RESPUESTAS DE LA COMISIÓN EUROPEA

AL INFORME ESPECIAL DEL TRIBUNAL DE CUENTAS EUROPEO

Ciberseguridad de las instituciones, órganos y organismos europeos: El nivel de preparación no es proporcional a las amenazas

Índice

El presente documento resume las respuestas de la Comisión Europea a las observaciones de un informe especial del Tribunal de Cuentas Europeo, de conformidad con el artículo 259 del Reglamento Financiero, y se publicará junto con el Informe Especial.

I. LAS RESPUESTAS DE LA COMISIÓN EN SÍNTESIS

a) Introducción general

La ciberseguridad se ha convertido en una de las principales prioridades políticas y operativas de la Comisión Europea. La crisis de la COVID ha acelerado nuestra dependencia de los servicios digitales (computación en nube, dispositivos móviles, inteligencia artificial). En los dos últimos años hemos asistido a un cambio masivo hacia el teletrabajo. Esto significa que tanto la ciberdelincuencia como el ciberespionaje, las dos principales amenazas a las que se enfrentan las instituciones, órganos y organismos de la Unión Europea (en lo sucesivo, IOUE), también se han puesto en línea de hecho y a lo grande. La Comisión es consciente de esta tendencia. Ha mostrado un liderazgo coherente y decisivo en materia de ciberseguridad. El Reglamento sobre la Ciberseguridad entró en vigor en 2019, entre otras cosas ampliando el mandato de la ENISA y haciéndola permanente. Dicho Reglamento también estableció una cooperación formal entre ENISA y el CERT-UE (el Equipo de respuesta a emergencias informáticas de las IOUE). En 2020, la Comisión propuso un refuerzo de la Directiva sobre seguridad de las redes y sistemas de información, que está a punto de alcanzar un acuerdo en la legislatura.

La Estrategia de Ciberseguridad de 2020 también incluía tres acciones relacionadas con la ciberseguridad de las IOUE. Anunciaba un Reglamento sobre la seguridad de la información en las instituciones, órganos y organismos de la UE, un Reglamento relativo a normas comunes sobre ciberseguridad para todas las instituciones, órganos y organismos de la UE y su intención de proporcionar una nueva base jurídica al CERT-UE para reforzar su mandato y su financiación y garantizar que cuente con los recursos adecuados ante el aumento de las amenazas, los riesgos y los incidentes.

El trabajo de preparación de estas propuestas ha progresado. Aunque aún no han sido adoptadas por el Colegio, su adopción está prevista para el primer trimestre de 2022. Las cuestiones importantes debatidas entre las instituciones en esta fase preparatoria se refieren a la base jurídica de la propuesta, así como a la capacidad presupuestaria de todas las instituciones, organismos y órganos de la UE para cumplir los requisitos, tanto en lo que se refiere a la financiación de su propia ciberseguridad como a la búsqueda de los recursos necesarios para financiar el CERT-UE, el presupuesto y en particular los puestos.

El nivel de preparación en materia de ciberseguridad de las instituciones, órganos y organismos de la UE presenta diferentes niveles. Algunas IOUE cuentan con resultados sólidos en cuanto a preparación cibernética y deben seguir desempeñando un papel de liderazgo, estimulando e inspirando avances y mejoras adicionales en todo el panorama de la ciberseguridad. Con el fin de lograr avances mensurables, es importante reconocer los distintos niveles de madurez entre las instituciones, organismos y órganos de la UE y establecer prioridades dirigiendo las medidas de mejora en primer lugar hacia aquellas instituciones, organismos y órganos de la UE donde las carencias detectadas dan lugar a la mayor exposición al riesgo.

b) Posición de la Comisión sobre las principales observaciones y recomendaciones del TCE

La Comisión acoge con satisfacción el informe del TCE sobre la ciberseguridad en las instituciones, los órganos y los organismos de la UE. Toma nota de que el informe subraya la importancia de los

marcos jurídicos comunes para todas las IOUE en relación con la seguridad de la información y la ciberseguridad para aumentar el nivel global de ciberseguridad en todos ellos. La Comisión observa que las principales observaciones y recomendaciones del TCE no se centran en la propia ciberseguridad operativa de la Comisión en sí, sino en el papel de la Comisión a la hora de proponer legislación para aumentar la madurez cibernética de las IOUE.

Los futuros Reglamentos sobre «La seguridad de la información de las IOUE» y las «Normas de ciberseguridad comunes para las instituciones, órganos y agencias de la UE» establecerán normas comunes para lograr niveles elevados de seguridad de la información y ciberseguridad, pero su aplicación, dentro del contexto organizativo y operativo de cada IOUE (en particular, sus perfiles de amenazas y riesgos) sigue quedando bajo la responsabilidad autónoma de cada uno. El Reglamento sobre la ciberseguridad propuesto contará con mecanismos de cumplimiento adecuados y proporcionales al objetivo y ámbito de las nuevas normas, sin perjuicio de la autonomía de las instituciones, órganos y organismos.

La Comisión preside actualmente el subgrupo de ciberseguridad del Comité interinstitucional sobre la transformación digital (ICDT), que es una designación rotatoria (por un período máximo de dos años). Cabe señalar que no se han asignado recursos específicos al trabajo del subgrupo: todas las acciones se basan en los mejores logros de los participantes con carácter voluntario.

La Comisión está de acuerdo con la idea general de reforzar los recursos y el mandato del CERT-UE.

Con esta premisa, la Comisión apoya las principales observaciones y recomendaciones del informe. Nuestra posición detallada se explica en los comentarios adicionales de la sección III. Respecto a las recomendaciones, la Comisión acepta las recomendaciones 1, letras a), b), c), d), e), f), g), y 2, letras a), b) y c).

c) Últimos avances pertinentes y próximas etapas

Ha finalizado una consulta formal a nivel de directores generales de las IOUE sobre los proyectos consolidados de los dos Reglamentos (seguridad de la información y ciberseguridad) y está en curso la evaluación de las respuestas recibidas, antes de la finalización del paquete y su adopción por el Colegio en el primer trimestre de 2022.

II. RESPUESTAS DE LA COMISIÓN A LAS PRINCIPALES OBSERVACIONES DEL TCE

1. Niveles de madurez en materia de ciberseguridad de las IOUE

La Comisión conviene en que, cuando se observa el nivel de gasto de las IOUE en materia de ciberseguridad, es importante tener en cuenta las amenazas y los riesgos.

De la misma forma, en relación con el aspecto de los recursos humanos, la estabilidad del personal de las IOUE se ve influida por diferentes factores. El mercado de contratación de expertos especializados en ciberseguridad es cada vez más complejo. En muchos casos, las normas sobre

recursos humanos no están adaptadas a los perfiles especializados (contratación, desarrollo profesional, formación). Además, la presión generalizada ejercida por la Autoridad Presupuestaria sobre los niveles de dotación de personal en las diversas IOUE significa que ámbitos emergentes de alta prioridad, como la ciberseguridad, siguen estando infradotados de puestos, en particular en servicios operativos internos.

La referencia a los avances en materia de gobernanza y gestión de riesgos debe tener en cuenta el hecho de que el seguimiento del cumplimiento está pasando ahora de la fase piloto a la del despliegue completo. Así pues, es normal que la cobertura sea hasta ahora bastante baja. Este proyecto de cumplimiento es la siguiente fase de un proceso de mejora de la madurez cibernética a largo plazo que comenzó con la definición de una metodología común de riesgo, la construcción de unas herramientas comunes, el despliegue de la gestión de la vulnerabilidad y la supervisión, prueba y validación del inventario de activos. Se ha avanzado a lo largo de este largo camino a pesar de la complejidad de la base de activos de la Comisión, con más de 1 000 sistemas de información operados por más de 50 Direcciones Generales y Organismos de Ejecución.

2. Mecanismos de las instituciones, órganos y organismos de la UE para la cooperación

El CERT-UE ha sido todo un éxito a la hora de promover la cooperación no solo entre las IOUE, sino también a nivel europeo, a través de su participación como miembro de pleno derecho de la red CSIRT creada en virtud de la Directiva SRI. De esa forma, el CERT-UE es un claro ejemplo de cómo pueden mejorarse la cooperación y los servicios de ciberseguridad. Las observaciones del TCE sobre el CERT-UE ilustran muy claramente el trabajo sobresaliente que está realizando este frente a un panorama de ciberamenazas cada vez más hostil y con una escasez crónica de recursos.

En virtud del actual Acuerdo Interinstitucional, las agencias descentralizadas y empresas comunes de la UE están representadas oficialmente en el Comité de Dirección del CERT-UE por ENISA. Aparte de eso, sus puntos de vista son defendidos en las reuniones del Comité de Dirección por un representante del Comité Consultivo de las TIC (ICTAC), a quien se permite asistir para ayudar a ENISA en su función de representación de las agencias, aunque que no tiene plaza oficial ni voto. El punto de la representación adecuada de las agencias en el Comité de Dirección del CERT-UE será abordado en la propuesta de Reglamento completando la composición del Comité de Dirección con un máximo de tres representantes designados por la red de agencias de la Unión (EUAN), a propuesta del Comité Consultivo de sus TIC.

La participación en el subgrupo de ciberseguridad del ICDT se realiza de acuerdo con las posibilidades, al nivel de compromiso decidido por cada IOUE. Se están estudiando mejoras para el intercambio de información sobre contratación, como un tema importante en el ámbito del Grupo de Trabajo 2 del subgrupo de Ciberseguridad, en la preparación del nuevo contrato marco de ciberseguridad.

En lo tocante a las herramientas comunes para servicios como el correo electrónico y la videoconferencia, todas las IOUE tienen ya la posibilidad de utilizar el sistema SECEM-2 aplicado por la Comisión para el correo electrónico cifrado, dependiendo de la gestión efectiva de las claves y los certificados de cifrado. Además, se está desarrollando SECABC, una herramienta para permitir el cifrado del correo electrónico entre instituciones, con intención de ofrecer acceso a esta herramienta a todas las IOUE a partir de 2022. La posibilidad de realizar videoconferencias seguras para servicios SNC ya se ha materializado y puede ampliarse a otras IOUE con carácter puntual

mediante la gestión de las identidades de los participantes en la reunión. En la propuesta de Reglamento sobre seguridad de la información también se abordará la forma de compartir información sensible (mediante etiquetado y marcado comunes).

3. Puesta en común de información acerca de incidentes significativos o vulnerabilidades

El hecho de que no todas las IOUE notifiquen al CERT-UE los incidentes significativos o vulnerabilidades se trata en el proyecto de Reglamento sobre la ciberseguridad, conforme a la propuesta de la Comisión en la Directiva SRI 2[1]. El nivel de ejecución dependerá de los recursos adicionales dedicados a ello por las instituciones, órganos y organismos autónomos de la UE. El ámbito de aplicación de dichas notificaciones sigue siendo limitado, también en virtud del Reglamento tal como se ha planeado actualmente, debido a la autonomía institucional de las instituciones, órganos y organismos autónomos de la UE. La propuesta de Reglamento sobre ciberseguridad tendrá mecanismos de cumplimiento adecuados y proporcionales al objetivo y ámbito de las nuevas normas, sin perjuicio de la autonomía de las instituciones, órganos y organismos.

III. RESPUESTAS DE LA COMISIÓN A LAS CONCLUSIONES Y RECOMENDACIONES DEL TCE

Recomendación 1 - Mejorar la preparación en materia de ciberseguridad de todas las IOUE mediante normas vinculantes comunes y más recursos para el CERT-UE

El texto de Reglamento propuesto incluirá medidas específicas diseñadas para aumentar más el nivel común de ciberseguridad. Las medidas citadas se traducirán en planes de ciberseguridad, definidos y aplicados a nivel de las IOUE, con arreglo a su propio marco de gobernanza de la ciberseguridad.

La Comisión acepta esta recomendación. Con referencia a las subrecomendaciones específicas, la Comisión señala lo siguiente:

a) La Comisión acepta la recomendación 1, letra a). El proyecto de Reglamento incluirá disposiciones relativas a los marcos de gobernanza y control, establecidos al máximo nivel de la dirección ejecutiva de cada IOUE, para garantizar una gestión eficaz y prudente de todos los riesgos de ciberseguridad.

[1] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148, [COM(2020) 823 final].

b) La Comisión acepta la recomendación 1, letra b). El proyecto de Reglamento reforzará la mención del enfoque basado en el riesgo para la gestión de la ciberseguridad dejando claro que, tras las evaluaciones, deben seguir las acciones, los planes de seguridad informática y la aplicación real de los controles esenciales.
c) La Comisión acepta la recomendación 1, letra c). La educación, la sensibilización y los programas de formación en materia de ciberseguridad se citarán en el proyecto de Reglamento como una parte del valor de referencia de la ciberseguridad.
d) La Comisión acepta la recomendación 1, letra d). Partiendo de nuestra experiencia, aunque las auditorías y pruebas periódicas son esenciales, no son suficientes para garantizar que se está progresando. Así pues, son necesarias la notificación regular y la transparencia, como parte del marco de gobernanza de la ciberseguridad con arreglo a la letra a).
e) La Comisión acepta la recomendación 1, letra e). El proyecto de Reglamento incluirá disposiciones relativas a la notificación al CERT-UE, por parte de las IOUE, de ciberamenazas, vulnerabilidades e incidentes significativos.
f) La Comisión acepta la recomendación 1, letra f). La Comisión apoya la necesidad de reforzar los recursos de CERT-UE. En el texto del proyecto de Reglamento se incluirán disposiciones relativas a la dotación de personal y a las contribuciones financieras de las IOUE.
g) La Comisión acepta la recomendación 1, letra g). La propuesta de Reglamento tendrá mecanismos de cumplimiento adecuados y proporcionales al objetivo y ámbito de las nuevas normas, respetando la autonomía institucional de las IOUE. El contenido del futuro Reglamento depende del resultado del procedimiento legislativo y es el resultado de una decisión tomada por el legislador de la UE con respecto a la propuesta realizada por la Comisión.

Recomendación 2 - Fomentar nuevas sinergias entre las IOUE en ámbitos seleccionados

La Comisión, que en la actualidad preside el subgrupo de ciberseguridad del Comité Interinstitucional sobre la transformación digital (ICDT), está de acuerdo con las recomendaciones de fomentar soluciones para el intercambio coherente y seguro de información sensible sobre proyectos de ciberseguridad y marcos comunes de adquisición pública y contratos para servicios de ciberseguridad.

La Comisión acepta esta recomendación. Con referencia a las subrecomendaciones específicas, la Comisión señala lo siguiente:

a) La Comisión acepta la recomendación 2, letra a). La Comisión está aportando iniciativas y servicios técnicos al subgrupo de Ciberseguridad del ICDT para promover y apoyar herramientas comunes para compartir información sensible, habilitando servicios como el correo electrónico y la videoconferencia. Señalamos también que se fijarán normas comunes para el marcado y el tratamiento de información sensible no clasificada en la propuesta de Reglamento sobre seguridad de la información.
b) La Comisión acepta la recomendación 2, letra b). Los grupos de trabajo existentes en el marco del subgrupo de ciberseguridad del ICDT están abordando este punto y se seguirá desarrollando. Se están estudiando mejoras en el intercambio de información sobre contratación en la preparación del nuevo contrato marco de ciberseguridad.
c) La Comisión acepta la recomendación 2, letra c). Las instituciones, órganos y organismos tienen acceso a contratos marco interinstitucionales en el ámbito de las TIC gestionados por la Comisión. La preparación del nuevo contrato marco de ciberseguridad será coordinada con el subgrupo de ciberseguridad del ICDT.

Recomendación 3 - Aumentar la atención del CERT-UE y la ENISA hacia las IOUE menos maduras

Los destinatarios de esta recomendación son el CERT-UE y la ENISA.