Parlamento Europeo
2019-2024

Comisión de Asuntos Constitucionales

2022/0085(COD)

31.1.2023

OPINIÓN

de la Comisión de Asuntos Constitucionales

para la Comisión de Industria, Investigación y Energía

sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión (COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Ponente de opinión: Markéta Gregorová

PA_Legam

BREVE JUSTIFICACIÓN

Durante los últimos años, la digitalización y el continuo progreso tecnológico han llevado a las instituciones, los órganos y los organismos de la Unión Europea a enfrentarse a un número creciente de amenazas para la ciberseguridad. La pandemia de COVID-19 ha agravado la situación, entre otras cosas debido a la generalización del teletrabajo, y los sofisticados ataques procedentes de una amplia variedad de fuentes han seguido aumentando.

En la actualidad, el panorama de la ciberseguridad, en concreto en materia de gobernanza, ciberhigiene, capacidad general y madurez, difiere considerablemente entre las instituciones, los órganos y los organismos de la Unión, lo que supone un nuevo obstáculo para una administración europea abierta, eficiente e independiente.

Por lo tanto, la ponente estima que es necesario sentar unas bases para que las instituciones, los órganos y los organismos de la Unión establezcan unos sistemas y requisitos comunes de ciberseguridad. De esta manera, la ciberseguridad evolucionaría en la misma dirección y se potenciaría la eficiencia y la independencia de la administración europea.

La ponente considera, además, que un marco de seguridad sólido y coherente es esencial para proteger a todo el personal, los datos, las redes de comunicación, los sistemas de información y los procesos de toma de decisiones de la Unión, contribuyendo así a su funcionamiento democrático. Una cultura de seguridad reforzada de las instituciones, los órganos y los organismos de la Unión también ayudaría a Europa a adaptarse a la era digital y a construir una economía preparada para el futuro al servicio de las personas.

ENMIENDAS

La Comisión de Asuntos Constitucionales pide a la Comisión de Industria, Investigación y Energía, competente para el fondo, que tome en consideración las siguientes enmiendas:

Enmienda 1

Propuesta de Reglamento
Considerando 1

Texto de la Comisión	*Enmienda*
(1) En la era digital, las tecnologías de la información y la comunicación son una piedra angular para una administración de la Unión abierta, eficiente e independiente. La constante evolución tecnológica y la complejidad e interconexión crecientes de los sistemas digitales amplifican los riesgos relacionados con la ciberseguridad y hacen	(1) En la era digital, las tecnologías de la información y la comunicación son una piedra angular para una administración de la Unión abierta, eficiente e independiente. La constante evolución tecnológica y la complejidad e interconexión crecientes de los sistemas digitales amplifican los riesgos relacionados con la ciberseguridad y hacen

que la administración de la Unión sea más vulnerable a las ciberamenazas y los incidentes, lo que, en última instancia, supone una amenaza para la continuidad de las actividades de la administración y su capacidad para proteger sus datos. El mayor recurso a los servicios en la nube, el uso extendido de las tecnologías de la información, un alto grado de digitalización, el trabajo a distancia y unas tecnologías y posibilidades de conexión en constante evolución son, hoy en día, características fundamentales de todas las actividades de las entidades de la administración de la Unión; sin embargo, la resiliencia digital aún no se ha desarrollado lo suficiente.	que la administración de la Unión sea más vulnerable a las ciberamenazas y los incidentes, lo que, en última instancia, supone una amenaza para la continuidad de las actividades de la administración y su capacidad para proteger sus datos. El mayor recurso a los servicios en la nube, el uso extendido de las tecnologías de la información ***y de las comunicaciones (TIC)***, un alto grado de digitalización, el trabajo a distancia y unas tecnologías y posibilidades de conexión en constante evolución son, hoy en día, características fundamentales de todas las actividades de las entidades de la administración de la Unión; sin embargo, la resiliencia digital aún no se ha desarrollado lo suficiente.

Justificación

La propuesta de la Comisión menciona «tecnologías de la información» donde debería decir «tecnologías de la información y de las comunicaciones», que es el término estándar en la Directiva SRI 2 y el Reglamento sobre la Ciberseguridad de la UE.

Enmienda 2

Propuesta de Reglamento
Considerando 2

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

expuestas que no dejan de expandirse y aprovechan rápidamente las vulnerabilidades.	de ataque expuestas que no dejan de expandirse y aprovechan rápidamente las vulnerabilidades.

Enmienda 3

Propuesta de Reglamento
Considerando 3

Texto de la Comisión	*Enmienda*
(3) Los entornos ***informáticos*** de las instituciones, los órganos y los organismos de la Unión se caracterizan por las interdependencias, los flujos de datos integrados y la estrecha colaboración entre sus usuarios. Debido a esa interconexión, toda perturbación, aunque en un primer momento se limite a una institución, un órgano o un organismo de la Unión, puede tener un efecto en cascada más amplio y acabar perjudicando, de manera grave y duradera, al resto. Además, en algunos casos, los entornos ***informáticos*** de las instituciones, los órganos o los organismos están conectados con los de los Estados miembros, de manera que un incidente en una entidad de la Unión puede suponer un riesgo para la ciberseguridad de los entornos ***informáticos*** de los Estados miembros y viceversa.	(3) Los entornos ***de las TIC*** de las instituciones, los órganos y los organismos de la Unión se caracterizan por las interdependencias, los flujos de datos integrados y la estrecha colaboración entre sus usuarios. Debido a esa interconexión, toda perturbación, aunque en un primer momento se limite a una institución, un órgano o un organismo de la Unión, puede tener un efecto en cascada más amplio y acabar perjudicando, de manera grave y duradera, al resto. Además, en algunos casos, los entornos ***de las TIC*** de las instituciones, los órganos o los organismos están conectados con los de los Estados miembros, de manera que un incidente en una entidad de la Unión puede suponer un riesgo para la ciberseguridad de los entornos ***de las TIC*** de los Estados miembros y viceversa.

Enmienda 4
Propuesta de Reglamento
Considerando 4

Texto de la Comisión	*Enmienda*
(4) Las instituciones, los órganos y los organismos de la Unión son blancos atractivos y, como tales, se enfrentan a agentes de riesgo altamente cualificados y dotados de amplios recursos, pero también a otro tipo de amenazas. Por otra parte, hay grandes diferencias de una entidad a otra en cuanto al grado de ciberresiliencia y su madurez, así como en cuanto a la	(4) Las instituciones, los órganos y los organismos de la Unión son blancos atractivos y, como tales, se enfrentan a agentes de riesgo altamente cualificados y dotados de amplios recursos, pero también a otro tipo de amenazas. Por otra parte, hay grandes diferencias de una entidad a otra en cuanto al grado de ciberresiliencia y su madurez, así como en cuanto a la

capacidad para detectar y responder a actividades informáticas malintencionadas. Así pues, para el funcionamiento de la administración europea, es necesario que las instituciones, los órganos y los organismos de la Unión alcancen un elevado nivel común de ciberseguridad a través de un código básico de ciberseguridad (normas mínimas de ciberseguridad a las que deberán ajustarse tanto las redes y los sistemas de información como sus operadores y usuarios con el fin de ***minimizar*** los riesgos relacionados con la ciberseguridad), así como mediante el intercambio de información y la colaboración.

capacidad para detectar y responder a actividades informáticas malintencionadas. Así pues, para el funcionamiento de la administración europea, es necesario que las instituciones, los órganos y los organismos de la Unión alcancen un elevado nivel común de ciberseguridad a través de un código básico de ciberseguridad (normas mínimas ***comunes*** de ciberseguridad a las que deberán ajustarse tanto las redes y los sistemas de información como sus operadores y usuarios con el fin de ***limitar*** los riesgos relacionados con la ciberseguridad), así como mediante el intercambio de información ***regular y eficaz*** y la colaboración ***y formación en materia de ciberseguridad***.

Enmienda 5

Propuesta de Reglamento
Considerando 7

Texto de la Comisión	*Enmienda*
(7) Las diferencias entre las instituciones, los órganos y los organismos de la Unión exigen flexibilidad en la ejecución, dado que no hay una solución única válida para todos los casos. Las medidas destinadas a garantizar un elevado nivel común de ciberseguridad ***no*** deben ***prever ninguna obligación que interfiera directamente en*** el desempeño de la misión ***o vulnere*** la autonomía institucional de cada institución, órgano y organismo de la Unión. Así pues, las instituciones, los órganos y los organismos deben establecer sus propios marcos para la gestión, la gobernanza y el control de riesgos en el ámbito de la ciberseguridad y adoptar sus propios códigos básicos y planes de ciberseguridad.	(7) Las diferencias entre las instituciones, los órganos y los organismos de la Unión exigen flexibilidad en la ejecución, dado que no hay una solución única válida para todos los casos. Las medidas destinadas a garantizar un elevado nivel común de ciberseguridad deben ***apoyar*** el desempeño de la misión ***y tener en cuenta*** la autonomía institucional de cada institución, órgano y organismo de la Unión. Así pues, las instituciones, los órganos y los organismos deben establecer sus propios marcos para la gestión, la gobernanza y el control de riesgos en el ámbito de la ciberseguridad y adoptar sus propios códigos básicos y planes de ciberseguridad***, teniendo en cuenta la coherencia y la interoperabilidad de sus respectivos marcos y sobre la base del marco común establecido por el presente Reglamento***.

Enmienda 6
Propuesta de Reglamento
Considerando 8

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

Enmienda 7

Propuesta de Reglamento
Considerando 9

Texto de la Comisión	*Enmienda*
(9) Para lograr un elevado nivel común de ciberseguridad es preciso que la ciberseguridad sea supervisada por el más alto nivel de dirección de cada institución, órgano y organismo de la Unión, que deberá aprobar un código básico de ciberseguridad que contemple los riesgos detectados en el marco que han de establecer las distintas entidades. Incorporar la cultura de la ciberseguridad, esto es, la práctica cotidiana de la ciberseguridad, ***es*** una parte integral de un código básico de ciberseguridad para las instituciones, los órganos y los organismos de la Unión.	(9) Para lograr un elevado nivel común de ciberseguridad es preciso que la ciberseguridad sea supervisada por ***un consejo común de la Unión con*** el más alto nivel de dirección de cada institución, órgano y organismo de la Unión, que deberá aprobar un código básico de ciberseguridad que contemple los riesgos detectados en el marco que han de establecer las distintas entidades. Incorporar la cultura de la ciberseguridad, esto es, la práctica cotidiana de la ciberseguridad, ***debe convertirse en*** una parte integral de un código básico de ciberseguridad para las instituciones, los

órganos y los organismos de la Unión.

Enmienda 8

Propuesta de Reglamento
Considerando 10

Texto de la Comisión	*Enmienda*
(10) Las instituciones, los órganos y los organismos de la Unión deben evaluar los riesgos que se derivan de sus relaciones con los proveedores y los prestadores de servicios, en particular de servicios de almacenamiento y tratamiento de datos o de seguridad administrada, y adoptar las medidas adecuadas para encarar esos riesgos. Dichas medidas han de incorporarse al código básico de ciberseguridad y especificarse con más detalle en documentos de orientación o recomendaciones emitidos por el CERT-UE. Al establecer medidas y directrices, es preciso tomar debidamente en consideración la legislación y las políticas pertinentes de la UE, en particular las evaluaciones de riesgos y las recomendaciones del Grupo de Cooperación SRI, como la Evaluación de riesgos coordinada de la UE y el Conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G. Además, ***podría*** exigirse la certificación de los productos, servicios y procesos de las TIC pertinentes, en virtud de los esquemas europeos de certificación de la ciberseguridad adoptados con arreglo al artículo 49 del Reglamento (UE) 2019/881.	(10) Las instituciones, los órganos y los organismos de la Unión deben evaluar los riesgos que se derivan de sus relaciones con los proveedores y los prestadores de servicios, en particular de servicios de almacenamiento y tratamiento de datos o de seguridad administrada, y adoptar las medidas adecuadas para encarar esos riesgos. ***Estos proveedores y prestadores de servicios deben ser evaluados minuciosamente, teniendo en cuenta todo el espectro de la cadena de suministro, así como el entorno económico y político en el que operan. Cuando las relaciones con estos proveedores y los prestadores de servicios supongan un riesgo para la integridad de los procesos democráticos en la Unión, deben cesarse sin demora indebida.*** Dichas medidas han de incorporarse al código básico de ciberseguridad y especificarse con más detalle en documentos de orientación o recomendaciones emitidos por el CERT-UE. Al establecer medidas y directrices, es preciso tomar debidamente en consideración la legislación y las políticas pertinentes de la UE, en particular las evaluaciones de riesgos y las recomendaciones del Grupo de Cooperación SRI, como la Evaluación de riesgos coordinada de la UE y el Conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G. Además, ***teniendo en cuenta el panorama de amenazas y la importancia de ganar resiliencia, debe*** exigirse la certificación de los productos, servicios y procesos de las TIC pertinentes ***utilizados en las instituciones, los órganos y los***

organismos de la Unión, en virtud de los esquemas europeos de certificación de la ciberseguridad adoptados con arreglo al artículo 49 del Reglamento (UE) 2019/881.

Enmienda 9

Propuesta de Reglamento
Considerando 13

Texto de la Comisión	*Enmienda*
(13) Muchos ciberataques se inscriben en campañas más amplias dirigidas contra grupos de instituciones, órganos y organismos de la Unión o comunidades de intereses que incluyen a instituciones, órganos y organismos de la Unión. A fin de facilitar la detección proactiva, la respuesta a incidentes o la adopción de medidas de mitigación, las instituciones, los órganos y los organismos de la Unión deben notificar al CERT-UE las ciberamenazas, las vulnerabilidades y los incidentes importantes y transmitir los datos técnicos necesarios para poder detectar, mitigar o responder a ciberamenazas, vulnerabilidades e incidentes similares que afecten a otras instituciones, órganos u organismos de la Unión. Siguiendo el mismo planteamiento previsto en la Directiva [propuesta SRI 2], cuando una entidad tenga conocimiento de un incidente importante, se le ha de exigir que transmita una ***notificación inicial*** al CERT-UE en un plazo de veinticuatro horas. De este modo, el CERT-UE podría difundir la información al resto de instituciones, órganos y organismos de la Unión, así como a los homólogos pertinentes, y ayudar así a proteger los entornos ***informáticos*** de la Unión y de sus homólogos frente a incidentes, amenazas y vulnerabilidades similares.	(13) Muchos ciberataques se inscriben en campañas más amplias dirigidas contra grupos de instituciones, órganos y organismos de la Unión o comunidades de intereses que incluyen a instituciones, órganos y organismos de la Unión. A fin de facilitar la detección proactiva, la respuesta a incidentes o la adopción de medidas de mitigación, las instituciones, los órganos y los organismos de la Unión deben notificar al CERT-UE las ciberamenazas, las vulnerabilidades y los incidentes importantes y transmitir los datos técnicos necesarios para poder detectar, mitigar o responder a ciberamenazas, vulnerabilidades e incidentes similares que afecten a otras instituciones, órganos u organismos de la Unión. Siguiendo el mismo planteamiento previsto en la Directiva [propuesta SRI 2], cuando una entidad tenga conocimiento de un incidente importante, se le ha de exigir que transmita una ***alerta rápida*** al CERT-UE ***sin demora indebida y en cualquier caso a más tardar*** en un plazo de veinticuatro horas. ***Se deben asignar recursos suficientes a las instituciones, los órganos y los organismos de la Unión para cumplir sus obligaciones de información de forma rápida y eficaz, con el fin de garantizar que el sistema diseñado funcione correctamente.*** De este modo, el CERT-UE podría difundir la información al resto de instituciones, órganos y organismos de la Unión, así como a los homólogos

pertinentes, y ayudar así a proteger los entornos ***de las TIC*** de la Unión y de sus homólogos frente a incidentes, amenazas y vulnerabilidades similares.

Enmienda 10

Propuesta de Reglamento
Considerando 14

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

Enmienda 11

Propuesta de Reglamento
Considerando 16

Texto de la Comisión	*Enmienda*
(16) El CIIC debe hacer un seguimiento del cumplimiento del presente Reglamento y de los documentos de orientación, las recomendaciones y los llamamientos a la acción emitidos por el CERT-UE. Es preciso que el CIIC cuente, para las cuestiones técnicas, con el respaldo de grupos técnicos consultivos***, constituidos***	(16) El CIIC debe hacer un seguimiento del cumplimiento del presente Reglamento y de los documentos de orientación, las recomendaciones y los llamamientos a la acción emitidos por el CERT-UE. Es preciso que el CIIC cuente, para las cuestiones técnicas, con el respaldo de grupos técnicos consultivos que trabajen en

en función de sus necesidades, que trabajen en estrecha cooperación con el CERT-UE, las instituciones, los órganos y los organismos de la Unión y, ***en su caso***, otras partes interesadas. Cuando sea necesario, el CIIC ha de emitir advertencias ***no vinculantes*** y ***recomendar*** auditorías.	estrecha cooperación con el CERT-UE, las instituciones, los órganos y los organismos de la Unión y, ***cuando proceda***, otras partes interesadas. Cuando sea necesario, el CIIC ha de emitir advertencias y ***recomendaciones para*** auditorías.

Enmienda 12

Propuesta de Reglamento
Considerando 17

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

Enmienda 13

Propuesta de Reglamento
Considerando 18

Texto de la Comisión	*Enmienda*
(18) En 2020, el Comité de Dirección del CERT-UE estableció un nuevo objetivo estratégico con miras a que el CERT-UE garantice, para el conjunto de las instituciones, los órganos y los organismos de la Unión, un exhaustivo nivel de ciberseguridad con el alcance y la amplitud adecuadas y en continua adaptación a las amenazas, ya sean actuales o inminentes, incluidos los ataques contra los dispositivos móviles, los entornos en la	(18) En 2020, el Comité de Dirección del CERT-UE estableció un nuevo objetivo estratégico con miras a que el CERT-UE garantice, para el conjunto de las instituciones, los órganos y los organismos de la Unión, un exhaustivo nivel de ciberseguridad con el alcance y la amplitud adecuadas y en continua adaptación a las amenazas, ya sean actuales o inminentes, incluidos los ataques contra los dispositivos móviles, los entornos en la

nube y los dispositivos del internet de las cosas. El objetivo estratégico comprende asimismo la intervención de centros de operaciones de seguridad (SOC) con amplias capacidades para supervisar las redes, así como un seguimiento veinticuatro horas al día, siete días a la semana, en caso de amenaza de gran gravedad. Para las instituciones, los órganos y los organismos de la Unión de mayor tamaño, el CERT-UE ha de prestar apoyo a sus equipos de seguridad ***informática***, en particular mediante un seguimiento de primera línea veinticuatro horas al día, siete días a la semana. Para las instituciones, los órganos y los organismos de la Unión de menor tamaño y algunos de tamaño mediano, el CERT-UE debe prestar todos los servicios.	nube y los dispositivos del internet de las cosas. El objetivo estratégico comprende asimismo la intervención de centros de operaciones de seguridad (SOC) con amplias capacidades para supervisar las redes, así como un seguimiento veinticuatro horas al día, siete días a la semana, en caso de amenaza de gran gravedad. Para las instituciones, los órganos y los organismos de la Unión de mayor tamaño, el CERT-UE ha de prestar apoyo a sus equipos de seguridad ***de las TIC***, en particular mediante un seguimiento de primera línea veinticuatro horas al día, siete días a la semana. Para las instituciones, los órganos y los organismos de la Unión de menor tamaño y algunos de tamaño mediano, el CERT-UE debe prestar todos los servicios.

Enmienda 14

Propuesta de Reglamento
Considerando 19 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(19 bis) A fin de garantizar una mejor aplicación de las medidas y directrices en materia de ciberseguridad para las instituciones, los órganos y los organismos de la Unión, así como para consolidar una cultura de ciberseguridad en ellas, el CERT-UE también debe mejorar la cooperación con la Red Europea de Competencias en Ciberseguridad y el Centro Europeo de Competencia en Ciberseguridad.

Enmienda 15

Propuesta de Reglamento
Considerando 20

Texto de la Comisión	*Enmienda*
(20) El CERT-UE, en su labor de apoyo	(20) El CERT-UE, en su labor de apoyo

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

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

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

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

Enmienda 16
Propuesta de Reglamento
Considerando 24

Texto de la Comisión

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

Enmienda

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

Enmienda 17

Propuesta de Reglamento
Considerando 25

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

Enmienda 18

Propuesta de Reglamento
Artículo 1 – párrafo 1 – letra a

Texto de la Comisión	*Enmienda*
a) la obligación, para las instituciones, los órganos y los organismos de la Unión, de adoptar un marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad;	*(No afecta a la versión española).*

Enmienda 19

Propuesta de Reglamento
Artículo 1 – párrafo 1 – letra c

Texto de la Comisión	*Enmienda*
c) normas sobre la organización y el funcionamiento del Centro de Ciberseguridad para las instituciones, los órganos y los organismos de la Unión (CERT-UE), y sobre la organización y el funcionamiento del Consejo Interinstitucional de Ciberseguridad (CIIC).	*(No afecta a la versión española).*

Enmienda 20

Propuesta de Reglamento
Artículo 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 2 bis
	Tratamiento de datos personales
	El tratamiento de datos personales en virtud del presente Reglamento por parte del CERT-UE, el CIIC y todas las instituciones, los órganos y los organismos de la Unión se llevará a cabo de conformidad con el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo.

Enmienda 21

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 2

Texto de la Comisión	*Enmienda*
2) «redes y sistemas de información»: las redes y los sistemas de información ***en el sentido del*** artículo ***4***, punto 1, de la Directiva [propuesta SRI 2];	2) «redes y sistemas de información»: las redes y los sistemas de información ***como se define en el*** artículo ***6***, punto 1, de la Directiva [propuesta SRI 2];

Enmienda 22

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 4

Texto de la Comisión	*Enmienda*
4) «ciberseguridad»: la ciberseguridad en el ***sentido del*** artículo ***4***, punto ***3***, ***de la Directiva [propuesta SRI 2]***;	4) «ciberseguridad»: la ciberseguridad ***como se define*** en el artículo ***2***, punto ***1***, ***del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo***[1 bis];
	[1 bis] 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).

Enmienda 23

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 5

Texto de la Comisión	*Enmienda*
5) «más alto nivel de dirección»: el cargo directivo, el órgano de gestión o el órgano de coordinación y supervisión al más alto nivel administrativo, habida cuenta de los sistemas de gobernanza de alto nivel de cada institución, órgano u organismo de la Unión;	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 ***con un mandato de tomar o autorizar decisiones***, habida cuenta de los sistemas de gobernanza de alto nivel de cada institución, órgano u organismo de la Unión;

Enmienda 24

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 7

Texto de la Comisión	*Enmienda*
7) «incidente importante»: todo incidente ***salvo aquel cuyas consecuencias sean limitadas y del*** que ***probablemente ya se tenga una buena comprensión en términos de método*** o ***tecnología***;	7) «incidente importante»: todo incidente ***que haya causado o pueda causar graves perturbaciones operativas para el funcionamiento de la entidad de la Unión o perjuicios económicos para la entidad de la Unión de que se trate, o*** que ***haya afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales*** o ***morales considerables***;

Enmienda 25

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 11

Texto de la Comisión	*Enmienda*
11) «ciberamenaza importante»: toda ciberamenaza ***en la que existan la intención***, ***la oportunidad y la capacidad*** de ***provocar un incidente importante***;	11) «ciberamenaza importante»: toda ciberamenaza ***según se define en el artículo 6***, ***punto 11,*** de ***la Directiva [propuesta SRI 2]***;

Enmienda 26

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 14

Texto de la Comisión	*Enmienda*
14) «riesgo ***de ciberseguridad***»: ***toda circunstancia o hecho razonablemente identificables que puedan ser perjudiciales para*** la ***seguridad de las redes y los sistemas de información***;	14) «riesgo»: ***todo riesgo según se define en el artículo 6, punto 9, de*** la ***Directiva [propuesta SRI 2]***;

Enmienda 27

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 14 bis (nuevo)

Texto de la Comisión	*Enmienda*
	14 bis) «entorno de TIC»: todo producto, servicio y proceso de TIC local o virtual, tal y como se definen en el artículo 2, puntos 12, 13 y 14, del Reglamento (UE) 2019/881, y toda red y sistema de información, tanto si pertenecen y son operados por una institución, un órgano o un organismo de la Unión como si están alojados o son operados por un tercero, incluidos dispositivos móviles, redes corporativas, redes profesionales no conectadas a internet y dispositivos conectados al entorno de TIC;

Justificación

Término trasladado del artículo 4, apartado 2, de la presente Propuesta al artículo que figura en las Definiciones, puesto que dicho término se emplea de forma sistemática en todo el texto. La definición propuesta para este término proviene de las definiciones de sus

componentes del artículo 2 del Reglamento sobre la Ciberseguridad (UE) 2019/881.

Enmienda 28

Propuesta de Reglamento
Artículo 3 – párrafo 1 – punto 15

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

Enmienda 29
Propuesta de Reglamento
Artículo 4 – apartado 1

Texto de la Comisión	*Enmienda*
1. Cada institución, órgano y organismo de la Unión, en apoyo de su misión y dentro del ejercicio de su autonomía institucional, establecerá su propio marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad («el marco»)***.*** ***A fin de garantizar*** la ***gestión eficaz y prudente*** de ***todos los riesgos relacionados con la ciberseguridad***, el más alto nivel de dirección de cada entidad supervisará esta labor. El marco deberá estar establecido a más tardar el ... [quince meses después de la entrada en vigor del presente Reglamento].	1. ***A partir de una auditoría de seguridad completa,*** cada institución, órgano y organismo de la Unión, en apoyo de su misión y dentro del ejercicio de su autonomía institucional, establecerá su propio marco interno de gestión, gobernanza y control de riesgos en el ámbito de la ciberseguridad («el marco»)***, teniendo en cuenta al mismo tiempo*** la ***coherencia y la interoperabilidad*** de ***su marco con los de otras instituciones***, ***órganos y organismos.*** El más alto nivel de dirección de cada entidad***, que será el responsable de garantizar la gestión eficaz y prudente de todos los riesgos relacionados con la ciberseguridad,*** supervisará esta labor. El marco deberá estar establecido a más tardar el ... [quince meses después de la ***fecha de*** entrada en vigor del presente Reglamento].

Enmienda 30

Propuesta de Reglamento
Artículo 4 – apartado 2

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

Enmienda 31
Propuesta de Reglamento
Artículo 4 – apartado 4

Texto de la Comisión	*Enmienda*
4. Cada institución, órgano y organismo de la Unión dispondrá de mecanismos eficaces para asegurar que un ***porcentaje adecuado*** de su presupuesto ***informático*** se destine a la ciberseguridad.	4. Cada institución, órgano y organismo de la Unión dispondrá de mecanismos eficaces para asegurar que ***al menos*** un ***10 %*** de su presupuesto ***de TIC agregado*** se destine a la ciberseguridad ***a medio plazo***.

Enmienda 32

Propuesta de Reglamento
Artículo 4 – apartado 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. El responsable local de ciberseguridad cooperará con el delegado de protección de datos a que se refiere el artículo 43 del Reglamento (UE) 2018/1725 cuando se solapen actividades que apliquen los principios de protección de datos desde el diseño y por defecto a las medidas de ciberseguridad, así como cuando se seleccionen medidas de ciberseguridad relacionadas con la protección de los datos personales y la gestión integrada de riesgos e incidentes de seguridad.

Enmienda 33

Propuesta de Reglamento
Artículo 5 – apartado 1

Texto de la Comisión	*Enmienda*
1. El más alto nivel de dirección de cada institución, órgano y organismo de la Unión aprobará el código básico de ciberseguridad de su propia entidad para abordar los riesgos detectados en el marco a que se refiere el artículo 4, apartado 1. Esto lo hará en apoyo de su misión y dentro del ejercicio de su autonomía institucional. El código básico de ciberseguridad, que deberá estar establecido a más tardar el ... [dieciocho meses después de la entrada en vigor del presente Reglamento], cubrirá los ámbitos enumerados en el anexo I y las medidas enumeradas en el anexo II.	1. El más alto nivel de dirección de cada institución, órgano y organismo de la Unión aprobará el código básico de ciberseguridad de su propia entidad para abordar los riesgos detectados en el marco a que se refiere el artículo 4, apartado 1. Esto lo hará en apoyo de su misión y dentro del ejercicio de su autonomía institucional***, respetando plenamente los requisitos del presente Reglamento y teniendo en cuenta la coherencia y la interoperabilidad de su marco con los de otras instituciones, órganos y organismos, así como los documentos de orientación y las recomendaciones adoptados por el CIIC a propuesta del CERT-UE y los esquemas de certificación de la ciberseguridad de la Unión aplicables***. El código básico de ciberseguridad, que deberá estar establecido a más tardar el ... [dieciocho meses después de la ***fecha de*** entrada en vigor del presente Reglamento], cubrirá los ámbitos enumerados en el anexo I y las medidas enumeradas en el

anexo II.

Enmienda 34

Propuesta de Reglamento
Artículo 5 – apartado 2

Texto de la Comisión	*Enmienda*
2. La alta dirección de cada institución, órgano y organismo de la Unión asistirá periódicamente a actividades de formación específicas a fin de adquirir los conocimientos y las capacidades suficientes para comprender y evaluar los riesgos de ciberseguridad y las prácticas de gestión de la ciberseguridad, así como su repercusión en las actividades de la organización.	2. La alta dirección de cada institución, órgano y organismo de la Unión asistirá periódicamente a actividades de formación específicas a fin de adquirir los conocimientos y las capacidades suficientes para comprender y evaluar los riesgos de ciberseguridad y las prácticas de gestión de la ciberseguridad, así como su repercusión en las actividades de la organización ***con recursos adecuados***. ***Además de estas actividades de formación específicas y a efectos de crear y consolidar una cultura de la ciberseguridad, el plan de ciberseguridad incluirá formaciones periódicas en materia de ciberseguridad para el personal que se actualizarán como mínimo cada dos años. Se garantizarán recursos suficientes para ofrecer una formación de calidad.***

Enmienda 35

Propuesta de Reglamento
Artículo 6 – párrafo 1

Texto de la Comisión	*Enmienda*
Cada institución, órgano y organismo de la Unión realizará, como mínimo cada ***tres*** años, una evaluación de la madurez de la ciberseguridad que englobará todos los elementos del entorno ***informático*** de la entidad descritos en el artículo 4, teniendo en cuenta, además, cualesquiera documentos de orientación y recomendaciones pertinentes adoptados de	Cada institución, órgano y organismo de la Unión realizará, ***antes de... [seis meses después de la entrada en vigor del presente Reglamento], y,*** como mínimo cada ***dos*** años ***a partir de esa fecha***, una evaluación de la madurez de la ciberseguridad que englobará todos los elementos del entorno ***de TIC*** de la entidad descritos en el artículo 4, teniendo en

conformidad con el artículo 13.	cuenta, además, cualesquiera documentos de orientación y recomendaciones pertinentes adoptados de conformidad con el artículo 13. ***La evaluación de la madurez se basará en auditorías independientes de ciberseguridad realizadas por prestadores autorizados.***

Enmienda 36

Propuesta de Reglamento
Artículo 7 – apartado 1

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

Enmienda 37

Propuesta de Reglamento
Artículo 7 – apartado 2

Texto de la Comisión	*Enmienda*
2. El plan de ciberseguridad especificará las funciones y responsabilidades del personal a efectos de su ejecución.	2. El plan de ciberseguridad especificará las funciones***, preparación*** y responsabilidades del personal a efectos de su ejecución.

Enmienda 38

Propuesta de Reglamento
Artículo 7 – apartado 3

Texto de la Comisión	*Enmienda*
3. El plan de ciberseguridad ***se diseñará teniendo en cuenta cualesquiera*** documentos de orientación y recomendaciones del CERT-UE que sean de aplicación.	3. El plan de ciberseguridad ***incluirá todas la medidas propuestas recogidas en los*** documentos de orientación y recomendaciones del CERT-UE que sean de aplicación.

Enmienda 39

Propuesta de Reglamento
Artículo 7 – apartado 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. Las instituciones, los órganos y los organismos de la Unión presentarán sus planes de ciberseguridad al CIIC. Estos planes se compartirán, en la medida de lo posible, sin correr el riesgo de revelar o comunicar a terceros no autorizados información sensible o confidencial sobre las disposiciones y capacidades técnicas de ciberseguridad concretas de la entidad de la Unión.

Enmienda 40

Propuesta de Reglamento
Artículo 9 – apartado 2 – letra a

Texto de la Comisión	*Enmienda*
a) hacer un seguimiento de la ejecución del presente Reglamento por parte de las instituciones, los órganos y los organismos de la Unión;	a) hacer un seguimiento de la ejecución del presente Reglamento por parte de las instituciones, los órganos y los organismos de la Unión ***y formular recomendaciones para lograr un elevado nivel común de ciberseguridad***;

Enmienda 41

Propuesta de Reglamento
Artículo 9 – apartado 3 – párrafo 1 – parte introductoria

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

Enmienda 42

Propuesta de Reglamento
Artículo 9 – apartado 3 – párrafo 1 – letra k bis (nueva)

Texto de la Comisión	*Enmienda*
	k bis) el Supervisor Europeo de Protección de Datos.

Enmienda 43

Propuesta de Reglamento
Artículo 10 – párrafo 1 – letra a bis (nueva)

Texto de la Comisión	*Enmienda*
	a bis) aprobar, sobre la base de una propuesta del director o de la directora del CERT-UE, recomendaciones para lograr un elevado nivel común de ciberseguridad, dirigidas a una o todas las instituciones, órganos y organismos de la Unión;

Enmienda 44

Propuesta de Reglamento
Artículo 11 – párrafo 1 – letra a

Texto de la Comisión	*Enmienda*
a) emitir una advertencia; cuando sea necesario en vista de la existencia de un riesgo de ciberseguridad imperioso, el público destinatario de la advertencia se restringirá según corresponda;	a) emitir una advertencia; cuando sea necesario en vista de la existencia de un riesgo de ciberseguridad imperioso, el público destinatario de la advertencia se restringirá según corresponda***, mediante una metodología común***;

Enmienda 45

Propuesta de Reglamento
Artículo 11 – párrafo 1 – letra b

Texto de la Comisión	*Enmienda*
b) ***recomendar*** al servicio de auditoría interna pertinente que lleve a cabo una auditoría.	b) ***ordenar*** al servicio de auditoría interna pertinente que lleve a cabo una auditoría.

Enmienda 46

Propuesta de Reglamento
Artículo 12 – apartado 1

Texto de la Comisión	*Enmienda*
1. La misión del CERT-UE, el Centro de Ciberseguridad interinstitucional y autónomo para el conjunto de las	1. La misión del CERT-UE, el Centro de Ciberseguridad interinstitucional y autónomo para el conjunto de las

instituciones, los órganos y los organismos de la Unión, será contribuir al refuerzo de la seguridad del entorno ***informático*** no clasificado de la totalidad de las instituciones, los órganos y los organismos de la Unión ofreciéndoles asesoramiento sobre ciberseguridad, prestándoles ayuda para prevenir, detectar, mitigar y responder a los incidentes, y proporcionándoles una función de centro de coordinación para el intercambio de información sobre ciberseguridad y la respuesta a incidentes.	instituciones, los órganos y los organismos de la Unión, será contribuir al refuerzo de la seguridad del entorno ***TIC*** no clasificado de la totalidad de las instituciones, los órganos y los organismos de la Unión ofreciéndoles asesoramiento sobre ciberseguridad, prestándoles ayuda para prevenir, detectar, mitigar y responder a los incidentes, y proporcionándoles una función de centro de coordinación para el intercambio de información sobre ciberseguridad y la respuesta a incidentes.

Enmienda 47

Propuesta de Reglamento
Artículo 12 – apartado 2 – letra d

Texto de la Comisión	*Enmienda*
d) pondrá en conocimiento del CIIC toda cuestión relacionada con la ejecución del presente Reglamento y de los documentos de orientación, las recomendaciones y los llamamientos a la acción;	d) pondrá en conocimiento del CIIC toda cuestión relacionada con la ejecución del presente Reglamento y de los documentos de orientación, las recomendaciones y los llamamientos a la acción ***y presentará propuestas para su subsanación***;

Enmienda 48

Propuesta de Reglamento
Artículo 12 – apartado 4

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

Ciberdelincuencia.

Enmienda 49

Propuesta de Reglamento
Artículo 12 – apartado 5 – parte introductoria

Texto de la Comisión	*Enmienda*
5. El CERT-UE podrá prestar los servicios no descritos en su catálogo de servicios («servicios facturables») que se indican a continuación:	5. El CERT-UE podrá prestar ***a las instituciones, órganos y organismos de la Unión*** los servicios no descritos en su catálogo de servicios («servicios facturables») que se indican a continuación:

Enmienda 50

Propuesta de Reglamento
Artículo 12 – apartado 5 – letra a

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

Enmienda 51

Propuesta de Reglamento
Artículo 12 – apartado 5 – letra b

Texto de la Comisión	*Enmienda*
b) servicios de apoyo a las operaciones o los proyectos de ciberseguridad de las instituciones, los órganos y los organismos de la Unión,	b) servicios de apoyo a las operaciones o los proyectos de ciberseguridad de las instituciones, los órganos y los organismos de la Unión,

distintos de los destinados a proteger sus entornos ***informáticos***, en virtud de acuerdos escritos y con la aprobación previa del CIIC;	distintos de los destinados a proteger sus entornos ***TIC***, en virtud de acuerdos escritos y con la aprobación previa del CIIC;

Enmienda 52
Propuesta de Reglamento
Artículo 12 – apartado 5 – letra c

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

Enmienda 53

Propuesta de Reglamento
Artículo 12 – apartado 6

Texto de la Comisión	*Enmienda*
6. El CERT-UE podrá organizar ejercicios de ciberseguridad o recomendar la participación en ejercicios en curso, en estrecha cooperación, cuando proceda, con la Agencia de la Unión Europea para la Ciberseguridad, con objeto de someter a prueba el nivel de ciberseguridad de las instituciones, los órganos y los organismos de la Unión.	6. El CERT-UE podrá organizar ejercicios de ciberseguridad o recomendar la participación en ejercicios en curso, en estrecha cooperación, cuando proceda, con la Agencia de la Unión Europea para la Ciberseguridad, con objeto de someter a prueba el nivel de ciberseguridad de las instituciones, los órganos y los organismos de la Unión ***de forma periódica***. ***Además, mediante una cooperación reforzada y programas conjuntos con la Red Europea de Competencias en Ciberseguridad y el Centro Europeo de Competencia en Ciberseguridad, el CERT-UE podrá apoyar la investigación e innovación, así como ayudar a fortalecer las capacidades en materia de ciberseguridad de las instituciones, los órganos y los***

organismos de la Unión.

Enmienda 54

Propuesta de Reglamento
Artículo 12 – apartado 7

Texto de la Comisión	*Enmienda*
7. El CERT-UE ***podrá prestar*** asistencia a las instituciones, los órganos y los organismos de la Unión en relación con incidentes en entornos ***informáticos*** clasificados si la ***Parte afectada*** lo ***solicita*** expresamente.	7. El CERT-UE ***prestará*** asistencia a las instituciones, los órganos y los organismos de la Unión en relación con incidentes en entornos ***TIC*** clasificados si ***las instituciones, los órganos o los organismos de*** la ***Unión afectados*** lo ***solicitan*** expresamente ***y si el CERT-UE cuenta con los recursos necesarios para hacerlo o recibe dichos recursos de la entidad afectada***.

Enmienda 55

Propuesta de Reglamento
Artículo 14 – párrafo 1

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

Enmienda 56

Propuesta de Reglamento
Artículo 16 – apartado 1

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

Enmienda 57

Propuesta de Reglamento
Artículo 16 – apartado 2

Texto de la Comisión	*Enmienda*
2. El CERT-UE podrá, sin necesidad de obtener el consentimiento de la ***Parte afectada***, intercambiar información específica sobre incidentes con sus homólogos nacionales de los Estados miembros con objeto de facilitar la detección de ciberamenazas o incidentes similares. No obstante, el CERT-UE únicamente podrá intercambiar información específica sobre incidentes en la que se revele la identidad del objetivo del incidente de ciberseguridad con el consentimiento previo de la ***Parte afectada***.	2. El CERT-UE podrá, sin necesidad de obtener el consentimiento de ***las instituciones, los órganos o los organismos de*** la ***Unión afectados y siempre que el tratamiento de los datos personales cumpla las disposiciones aplicables del Reglamento (UE) 2018/1725***, intercambiar información específica sobre incidentes con sus homólogos nacionales de los Estados miembros con objeto de facilitar la detección de ciberamenazas o incidentes similares. No obstante, el CERT-UE únicamente podrá intercambiar información específica sobre incidentes en la que se revele la identidad del objetivo del incidente de ciberseguridad con el consentimiento previo de ***las instituciones, los órganos o los organismos de*** la ***Unión afectados***.

Enmienda 58

Propuesta de Reglamento
Artículo 17 – apartado 1

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

Enmienda 59

Propuesta de Reglamento
Artículo 17 – apartado 2

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

Enmienda 60

Propuesta de Reglamento
Artículo 17 – apartado 3

Texto de la Comisión	*Enmienda*
3. El CERT-UE podrá, con el consentimiento de la ***Parte afectada*** por un incidente, facilitar información relacionada con el incidente a socios que puedan contribuir a su análisis.	3. El CERT-UE podrá, con el consentimiento de ***las instituciones, órganos y organismos de*** la ***Unión afectados*** por un incidente, facilitar información relacionada con el incidente a socios que puedan contribuir a su análisis.

Enmienda 61

Propuesta de Reglamento
Artículo 19 – apartado -1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	-1. Las instituciones, los órganos o los organismos de la Unión podrán facilitar voluntariamente al CERT-UE información sobre las ciberamenazas, incidentes, cuasiincidentes y vulnerabilidades que les afecten. El CERT-UE velará por disponer de medios eficaces de comunicación al objeto de facilitar el intercambio de información con las entidades de la Unión. El CERT-UE podrá dar prioridad a la tramitación de notificaciones obligatorias sobre la de notificaciones voluntarias.

Enmienda 62

Propuesta de Reglamento
Artículo 19 – apartado 1

Texto de la Comisión	*Enmienda*
1. ***Con miras a coordinar la gestión de vulnerabilidades y la respuesta a incidentes***, el CERT-UE podrá solicitar a las ***instituciones***, ***los*** órganos y ***los*** organismos de la Unión que le faciliten	1. ***A fin de desempeñar su misión y las tareas establecidas en el artículo 12***, el CERT-UE podrá solicitar a las ***instituciones***, órganos y organismos de la Unión que le faciliten información acerca

información acerca de sus respectivos inventarios de sistemas ***informáticos que sea pertinente para el desempeño*** de ***su labor.*** La ***institución, el órgano o el organismo*** objeto de la solicitud transmitirá sin demora indebida la información solicitada, así como toda actualización posterior de la información.	de sus respectivos inventarios de sistemas ***TIC, en particular información sobre ciberamenazas, cuasiincidentes, vulnerabilidades, indicadores*** de ***compromiso, alertas de ciberseguridad y recomendaciones relativas a*** la ***configuración de las herramientas de ciberseguridad para detectar ciberincidentes. La entidad*** objeto de la solicitud transmitirá sin demora indebida la información solicitada, así como toda actualización posterior de la información.

Enmienda 63

Propuesta de Reglamento
Artículo 19 – apartado 2

Texto de la Comisión	*Enmienda*
2. Las instituciones, los órganos y los organismos de la Unión facilitarán al CERT-UE, previa solicitud y sin demora indebida, información digital creada mediante el uso de los dispositivos electrónicos implicados en sus respectivos incidentes. El CERT-UE podrá aclarar con más detalle el tipo de información digital que necesita a efectos del conocimiento situacional y la respuesta a incidentes.	*(No afecta a la versión española).*

Enmienda 64
Propuesta de Reglamento
Artículo 20 – título

Texto de la Comisión	*Enmienda*
Obligaciones de ***notificación***	Obligaciones de ***información***

Enmienda 65

Propuesta de Reglamento
Artículo 20 – apartado 1 – párrafo 1

Texto de la Comisión	*Enmienda*
Las instituciones, los órganos y los organismos de la Unión ***transmitirán al CERT-UE*** una ***notificación inicial*** de las ciberamenazas, las vulnerabilidades y los incidentes importantes sin demora indebida, y en todo caso dentro de las veinticuatro horas siguientes a su constatación.	Las instituciones, los órganos y los organismos de la Unión ***alertarán en*** una ***fase temprana al CERT-UE*** de las ciberamenazas, las vulnerabilidades y los incidentes importantes sin demora indebida, y en todo caso dentro de las veinticuatro horas siguientes a su constatación. ***En su caso, dicha alerta temprana indicará si el incidente importante ha sido causado presumiblemente por actos ilícitos o malintencionados y si tiene o podría tener repercusiones transfronterizas.***

Enmienda 66

Propuesta de Reglamento
Artículo 20 – apartado 1 – párrafo 2

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

Enmienda 67

Propuesta de Reglamento
Artículo 20 – apartado 2 – parte introductoria

Texto de la Comisión	*Enmienda*
2. Adicionalmente, las instituciones, los órganos y los organismos de la Unión ***notificarán*** al CERT-UE, sin demora indebida, los detalles técnicos pertinentes sobre las ciberamenazas, las vulnerabilidades y los incidentes que faciliten la detección, la respuesta a incidentes o la adopción de medidas de mitigación. La notificación incluirá, si se	2. Adicionalmente, las instituciones, los órganos y los organismos de la Unión ***enviarán una notificación*** al CERT-UE, sin demora indebida ***y***, ***en cualquier caso, en las setenta y dos horas posteriores a que se haya tenido constancia del incidente importante, actualizarán la advertencia temprana y ofrecerán una evaluación inicial de dicho incidente, su***

dispone de ella, la información siguiente:	***gravedad y sus consecuencias, con*** los detalles técnicos pertinentes sobre las ciberamenazas, las vulnerabilidades y los incidentes que faciliten la detección, la respuesta a incidentes o la adopción de medidas de mitigación. La notificación incluirá, si se dispone de ella, la información siguiente:

Enmienda 68
Propuesta de Reglamento
Artículo 20 – apartado 2 – párrafo 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	En casos debidamente justificados y previo acuerdo del CERT-UE, la institución, el órgano o el organismo de la Unión de que se trate podrá incumplir dicho plazo.

Enmienda 69

Propuesta de Reglamento
Artículo 20 – apartado 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. A más tardar un mes después de presentar la notificación de un incidente importante, las instituciones, los órganos y los organismos de la Unión presentarán un informe final al CERT-UE en el que se recojan, al menos, los siguientes elementos:
	a) una descripción detallada del incidente importante, su gravedad y sus efectos;
	b) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente importante;
	c) las medidas de mitigación aplicadas y en curso;
	d) cuando proceda, los efectos transfronterizos del incidente importante.

	Cuando el incidente importante siga en curso en el momento de la presentación del informe final contemplado en el párrafo primero, se presentará un informe de la situación en ese momento y un informe final en el plazo de un mes a partir de la fecha del incidente.

Enmienda 70

Propuesta de Reglamento
Artículo 20 – apartado 2 ter (nuevo)

Texto de la Comisión	*Enmienda*
	2 ter. En casos debidamente justificados y previo acuerdo del CERT-UE, la institución, el órgano o el organismo de la Unión de que se trate podrá incumplir el plazo establecido en el párrafo 2 bis.

Enmienda 71

Propuesta de Reglamento
Artículo 20 – apartado 3

Texto de la Comisión	*Enmienda*
3. El CERT-UE presentará mensualmente a la ENISA un informe resumido que contendrá datos anonimizados y agregados sobre las ciberamenazas, las vulnerabilidades y los incidentes importantes notificados de conformidad con el apartado 1.	3. El CERT-UE presentará mensualmente a la ENISA un informe resumido que contendrá datos anonimizados y agregados sobre las ciberamenazas, las vulnerabilidades y los incidentes importantes notificados de conformidad con el apartado 1. ***Dicho informe se incorporará al informe bienal sobre la situación de la ciberseguridad en la Unión con arreglo al artículo 18 de la Directiva [propuesta SRI 2].***

Enmienda 72

Propuesta de Reglamento
Artículo 20 – apartado 4

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

Enmienda 73

Propuesta de Reglamento
Artículo 20 – apartado 5

Texto de la Comisión	*Enmienda*
5. Las obligaciones de notificación no serán aplicables a la ICUE ni a la información que una institución, un órgano o un organismo de la Unión haya recibido de un servicio de seguridad o de inteligencia de un Estado miembro con la condición explícita de que no se comparta con el CERT-UE.	***suprimido***

Enmienda 74

Propuesta de Reglamento
Artículo 24 – apartado 2

Texto de la Comisión	*Enmienda*
2. La Comisión informará de la ejecución del presente Reglamento al Parlamento Europeo y al Consejo a más tardar transcurridos ***cuarenta*** y ***ocho*** meses desde la entrada en vigor del presente Reglamento, y posteriormente cada ***tres*** años.	2. La Comisión informará de la ejecución del presente Reglamento al Parlamento Europeo y al Consejo a más tardar transcurridos ***treinta*** y ***seis*** meses desde la entrada en vigor del presente Reglamento, y posteriormente cada ***dos*** años.

Enmienda 75

Propuesta de Reglamento
Artículo 24 – apartado 3

Texto de la Comisión	*Enmienda*
3. La Comisión evaluará el funcionamiento del presente Reglamento e informará de sus conclusiones al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones al menos ***cinco*** años después de la entrada en vigor.	3. La Comisión evaluará el funcionamiento del presente Reglamento e informará de sus conclusiones al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones al menos ***tres*** años después de la entrada en vigor***, dada la rápida evolución del panorama de las amenazas cibernéticas***.

Enmienda 76

Propuesta de Reglamento
Anexo I – párrafo 1 – parte introductoria

Texto de la Comisión	*Enmienda*
El código básico de ciberseguridad cubrirá los ámbitos siguientes:	El código básico de ciberseguridad cubrirá ***al menos*** los ámbitos siguientes:

Enmienda 77

Propuesta de Reglamento
Anexo I – párrafo 1 – punto 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis) formación en materia de ciberseguridad para el personal;

Enmienda 78

Propuesta de Reglamento
Anexo I – párrafo 1 – punto 3

Texto de la Comisión	*Enmienda*
3) gestión de activos, incluidos un inventario de los activos ***informáticos*** y un	3) ***adquisición y*** gestión de activos, incluidos un inventario de los activos ***TIC***

trazado de la red ***informática***;	y un trazado de la red ***TIC***;

Enmienda 79

Propuesta de Reglamento
Anexo I – párrafo 1 – punto 7

Texto de la Comisión	*Enmienda*
7) adquisición, desarrollo y mantenimiento de sistemas;	7) adquisición, desarrollo y mantenimiento de sistemas***, incluido el desarrollo interno de software de código abierto***;

Enmienda 80

Propuesta de Reglamento
Anexo I – párrafo 1 – punto 7 bis (nuevo)

Texto de la Comisión	*Enmienda*
	7 bis) auditorías de ciberseguridad;

Enmienda 81

Propuesta de Reglamento
Anexo I – párrafo 1 – punto 9

Texto de la Comisión	*Enmienda*
9) gestión de incidentes, incluidas estrategias tales como el seguimiento de la seguridad y el registro secuencial para mejorar la preparación, la respuesta y la recuperación en caso de incidente y la cooperación con el CERT-UE;	9) gestión de incidentes, incluidas estrategias tales como el seguimiento de la seguridad y el registro secuencial para mejorar la preparación, la respuesta y la recuperación en caso de incidente***, el cumplimiento y la reducción de los plazos referentes a las obligaciones de información,*** y la cooperación con el CERT-UE;

Enmienda 82

Propuesta de Reglamento
Anexo I – párrafo 1 – punto 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis) formación periódica en materia de ciberseguridad para el personal;

Enmienda 83

Propuesta de Reglamento
Anexo II – párrafo 1 – punto 4 – letra a

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

PROCEDIMIENTO DE LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN

Título	Establecimiento de medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión
Referencias	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Comisión competente para el fondo Fecha del anuncio en el Pleno	ITRE 4.4.2022
Opinión emitida por Fecha del anuncio en el Pleno	AFCO 4.4.2022
Ponente de opinión Fecha de designación	Markéta Gregorová 20.6.2022
Examen en comisión	26.10.2022 1.12.2022
Fecha de aprobación	25.1.2023
Resultado de la votación final	+: 24 –: 0 0: 0
Miembros presentes en la votación final	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Suplentes presentes en la votación final	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Suplentes (art. 209, apdo. 7) presentes en la votación final	Leszek Miller

VOTACIÓN FINAL NOMINAL EN LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Explicación de los signos utilizados
+ : a favor
- : en contra
0 : abstenciones