados de las evaluaciones de la madurez de la ciberseguridad podrán examinarse en el seno de dicho Consejo o en la red informal de responsables locales de ciberseguridad a fin de aprender de la experiencia adquirida y compartir buenas prácticas.

Artículo 8

Medidas de gestión de riesgos de ciberseguridad

1. Sin demora indebida y, en cualquier caso, a más tardar el … [*veinte meses a partir de la fecha de entrada en vigor del presente Reglamento*], cada entidad de la Unión adoptará, bajo la supervisión de su más alto nivel de dirección, las medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos de ciberseguridad identificados en el marco y prevenir o minimizar los efectos de los incidentes. Teniendo en cuenta el estado de la tecnología y, en su caso, las normas técnicas europeas e internacionales, dichas medidas garantizarán un nivel de seguridad de los sistemas de redes y de información en todo el entorno de TIC que guarde proporción con los riesgos de ciberseguridad existentes. Al evaluar la proporcionalidad de dichas medidas, se tendrá debidamente en cuenta el grado de exposición de la entidad de la Unión a los riesgos de ciberseguridad, el tamaño de dicha entidad y la probabilidad de que se produzcan incidentes y la gravedad de estos, incluidos sus efectos sociales, económicos e interinstitucionales.

2. Las entidades de la Unión abordarán al menos los siguientes aspectos en la aplicación de las medidas de gestión de riesgos de ciberseguridad:

a) la política de ciberseguridad, incluidas las medidas necesarias para alcanzar los objetivos y prioridades a que se refieren el artículo 6 y el apartado 3 del presente artículo;

b) las políticas de análisis de riesgos de ciberseguridad y seguridad de los sistemas de información;

c) los objetivos de la política de ciberseguridad relativos al uso de servicios de computación en nube;

d) la auditoría de ciberseguridad, cuando proceda, que podrá incluir una evaluación de los riesgos de ciberseguridad, de la vulnerabilidad y de las ciberamenazas, y las pruebas de penetración realizadas periódicamente por un proveedor privado de confianza;

e) la aplicación de las recomendaciones resultantes de las auditorías de ciberseguridad a que se refiere la letra d) por medio de actualizaciones de la ciberseguridad y de la política de ciberseguridad;

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

g) la gestión de activos, incluidos un inventario de los activos de TIC y la cartografía de las redes de TIC;

h) la seguridad en materia de recursos humanos y el control del acceso;

i) la seguridad de las operaciones;

j) la seguridad de las comunicaciones;

k) la adquisición, el desarrollo y el mantenimiento de los sistemas, incluidas las políticas de gestión y divulgación de vulnerabilidades;

l) cuando sea posible, las políticas de transparencia del código fuente;

m) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad de la Unión y sus proveedores o prestadores de servicios directos;

n) la gestión de incidentes y la cooperación con el CERT-EU, como el mantenimiento de los registros y del seguimiento de seguridad;

o) la gestión de la continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis, y

p) la promoción y el desarrollo de programas de educación, capacidades, concienciación, ejercicios y formación en materia de ciberseguridad.

A efectos del párrafo primero, letra m), las entidades de la Unión tendrán en cuenta las vulnerabilidades específicas de cada proveedor y prestador de servicios directo y la calidad general de los productos y de las prácticas de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro.

3. Las entidades de la Unión adoptarán al menos las siguientes medidas concretas de gestión de riesgos de ciberseguridad:

a) disposiciones técnicas para permitir y mantener el teletrabajo;

b) medidas concretas para avanzar hacia principios de confianza cero;

c) uso de la autenticación multifactor como norma en la totalidad de los sistemas de redes y de información;

d) uso de la criptografía y el cifrado, y en particular el cifrado de extremo a extremo, así como de la firma digital segura;

e) en su caso, implantación de comunicaciones de voz, vídeo y texto seguras, y de sistemas de comunicaciones de emergencia seguras dentro de la entidad de la Unión;

f) medidas proactivas para la detección y retirada de programas maliciosos y programas espía;

g) garantía de la seguridad de la cadena de suministro de software mediante criterios para la evaluación y desarrollo seguros de software;

h) establecimiento y adopción de programas de formación sobre ciberseguridad que guarden proporción con las tareas exigidas y las capacidades previstas para el más alto nivel de dirección y para el personal de la entidad de la Unión encargado de garantizar la aplicación efectiva del presente Reglamento;

i) formación periódica en materia de ciberseguridad para el personal;

j) cuando sea pertinente, participación en análisis de riesgos de interconexión entre entidades de la Unión;

k) introducción de mejoras en las normas de contratación pública a fin de garantizar un elevado nivel común de ciberseguridad mediante:

   i) la eliminación de los obstáculos contractuales que limitan la comunicación de información al CERT-EU, por parte de los proveedores de servicios de TIC, acerca de incidentes, vulnerabilidades y ciberamenazas,

   ii) obligaciones contractuales de notificar incidentes, vulnerabilidades y ciberamenazas, así como de disponer de mecanismos adecuados de respuesta y seguimiento de incidentes.

Artículo 9

Planes de ciberseguridad

1. A partir de las conclusiones extraídas de la evaluación de madurez de la ciberseguridad realizada en virtud del artículo 7 y teniendo en cuenta los activos y los riesgos determinados en el marco, así como las medidas de gestión de riesgos de ciberseguridad adoptadas en virtud del artículo 8, el más alto nivel de dirección de cada entidad de la Unión aprobará un plan de ciberseguridad sin demora indebida y, en cualquier caso, a más tardar el … [*veinticuatro meses a partir de la fecha de entrada en vigor del presente Reglamento*]. El objetivo del plan de ciberseguridad será aumentar el nivel global de ciberseguridad de la entidad de la Unión de que se trate y contribuir así a la mejora de un elevado nivel común de ciberseguridad dentro de las entidades de la Unión. El plan de ciberseguridad incluirá, como mínimo, las medidas de gestión de riesgos de ciberseguridad adoptadas en virtud del artículo 8. El plan de ciberseguridad se revisará cada dos años, o con más frecuencia de ser necesario, tras la evaluación de madurez de la ciberseguridad realizada en virtud del artículo 7 o tras cualquier revisión sustancial del marco.

2. El plan de ciberseguridad incluirá el plan de gestión de cibercrisis de la entidad de la Unión para los incidentes graves.

3. Cada entidad de la Unión presentará su plan de ciberseguridad final al Consejo Interinstitucional de Ciberseguridad creado en virtud del artículo 10.

Capítulo III
Consejo Interinstitucional de Ciberseguridad

Artículo 10

Consejo Interinstitucional de Ciberseguridad

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

2. El CIIC será responsable de:

   a) hacer un seguimiento de la aplicación del presente Reglamento por parte de las entidades de la Unión y apoyar dicha aplicación;

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

3. El CIIC estará compuesto por:

   a) un representante designado por cada una de las instituciones siguientes:

      i) el Parlamento Europeo,

      ii) el Consejo Europeo,

iii) el Consejo de la Unión Europea,

iv) la Comisión,

v) el Tribunal de Justicia de la Unión Europea,

vi) el Banco Central Europeo,

vii) el Tribunal de Cuentas,

viii) el Servicio Europeo de Acción Exterior,

ix) el Comité Económico y Social Europeo,

x) el Comité de las Regiones,

xi) el Banco Europeo de Inversiones,

xii) el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad,

xiii) la ENISA,

xiv) el Supervisor Europeo de Protección de Datos (SEPD),

xv) la Agencia de la Unión Europea para el Programa Espacial;

b) tres representantes designados por la EUAN, a propuesta de su Comité consultivo para las TIC, que representarán los intereses de los órganos y organismos de la Unión que gestionen sus propios entornos de TIC y que no estén incluidos en la letra a).

Las entidades de la Unión representadas en el CIIC procurarán lograr el equilibrio de género entre los representantes designados.

4. Los miembros del CIIC podrán estar asistidos por sus suplentes. El presidente podrá invitar a otros representantes de las entidades de la Unión a que se refiere el apartado 3 o de otras entidades de la Unión a asistir a las reuniones del CIIC sin derecho de voto.

5. El director del CERT-EU y los presidentes del Grupo de Cooperación, de la red de CSIRT y de EU-CyCLONe, establecidos, respectivamente, en virtud de los artículos 14, 15 y 16 de la Directiva (UE) 2022/2555, o sus suplentes, podrán participar en las reuniones del CIIC como observadores. En casos excepcionales, el CIIC podrá disponer otra cosa, de conformidad con su reglamento interno.

6. El CIIC aprobará su reglamento interno.

7. De conformidad con dicho reglamento interno, el CIIC designará a su presidente, de entre sus miembros, por un período de tres años. Su suplente pasará a ser miembro de pleno derecho del CIIC durante el mismo período.

8. El CIIC se reunirá al menos tres veces al año a iniciativa de su presidente, a petición del CERT-EU o a petición de cualquiera de sus miembros.

9. 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 del CIIC no tendrá voto, salvo que se produzca un empate, en cuyo caso podrá emitir un voto de calidad.

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

11. La Comisión prestará servicios de secretaría al CIIC y dicha secretaría rendirá cuentas al presidente del CIIC.

12. Los representantes nombrados por la EUAN transmitirán las decisiones del CIIC a los miembros de la EUAN. Todo miembro de la EUAN estará autorizado a plantear a dichos representantes o al presidente del CIIC cualquier cuestión que considere que debe ponerse en conocimiento del CIIC.

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

14. A más tardar el … [*doce meses a partir de la fecha de entrada en vigor del presente Reglamento*], y anualmente a partir de entonces, el CIIC presentará al Parlamento Europeo y al Consejo un informe en el que se detallarán los avances realizados en la aplicación del presente Reglamento y se especificará, en particular, el grado de cooperación del CERT-EU con sus homólogos en cada uno de los Estados miembros. El informe se incorporará al informe bienal sobre la situación de la ciberseguridad en la Unión adoptado en virtud del artículo 18 de la Directiva (UE) 2022/2555.

Artículo 11

Funciones del CIIC

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

a) proporcionar orientación al director del CERT-EU;

b) hacer un seguimiento y supervisar eficazmente la aplicación del presente Reglamento y apoyar a las entidades de la Unión para reforzar su ciberseguridad, incluyendo, cuando proceda, la solicitud de informes *ad hoc* a las entidades de la Unión y al CERT-EU;

c) tras un debate estratégico, adoptar una estrategia plurianual sobre el aumento del nivel de ciberseguridad de las entidades de la Unión, evaluar dicha estrategia periódicamente, en cualquier caso cada cinco años, y, de ser necesario, modificar la estrategia;

d) establecer la metodología y los aspectos organizativos para la realización de revisiones interpares voluntarias por parte de las entidades de la Unión, para aprender de las experiencias compartidas, reforzar la confianza mutua, lograr un elevado nivel común de ciberseguridad y mejorar las capacidades de ciberseguridad de las entidades de la Unión, garantizando que dichas revisiones interpares sean realizadas por expertos en ciberseguridad designados por una entidad de la Unión distinta de la entidad de la Unión objeto de revisión y que la metodología se base en el artículo 19 de la Directiva (UE) 2022/2555 y, en su caso, se adapte a las entidades de la Unión;

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

f) aprobar, sobre la base de una propuesta del director del CERT-EU, el catálogo de servicios del CERT-EU y toda actualización al respecto;

g) aprobar, sobre la base de una propuesta del director del CERT-EU, el plan financiero anual de ingresos y gastos, incluida la dotación de personal, para las actividades del CERT-EU;

h) aprobar, sobre la base de una propuesta del director del CERT-EU, las disposiciones de los acuerdos de nivel de servicio;

i) examinar y aprobar el informe anual elaborado por el director del CERT-EU sobre las actividades y la gestión de fondos del CERT-EU;

j) aprobar y hacer un seguimiento de los indicadores clave de rendimiento (KPI, por sus siglas en inglés) del CERT-EU establecidos sobre la base de una propuesta de su director;

k) aprobar los acuerdos de cooperación, los acuerdos de nivel de servicio o los contratos celebrados entre el CERT-EU y otras entidades en virtud del artículo 18;

l) adoptar directrices y recomendaciones sobre la base de una propuesta del CERT-EU de conformidad con el artículo 14 y dar instrucciones al CERT-EU para que emita, retire o modifique alguna propuesta de directrices o de recomendaciones o algún llamamiento a la acción;

m) establecer grupos de asesoramiento técnico con tareas concretas para asistir al CIIC en su labor, aprobar su mandato y nombrar a los respectivos presidentes;

n) recibir y evaluar los documentos e informes presentados por las entidades de la Unión con arreglo al presente Reglamento, como las evaluaciones de madurez de la ciberseguridad;

o) facilitar la creación de un grupo informal de responsables locales de ciberseguridad de las entidades de la Unión, apoyado por la ENISA, con el objetivo de intercambiar mejores prácticas e información en relación con la aplicación del presente Reglamento;

p) teniendo en cuenta la información proporcionada por el CERT-EU sobre los riesgos de ciberseguridad detectados y las lecciones aprendidas, supervisar la adecuación de los mecanismos de interconexión entre los entornos de TIC de las entidades de la Unión y asesorar sobre posibles mejoras;

q) establecer un plan de gestión de cibercrisis para apoyar, desde el punto de vista operativo, la gestión coordinada de los incidentes graves que afecten a las entidades de la Unión y contribuir al intercambio periódico de información pertinente, en particular en lo que se refiere a los efectos y la gravedad de los incidentes graves y las posibles formas de reducir sus efectos;

r) coordinar la adopción de los planes de gestión de cibercrisis de las distintas entidades de la Unión, a que se refiere el artículo 9, apartado 2;

s) adoptar recomendaciones en relación con la seguridad de la cadena de suministro a que se refiere el artículo 8, apartado 2, párrafo primero, letra m), teniendo en cuenta los resultados de las evaluaciones de riesgo coordinadas a escala de la Unión sobre las cadenas de suministro críticas a las que se refiere el artículo 22 de la Directiva (UE) 2022/2555 para apoyar a las entidades de la Unión en la adopción de medidas de gestión de riesgos de ciberseguridad eficaces y proporcionadas.

Artículo 12

Cumplimiento

1. El CIIC, en virtud del artículo 10, apartado 2, y del artículo 11, hará un seguimiento efectivo de la aplicación, por parte de las entidades de la Unión, del presente Reglamento y de las directrices, las recomendaciones y los llamamientos a la acción adoptados. El CIIC podrá solicitar a las entidades de la Unión la información o la documentación necesarias a tal efecto. A los efectos de la adopción de medidas de cumplimiento con arreglo al presente artículo, cuando la entidad de la Unión de que se trate esté representada directamente en el CIIC, dicha entidad de la Unión no tendrá derecho de voto.

2. Cuando el CIIC constate que una entidad de la Unión no ha aplicado de manera efectiva el presente Reglamento, o las directrices, las recomendaciones o los llamamientos a la acción emitidos en virtud del presente Reglamento, podrá, sin perjuicio de los procedimientos internos de la entidad de la Unión de que se trate y tras haber dado la oportunidad a esta última de presentar observaciones:

   a) comunicar un dictamen motivado a la entidad de la Unión de que se trate con las deficiencias observadas en la aplicación del presente Reglamento;

   b) proporcionar, después de consultar con el CERT-EU, directrices a la entidad de la Unión de que se trate para garantizar que su marco, sus medidas de gestión de riesgos de ciberseguridad, su plan de ciberseguridad y sus informes cumplan lo dispuesto en el presente Reglamento dentro de un plazo concreto;

c) formular una advertencia para subsanar las deficiencias detectadas en un plazo concreto, incluidas las recomendaciones para modificar las medidas adoptadas por la entidad de la Unión de que se trate en virtud del presente Reglamento;

d) emitir una notificación motivada a la entidad de la Unión de que se trate, en caso de que las deficiencias señaladas en una advertencia formulada con arreglo a la letra c) no se hayan subsanado suficientemente en el plazo concreto;

e) formular:

i) una recomendación de que se efectúe una auditoría, o

ii) una solicitud para que un servicio de auditoría externo efectúe una auditoría;

f) si procede, informar al Tribunal de Cuentas, en el marco de su mandato, del presunto incumplimiento;

g) formular una recomendación para que todos los Estados miembros y entidades de la Unión apliquen una suspensión temporal de los flujos de datos a la entidad de la Unión de que se trate.

A efectos del párrafo primero, letra c), los destinatarios de una advertencia se limitarán adecuadamente, cuando sea necesario ante la existencia de un riesgo de ciberseguridad.

Las advertencias y las recomendaciones formuladas en virtud del párrafo primero irán dirigidas al más alto nivel de dirección de la entidad de la Unión de que se trate.

3. Cuando el CIIC haya adoptado medidas con arreglo al apartado 2, párrafo primero, letras a) a g), la entidad de la Unión de que se trate proporcionará datos sobre las medidas y acciones emprendidas para subsanar las presuntas deficiencias detectadas por el CIIC. La entidad de la Unión de que se trate presentará dichos datos en un plazo razonable que se pactará con el CIIC.

4. Cuando el CIIC considere que una entidad de la Unión ha incumplido de forma continuada el presente Reglamento debido directamente a las acciones u omisiones de un funcionario u otro agente de la Unión, incluso al más alto nivel de dirección, el CIIC solicitará a la entidad de la Unión de que se trate que adopte las medidas oportunas, solicitándole incluso que considere la posibilidad de adoptar medidas de carácter disciplinario, de conformidad con las normas y procedimientos previstos en el Estatuto de los funcionarios y cualesquiera otras normas y procedimientos aplicables. A tal efecto, el CIIC transmitirá la información necesaria a la entidad de la Unión de que se trate.

5. Cuando las entidades de la Unión comuniquen que no están en disposición de cumplir los plazos establecidos en el artículo 6, apartado 1, y en el artículo 8, apartado 1, el CIIC podrá autorizar la prórroga de tales plazos, en casos debidamente justificados y teniendo en cuenta el tamaño de la entidad de la Unión.

Capítulo IV
CERT-EU

Artículo 13

Misión y funciones del CERT-EU

1. La misión del CERT-EU será contribuir al refuerzo de la seguridad del entorno de TIC no clasificado de las entidades de la Unión ofreciéndoles asesoramiento sobre ciberseguridad, prestándoles ayuda para prevenir, detectar, gestionar, mitigar y responder a incidentes, y recuperarse de ellos, y actuando como centro de coordinación para el intercambio de información sobre ciberseguridad y la respuesta a incidentes.

2. El CERT-EU recopilará, gestionará, analizará y compartirá con las entidades de la Unión información sobre las ciberamenazas, las vulnerabilidades y los incidentes relacionados con infraestructuras de TIC no clasificadas. Coordinará las respuestas a los incidentes a escala interinstitucional y de las entidades de la Unión, entre otros medios prestando asistencia operativa especializada o coordinando la prestación de dicha asistencia.

3. El CERT-EU desempeñará las funciones siguientes para asistir a las entidades de la Unión:

   a) les prestará apoyo en la aplicación del presente Reglamento y contribuirá a la coordinación de su aplicación a través de las medidas enumeradas en el artículo 14, apartado 1, o de informes *ad hoc* solicitados por el CIIC;

b) ofrecerá servicios ordinarios de CSIRT a las entidades de la Unión 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 17 y 18;

d) pondrá en conocimiento del CIIC todo problema relacionado con la aplicación del presente Reglamento y de las directrices, las recomendaciones y los llamamientos a la acción;

e) sobre la base de la información a que se refiere el apartado 2, contribuirá al conocimiento situacional de la Unión en el ámbito cibernético en estrecha cooperación con la ENISA;

f) coordinará la gestión de incidentes graves;

g) ejercerá, respecto de las entidades de la Unión, la función equivalente a la de coordinador designado a efectos de la divulgación coordinada de las vulnerabilidades según lo dispuesto en el artículo 12, apartado 1, de la Directiva (UE) 2022/2555;

h) proporcionará, a petición de una entidad de la Unión, una exploración proactiva y no intrusiva de los sistemas de redes y de información de acceso público de dicha entidad de la Unión.

La información a que se refiere el párrafo primero, letra e), se compartirá con el CIIC, la red de CSIRT y el Centro de Inteligencia y de Situación de la Unión Europea (EU INTCEN, por sus siglas en inglés), cuando proceda y resulte adecuado, y en función de las condiciones de confidencialidad adecuadas.

4. El CERT-EU podrá, de conformidad con los artículos 17 o 18, según proceda, cooperar con las comunidades de ciberseguridad pertinentes dentro de la Unión y sus Estados miembros, entre otros, 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 entidades de la Unión;

b) cooperación operativa en relación con la red de CSIRT, también en lo referente a la asistencia mutua;

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

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

5. Dentro de sus competencias, el CERT-EU entablará una cooperación estructurada con la ENISA 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. El CERT-EU podrá cooperar e intercambiar información con el Centro Europeo de Ciberdelincuencia de Europol.

6. El CERT-EU podrá prestar los servicios no descritos en su catálogo de servicios (en lo sucesivo, «servicios facturables») que se indican a continuación:

a) servicios de apoyo a la ciberseguridad del entorno de TIC de las entidades de la Unión distintos de los referidos en el apartado 3, sobre la base de acuerdos de nivel de servicio y en función de los recursos disponibles, en particular el seguimiento de las redes de amplio espectro, incluido el seguimiento de primera línea, veinticuatro horas al día y siete días a la semana, de las ciberamenazas muy graves;

b) servicios de apoyo a las operaciones o los proyectos de ciberseguridad de las entidades de la Unión distintos de los destinados a proteger sus entornos de TIC, sobre la base de acuerdos escritos y con la aprobación previa del CIIC;

c) previa solicitud, una exploración proactiva de los sistemas de redes y de información de la entidad de la Unión de que se trate para detectar vulnerabilidades con posibles repercusiones significativas;

d) servicios de apoyo a la seguridad del entorno de TIC de organizaciones distintas de las entidades de la Unión que cooperen estrechamente con estas, por ejemplo, mediante el desempeño de funciones o responsabilidades encomendadas con arreglo al Derecho de la Unión, en virtud de acuerdos escritos y con la aprobación previa del CIIC.

Por lo que respecta al párrafo primero, letra d), el CERT-EU podrá celebrar, con carácter excepcional, acuerdos de nivel de servicio con entidades distintas de las entidades de la Unión, previa aprobación del CIIC.

7. El CERT-EU organizará ejercicios de ciberseguridad y podrá participar en ellos o recomendar la participación en ejercicios en curso, cuando proceda en estrecha cooperación con la ENISA, con objeto de someter a prueba el nivel de ciberseguridad de las entidades de la Unión.

8. El CERT-EU podrá prestar asistencia a las entidades de la Unión en relación con incidentes en sistemas de redes y de información que manejen ICUE cuando lo soliciten expresamente las entidades de la Unión afectadas, de conformidad con sus respectivos procedimientos. La prestación de asistencia por parte del CERT-EU con arreglo al presente apartado se entenderá sin perjuicio de la normativa aplicable relativa a la protección de la información clasificada.

9. El CERT-EU informará a las entidades de la Unión sobre sus procedimientos y procesos de gestión de incidentes.

10. El CERT-EU proporcionará, con un alto grado de confidencialidad y fiabilidad, a través de los mecanismos de cooperación y canales de información adecuados, información pertinente y anonimizada sobre incidentes graves y la forma en que se gestionaron. Dicha información se incluirá en el informe a que se refiere el artículo 10, apartado 14.

11. En cooperación con el SEPD, el CERT-EU apoyará a las entidades de la Unión de que se trate cuando hagan frente a incidentes que den lugar a violaciones de la seguridad de los datos personales, sin perjuicio de las competencias y funciones del SEPD como autoridad de control en virtud del Reglamento (UE) 2018/1725.

12. El CERT-EU, a petición expresa de los departamentos temáticos de las entidades de la Unión, podrá facilitar asesoramiento o información técnicos sobre cuestiones políticas pertinentes.

Artículo 14

Directrices, recomendaciones y llamamientos a la acción

1. En apoyo de la aplicación del presente Reglamento, el CERT-EU:

a) emitirá llamamientos a la acción, en los que se describirán determinadas medidas urgentes de seguridad que se insta a las entidades de la Unión a adoptar en un plazo determinado;

b) propondrá al CIIC directrices dirigidas a la totalidad o a un subconjunto de las entidades de la Unión;

c) propondrá al CIIC recomendaciones dirigidas a entidades específicas de la Unión.

Por lo que respecta al párrafo primero, letra a), la entidad de la Unión de que se trate informará al CERT-EU, sin demora indebida tras recibir el llamamiento a la acción, de cómo se han aplicado las medidas urgentes de seguridad.

2. Las directrices y las recomendaciones podrán incluir:

a) metodologías comunes y un modelo para evaluar la madurez en materia de ciberseguridad de las entidades de la Unión, incluidos los baremos o KPI correspondientes, que sirvan de referencia en apoyo de la mejora continua de la ciberseguridad en todas las entidades de la Unión y faciliten la priorización de los ámbitos y las medidas de ciberseguridad teniendo en cuenta la posición de las entidades en materia de ciberseguridad;

b) disposiciones para la gestión de riesgos de ciberseguridad y las medidas de gestión de riesgos de ciberseguridad, o mejoras al respecto;

c) mecanismos de las evaluaciones de madurez en materia de ciberseguridad y los planes de ciberseguridad;

d) cuando proceda, el uso de tecnologías, arquitecturas y mejores prácticas de código abierto comunes con miras a la interoperabilidad y el establecimiento de normas comunes, incluido un enfoque coordinado en relación con la seguridad de las cadenas de suministro;

e) cuando proceda, información para facilitar el uso de instrumentos de contratación común para la compra a terceros de los correspondientes servicios y productos de ciberseguridad;

f) mecanismos de intercambio de información en virtud del artículo 20.

Artículo 15

Dirección del CERT-EU

1. La Comisión, tras obtener la aprobación por mayoría de dos tercios de los miembros del CIIC, nombrará al director del CERT-EU. Se consultará al CIIC en todas las fases del procedimiento de nombramiento, en particular por lo que respecta a la redacción de las convocatorias para la provisión de vacantes, el examen de las candidaturas y la designación de los comités de selección para el puesto. El procedimiento de selección, incluida la lista definitiva de candidatos preseleccionados a partir de la cual se nombrará al director del CERT-EU, garantizará una representación equitativa de cada género, teniendo en cuenta las candidaturas presentadas.

2. El director del CERT-EU será responsable del correcto funcionamiento del CERT-EU y actuará dentro de los límites de sus atribuciones y bajo la dirección del CIIC. El director del CERT-EU informará periódicamente al presidente del CIIC y presentará informes *ad hoc* al CIIC a petición de este.

3. El director del CERT-EU prestará asistencia al ordenador delegado competente en la redacción del informe anual de actividades que contenga datos financieros y de gestión, incluidos los resultados de los controles, elaborado de conformidad con el artículo 74, apartado 9, del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo[1], e informará periódicamente al ordenador delegado sobre la aplicación de las medidas respecto de las cuales se le hayan subdelegado competencias al director del CERT-EU.

4. El director del CERT-EU elaborará anualmente un plan financiero de ingresos y gastos administrativos en relación con sus actividades, una propuesta de programa de trabajo anual, una propuesta de catálogo de servicios del CERT-EU, propuestas de revisión del catálogo de servicios, propuestas de disposiciones de los acuerdos de nivel de servicio y propuestas de KPI del CERT-EU que deberá aprobar el CIIC de conformidad con el artículo 11. A la hora de revisar la lista de servicios del catálogo del CERT-EU, su director tendrá en cuenta los recursos que hayan sido asignados al CERT-EU.

---

1 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).

5. El director del CERT-EU presentará, al menos una vez al año, informes al CIIC y a su presidente sobre las actividades y el desempeño del CERT-EU durante el período de referencia, también sobre 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-EU, incluidos los informes a que se refiere el artículo 11. Dichos informes incluirán el programa de trabajo para el período siguiente, el plan financiero de ingresos y gastos, incluidas la dotación de personal, las actualizaciones previstas del catálogo de servicios del CERT-EU y una evaluación de las repercusiones esperadas que dichas actualizaciones puedan tener en términos de recursos financieros y humanos.

Artículo 16

Aspectos financieros y de personal

1. El CERT-EU se integrará en la estructura administrativa de alguna dirección general de la Comisión con el fin de beneficiarse de las estructuras de apoyo administrativo, financiero y contable de la Comisión, manteniendo al mismo tiempo su condición de proveedor de servicios interinstitucional autónomo para todas las entidades de la Unión. La Comisión informará al CIIC sobre la sede administrativa del CERT-EU y sobre cualquier modificación al respecto. La Comisión revisará los acuerdos administrativos relacionados con el CERT-EU de forma periódica y, en cualquier caso, antes del establecimiento de cualquier marco financiero plurianual en virtud del artículo 312 del TFUE, a fin de permitir la adopción de las medidas adecuadas. La revisión incluirá la posibilidad de constituir el CERT-EU en organismo de la Unión.

2. En la aplicación de los procedimientos administrativos y financieros, el director del CERT-EU actuará bajo la autoridad de la Comisión y bajo la supervisión del CIIC.

3. Las funciones y actividades del CERT-EU, incluidos los servicios que preste en virtud del artículo 13, apartados 3, 4, 5 y 7, y el artículo 14, apartado 1, a las entidades 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-EU se detallarán en una nota a pie de página de la plantilla de personal de la Comisión.

4. Las entidades de la Unión distintas de las mencionadas en el apartado 3 del presente artículo efectuarán una contribución financiera anual al CERT-EU para cubrir los servicios prestados por este de conformidad con dicho apartado. Las contribuciones se basarán en orientaciones del CIIC y serán pactadas entre cada entidad de la Unión y el CERT-EU 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 del presente artículo como ingresos afectados internos, de conformidad con lo previsto en el artículo 21, apartado 3, letra c), del Reglamento (UE, Euratom) 2018/1046.

5. Los costes de los servicios previstos en el artículo 13, apartado 6, se recuperarán de las entidades de la Unión que reciban los servicios del CERT-EU. Los ingresos se asignarán a las líneas presupuestarias con las que se cubran los costes.

Artículo 17

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

1. El CERT-EU cooperará e intercambiará información, sin demora indebida, con sus homólogos de los Estados miembros, en particular los CSIRT designados o establecidos en virtud del artículo 10 de la Directiva (UE) 2022/2555, o, cuando proceda, las autoridades competentes y los puntos de contacto únicos designados o establecidos en virtud del artículo 8 de dicha Directiva, en lo concerniente a incidentes, ciberamenazas, vulnerabilidades y cuasiincidentes, posibles contramedidas, así como mejores prácticas y cualesquiera cuestiones pertinentes para la mejora de la protección del entorno de TIC de las entidades de la Unión, entre otros, a través de la red de CSIRT establecida en virtud del artículo 15 de la Directiva (UE) 2022/2555. El CERT-EU prestará apoyo a la Comisión en EU-CyCLONe, establecida en virtud del artículo 16 de la Directiva (UE) 2022/2555 sobre la gestión coordinada de los incidentes de ciberseguridad a gran escala y las crisis.

2. Cuando el CERT-EU tenga conocimiento de algún incidente significativo que se produzca en el territorio de un Estado miembro, lo notificará, sin demora, al homólogo pertinente de ese Estado miembro, de conformidad con el apartado 1.

3. Siempre que los datos personales estén protegidos de conformidad con el Derecho de la Unión aplicable en materia de protección de datos, el CERT-EU intercambiará, sin demora indebida, información específica pertinente sobre incidentes con sus homólogos de los Estados miembros para facilitar la detección de ciberamenazas o incidentes similares, o para contribuir al análisis de un incidente, sin la autorización de la entidad de la Unión afectada. El CERT-EU intercambiará información específica sobre incidentes en la que se revele la identidad del objetivo del incidente únicamente si concurre alguna de las condiciones siguientes:

a) la entidad de la Unión afectada dé su consentimiento;

b) cuando la entidad de la Unión afectada no dé su consentimiento tal como dispone la letra a), pero la divulgación de la identidad de la entidad de la Unión afectada mejore la probabilidad de evitar o mitigar incidentes en otros lugares;

c) la entidad de la Unión afectada ya haya hecho público que se vio afectada.

Las decisiones de intercambiar información específica sobre incidentes que revele la identidad del objetivo del incidente en virtud del párrafo primero, letra b), serán aprobadas por el director del CERT-EU. Antes de tomar dicha decisión, el CERT-EU se pondrá en contacto por escrito con la entidad de la Unión afectada, para explicar claramente cómo la revelación de su identidad ayudaría a evitar o mitigar incidentes en otros lugares. El director del CERT-EU proporcionará la explicación y solicitará expresamente a la entidad de la Unión afectada que declare si da su consentimiento en un plazo determinado. El director del CERT-EU también informará a la entidad de la Unión afectada de que, a la luz de la explicación proporcionada, se reserva el derecho a revelar la información incluso sin consentimiento. Se informará a la entidad de la Unión afectada antes de revelar la información.

Artículo 18

Cooperación del CERT-EU con otros homólogos

1. El CERT-EU podrá cooperar con otros homólogos pertenecientes a la Unión distintos de los mencionados en el artículo 17, que deban cumplir los requisitos de la Unión en materia de ciberseguridad, incluidos los de sectores específicos de la industria, 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, el CERT-EU solicitará la aprobación previa del CIIC en función de cada caso. Cuando el CERT-EU establezca una cooperación con dichos homólogos, informará a los homólogos pertinentes de los Estados miembros a que se refiere el artículo 17, apartado 1, del Estado miembro en el que esté ubicado el homólogo. Cuando proceda y resulte apropiado, dicha cooperación y sus condiciones, incluidas las relativas a la ciberseguridad, la protección de datos y el manejo de la información, se establecerán en acuerdos de confidencialidad específicos, como contratos o acuerdos administrativos. Los acuerdos de confidencialidad no requerirán la aprobación previa del CIIC, pero sí se informará a su presidente. En caso de necesidad urgente e inminente de intercambiar información sobre ciberseguridad en interés de las entidades de la Unión o de otra parte, el CERT-EU podrá hacerlo con una entidad cuya competencia, capacidad y experiencia específicas sean necesarios justificadamente para prestar asistencia ante tal necesidad urgente e inminente, incluso si el CERT-EU no cuenta con un acuerdo de confidencialidad con dicha entidad. En tales casos, el CERT-EU informará inmediatamente al presidente del CIIC e informará al CIIC mediante informes periódicos o reuniones.

2. El CERT-EU podrá cooperar con socios, como entidades comerciales, incluidas entidades de sectores específicos de la industria, organizaciones internacionales, entidades nacionales no pertenecientes a la Unión o expertos individuales, con el fin de recopilar información sobre ciberamenazas, cuasiincidentes, vulnerabilidades y posibles contramedidas generales y específicas. A los efectos de una cooperación más amplia con dichos socios, el CERT-EU solicitará la aprobación previa del CIIC en función de cada caso.

3. El CERT-EU podrá proporcionar, con el consentimiento de la entidad de la Unión afectada por un incidente y siempre que exista un acuerdo o contrato de confidencialidad con el homólogo o socio pertinente, información relacionada con el incidente específico a los homólogos o socios a que se refieren los apartados 1 y 2 con el único fin de contribuir a su análisis.

Capítulo V

Obligaciones de cooperación e información

Artículo 19

Manejo de la información

1. Las entidades de la Unión y el CERT-EU respetarán la obligación de secreto profesional de conformidad con el artículo 339 del TFUE u otros marcos equivalentes aplicables.

2. Toda solicitud de acceso del público a documentos que obren en poder del CERT-EU se atendrá al Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo[1], lo que se aplica también a la obligación, prevista en dicho Reglamento, de consultar a otras entidades de la Unión o, si procede, a los Estados miembros cuando la solicitud se refiera a sus documentos.

3. El manejo de información por las entidades de la Unión y el CERT-EU cumplirá las normas aplicables a la seguridad de la información.

Artículo 20

Mecanismos de intercambio de información sobre ciberseguridad

1. De forma voluntaria, las entidades de la Unión podrán notificar y proporcionar al CERT-EU información sobre incidentes, ciberamenazas, cuasiincidentes y vulnerabilidades que les afecten. El CERT-EU velará por disponer de medios eficaces de comunicación, con un alto grado de trazabilidad, confidencialidad y fiabilidad, al objeto de facilitar el intercambio de información con las entidades de la Unión. Al tratar las notificaciones, el CERT-EU podrá dar prioridad a la tramitación de notificaciones obligatorias sobre la de notificaciones voluntarias. Sin perjuicio de lo dispuesto en el artículo 12, la notificación voluntaria no dará lugar a la imposición de obligaciones adicionales a la entidad de la Unión notificante a las que no estaría sujeta de no haber presentado dicha notificación.

---

[1] 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).

2. A fin de desempeñar su misión y las funciones atribuidas en virtud del artículo 13, el CERT-EU podrá solicitar a las entidades de la Unión que le proporcionen información acerca de sus respectivos inventarios de sistemas de TIC, incluida información sobre ciberamenazas, cuasiincidentes, vulnerabilidades, indicadores de compromiso, alertas de ciberseguridad y recomendaciones relativas a la configuración de las herramientas de ciberseguridad para detectar incidentes. La entidad de la Unión objeto de la solicitud transmitirá sin demora indebida la información solicitada, así como toda actualización posterior de la información.

3. El CERT-EU podrá intercambiar con las entidades de la Unión información específica sobre incidentes en la que se revele la identidad de la entidad de la Unión afectada por el incidente, siempre que esta dé su consentimiento. Cuando una entidad de la Unión deniegue su consentimiento, comunicará al CERT-EU los motivos que justifiquen su decisión.

4. Previa solicitud, las entidades de la Unión compartirán información con el Parlamento Europeo y el Consejo sobre la finalización de los planes de ciberseguridad.

5. El CIIC o el CERT-EU, según proceda, compartirán, previa solicitud, directrices, recomendaciones y llamamientos a la acción con el Parlamento Europeo y el Consejo.

6. Las obligaciones de intercambio de información establecidas en el presente artículo no se exigirán respecto de:

   a) la ICUE;

b) la información cuya distribución ulterior haya sido excluida mediante una marca visible, a menos que se haya autorizado expresamente su intercambio con el CERT-EU.

Artículo 21

Obligaciones de notificación

1. Un incidente se considerará significativo si:

a) ha causado o puede causar graves perturbaciones operativas o pérdidas económicas para la entidad de la Unión afectada;

b) ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

2. Las entidades de la Unión presentarán al CERT-EU:

a) sin demora indebida, y en cualquier caso en el plazo de veinticuatro horas desde que se haya tenido constancia del incidente significativo, una alerta temprana en la que se indicará, cuando proceda, si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada o puede tener repercusiones entre entidades o repercusiones transfronterizas;

b) sin demora indebida, y en cualquier caso en el plazo de setenta y dos horas desde que se haya tenido constancia del incidente significativo, una notificación del incidente en la que se actualizará, cuando proceda, la información a que se refiere la letra a) y se expondrá una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles;

c) a petición del CERT-EU, un informe intermedio con las actualizaciones pertinentes sobre la situación;

d) un informe final, a más tardar un mes después de presentar la notificación del incidente a que se refiere la letra b), en el que se recojan, entre otros, los siguientes elementos:

   i) una descripción detallada del incidente, incluidos su gravedad y repercusiones,

   ii) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente,

   iii) las medidas paliativas aplicadas y en curso,

   iv) cuando proceda, las repercusiones transfronterizas o entre entidades del incidente;

e) en el caso de que el incidente esté ocurriendo en el mismo momento de la presentación del informe final mencionado en la letra d), un informe de la situación en ese momento y un informe final en el plazo de un mes a partir de que se haya gestionado el incidente.

3. Las entidades de la Unión informarán, sin demora indebida, y en cualquier caso en el plazo de veinticuatro horas desde la constatación de un incidente significativo, a los homólogos pertinentes a los que se refiere el artículo 17, apartado 1, del Estado miembro en el que estén ubicadas, de que se ha producido un incidente significativo.

4. Las entidades de la Unión notificarán, entre otras cosas, cualquier información que permita al CERT-EU determinar las repercusiones entre entidades, las repercusiones en el Estado miembro de acogida o las repercusiones transfronterizas después de un incidente significativo. Sin perjuicio de lo dispuesto en el artículo 12, el mero acto de notificar no incrementará la responsabilidad de la entidad de la Unión.

5. Cuando proceda, las entidades de la Unión comunicarán, sin demora indebida, a los usuarios de los sistemas de redes y de información afectados o de otros componentes del entorno de TIC que puedan verse afectados por un incidente significativo o una ciberamenaza significativa y que, en su caso, deban adoptar medidas paliativas, las medidas o soluciones que pueden adoptar en respuesta al incidente o la amenaza. Cuando proceda, las entidades de la Unión informarán de la propia ciberamenaza significativa a dichos usuarios.

6. Cuando un incidente significativo o una ciberamenaza significativa afecte a un sistema de redes y de información o a un componente del entorno de TIC de una entidad de la Unión de la que se tenga conocimiento que está conectada con el entorno de TIC de otra entidad de la Unión, el CERT-EU emitirá la correspondiente alerta de ciberseguridad.

7. A petición del CERT-EU, las entidades de la Unión le proporcionarán, sin demora indebida, la información digital generada por el uso de dispositivos electrónicos implicados en sus respectivos incidentes. El CERT-EU podrá proporcionar más detalles sobre el tipo de información que necesita a efectos del conocimiento situacional y la respuesta a incidentes.

8. El CERT-EU presentará al CIIC, a la ENISA, al EU INTCEN y a la red de CSIRT, cada tres meses, un informe de síntesis que contendrá datos anonimizados y agregados sobre los incidentes significativos, los incidentes, las ciberamenazas, los cuasiincidentes y las vulnerabilidades en virtud del artículo 20 y los incidentes significativos notificados en virtud del apartado 2 del presente artículo. El informe de síntesis se incorporará al informe bienal sobre la situación de la ciberseguridad en la Unión, adoptado en virtud del artículo 18 de la Directiva (UE) 2022/2555.

9. A más tardar el … [*seis meses a partir de la fecha de entrada en vigor del presente Reglamento*], el CIIC emitirá directrices o recomendaciones que especifiquen con mayor detalle los mecanismos, el formato y el contenido de las notificaciones previstas en el presente artículo. Al preparar dichas directrices o recomendaciones, el CIIC tendrá en cuenta cualquier acto de ejecución adoptado en virtud del artículo 23, apartado 11, de la Directiva (UE) 2022/2555 en el que se especifique el tipo de información, el formato y el procedimiento de las notificaciones. El CERT-EU difundirá los detalles técnicos pertinentes a fin de facilitar la detección proactiva, la respuesta a incidentes o la adopción de medidas paliativas por parte de las entidades de la Unión.

10. Las obligaciones de notificación establecidas en el presente artículo no se exigirán respecto de:

a) la ICUE;

b) la información cuya distribución ulterior haya sido excluida mediante una marca visible, a menos que se haya autorizado expresamente su intercambio con el CERT-EU.

Artículo 22

Coordinación de la respuesta a incidentes y cooperación

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

a) las entidades de la Unión;

b) los homólogos a que se refieren los artículos 17 y 18.

2. El CERT-EU, cuando proceda en estrecha cooperación con la ENISA, facilitará la coordinación de la respuesta a incidentes entre las entidades de la Unión, incluyendo lo siguiente:

a) contribución a una comunicación externa coherente;

b) apoyo mutuo, como el intercambio de información pertinente para las entidades de la Unión, o la prestación de asistencia, cuando proceda directamente *in situ*;

c) uso óptimo de los recursos operativos;

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

3. El CERT-EU, en estrecha cooperación con la ENISA, apoyará a las entidades de la Unión en lo que respecta al conocimiento situacional en materia de incidentes, ciberamenazas, vulnerabilidades y cuasiincidentes, y compartirá información sobre los avances en materia de ciberseguridad.

4. A más tardar el … [*doce meses a partir de la fecha de entrada en vigor del presente Reglamento*], el CIIC adoptará, sobre la base de una propuesta del CERT-EU, directrices o recomendaciones sobre la coordinación de la respuesta a incidentes y la cooperación en caso de incidentes significativos. Cuando se sospeche que un incidente es de carácter delictivo, el CERT-EU ofrecerá asesoramiento sobre el modo de notificar el incidente a las autoridades policiales, sin demora indebida.

5. Previa solicitud específica de un Estado miembro y tras la aprobación de las entidades de la Unión de que se trate, el CERT-EU podrá recurrir a expertos de la lista a que se refiere el artículo 23, apartado 4, para contribuir a la respuesta a un incidente grave que tenga repercusiones en dicho Estado miembro, o a un incidente de ciberseguridad a gran escala, de conformidad con el artículo 15, apartado 3, letra g), de la Directiva (UE) 2022/2555. Las normas específicas sobre el acceso y el recurso a expertos técnicos de las entidades de la Unión serán aprobadas por el CIIC sobre la base de una propuesta del CERT-EU.

Artículo 23

Gestión de incidentes graves

1. Con el fin de apoyar desde el punto de vista operativo la gestión coordinada de incidentes graves que afecten a entidades de la Unión y de contribuir al intercambio periódico de información pertinente entre las entidades de la Unión y con los Estados miembros, el CIIC establecerá un plan de gestión de cibercrisis, en virtud del artículo 11, letra q), basado en las actividades a que se refiere el artículo 22, apartado 2, en estrecha cooperación con el CERT-EU y con la ENISA. El plan de gestión de cibercrisis incluirá al menos los elementos siguientes:

   a) los mecanismos para la coordinación y el flujo de información entre las entidades de la Unión para la gestión de incidentes graves en el plano operativo;

   b) procedimientos operativos normalizados comunes (SOPs por sus siglas en inglés);

   c) una taxonomía común de la gravedad de los incidentes graves y los elementos causantes de crisis;

   d) ejercicios periódicos;

   e) los canales de comunicación seguros que han de utilizarse.

2. Con arreglo al plan de gestión de cibercrisis establecido en virtud del apartado 1 del presente artículo y sin perjuicio de lo dispuesto en el artículo 16, apartado 2, párrafo primero, de la Directiva (UE) 2022/2555, el representante de la Comisión en el CIIC será el punto de contacto para el intercambio de información pertinente sobre incidentes graves con EU-CyCLONe.

3. El CERT-EU coordinará la gestión de los incidentes graves entre las entidades de la Unión. Llevará un inventario de los conocimientos técnicos disponibles que serían necesarios para la respuesta a incidentes en caso de incidentes graves y asistirá al CIIC a coordinar los planes de gestión de cibercrisis de las entidades de la Unión para los incidentes graves a que se refiere el artículo 9, apartado 2.

4. Las entidades de la Unión contribuirán al inventario de conocimientos técnicos proporcionando una lista, que actualizarán anualmente, en la que figuren los expertos disponibles en sus respectivas organizaciones, junto con una descripción detallada de sus capacidades técnicas específicas.

Capítulo VI
Disposiciones finales

Artículo 24

Reasignación presupuestaria inicial

Para garantizar un funcionamiento correcto y estable del CERT-EU, la Comisión podrá proponer la reasignación a su presupuesto de recursos de personal y financieros, para su utilización en las operaciones del CERT-EU. La reasignación será efectiva al mismo tiempo que el primer presupuesto anual de la Unión adoptado tras la entrada en vigor del presente Reglamento.

Artículo 25

Revisión

1. A más tardar el … [*doce meses a partir de la fecha de entrada en vigor del presente Reglamento*], y anualmente a partir de entonces, el CIIC, asistido por el CERT-EU, informará a la Comisión acerca de la aplicación del presente Reglamento. El CIIC podrá formular recomendaciones a la Comisión para que revise el presente Reglamento.

2. A más tardar el … [*36 meses a partir de la fecha de entrada en vigor del presente Reglamento*], y posteriormente cada dos años, la Comisión evaluará la aplicación del presente Reglamento y la experiencia adquirida tanto de tipo estratégico como operativo, e informará de ello al Parlamento Europeo y al Consejo.

El informe a que se refiere el párrafo primero del presente apartado incluirá la revisión prevista en el artículo 16, apartado 1, sobre la posibilidad de constituir el CERT-EU en organismo de la Unión.

3. A más tardar el … [*cinco años a partir de la fecha de entrada en vigor del presente Reglamento*], la Comisión evaluará el funcionamiento del presente Reglamento y presentará un informe al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La Comisión evaluará asimismo la conveniencia de incluir sistemas de redes y de información que manejen ICUE en el ámbito de aplicación del presente Reglamento, teniendo en cuenta otros actos legislativos de la Unión aplicables a dichos sistemas. El informe irá acompañado, en su caso, de una propuesta legislativa.

Artículo 26

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 Estrasburgo, el

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