



Bruselas, 24 de junio de 2022
(OR. en)

10307/22

TELECOM 276
CYBER 225
COMPET 506
MI 483
FIN 699

RESULTADO DE LOS TRABAJOS

De: Secretaría General del Consejo

Fecha: 16 de junio de 2022

A: Delegaciones

N.º doc. prec.: 9616/22

Asunto: Informe Especial 03/2022 del Tribunal de Cuentas Europeo titulado
*«Despliegue de la tecnología 5G en la UE: Retrasos en el despliegue de
redes y problemas de seguridad que siguen sin resolverse»*
- Conclusiones del Consejo (16 de junio de 2022)

Adjunto se remite a las delegaciones las Conclusiones del Consejo sobre el Informe Especial 03/2022 del Tribunal de Cuentas Europeo titulado «Despliegue de la 5G en la UE: Retrasos en el despliegue de redes y problemas de seguridad que siguen sin resolverse», adoptado por el Consejo (Empleo, Política Social, Sanidad y Consumidores) en su sesión n.º 3882 del 16 de junio de 2022.

CONCLUSIONES DEL CONSEJO

**sobre el Informe Especial 03/2022 del Tribunal de Cuentas Europeo
titulado**

**«Despliegue de la tecnología 5G en la UE: Retrasos en el despliegue de redes y problemas de
seguridad que siguen sin resolverse»**

EL CONSEJO DE LA UNIÓN EUROPEA,

RECORDANDO

– sus Conclusiones encaminadas a mejorar el estudio de los informes especiales elaborados por el Tribunal de Cuentas en el marco de la aprobación de la gestión presupuestaria¹;

1. TOMA NOTA del Informe Especial 03/2022 del Tribunal de Cuentas Europeo titulado «Despliegue de la tecnología 5G en la UE: Retrasos en el despliegue de redes y problemas de seguridad que siguen sin resolverse»², que abarca en general el período comprendido entre 2016 y mayo de 2021.
2. DESTACA la importancia estratégica de un despliegue oportuno de las redes 5G de alta calidad en la Unión para propiciar modelos empresariales y servicios públicos innovadores esenciales para el funcionamiento del mercado interior.
3. PONE DE RELIEVE que las demoras en la asignación del espectro pueden explicarse por diferentes razones y que la situación en lo que respecta al despliegue de la tecnología 5G puede haber cambiado en algunos Estados miembros desde que se recopilaron y procesaron los datos. Por consiguiente, HACE HINCAPIÉ EN la importancia de utilizar datos verificados y en la necesidad de que las conclusiones se basen en unos criterios y una metodología claros.

¹ 7515/00 + COR 1.

² WK 5636/22 INIT.

4. RECUERDA sus Conclusiones sobre la importancia de la tecnología 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G, en las que se INSTABA a los Estados miembros y a la Comisión a que, con el apoyo de la ENISA, tomaran todas las medidas necesarias dentro de sus competencias para garantizar la seguridad y la integridad de las redes de comunicaciones electrónicas, en particular de las redes 5G, y siguieran consolidando un planteamiento coordinado para atender los problemas de seguridad de las tecnologías 5G y determinaran metodologías y herramientas comunes eficaces para mitigar los riesgos relacionados con las redes 5G³.
5. RECUERDA el enfoque de estrecha cooperación entre los Estados miembros y la Comisión que condujo a la adopción del conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G⁴, que proporciona un marco de medidas para mitigar las amenazas para la seguridad asociadas a las redes 5G, con vistas a promover un nivel adecuado de seguridad de estas redes en el mercado interior.
6. HACE HINCAPIÉ EN la importancia de que los Estados miembros culminen la aplicación del conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G, en particular en lo que respecta a la aplicación de las restricciones pertinentes a los proveedores que se consideren de alto riesgo para recursos clave definidos como críticos y sensibles en la evaluación coordinada de riesgos de la UE⁵.
7. PONE DE RELIEVE que el conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G constituye un instrumento ágil basado en el riesgo para atender los problemas de seguridad identificados, que permite gestionar los aspectos relacionados con la ciberseguridad de las tecnologías 5G de manera oportuna y eficiente, a la vez que respeta las competencias de los Estados miembros y su responsabilidad exclusiva en materia de seguridad nacional, de conformidad con el artículo 4, apartado 2, del Tratado de la Unión Europea, también en el ámbito de la ciberseguridad.

³ ST 14517/19.

⁴ [Cybersecurity of 5G networks EU Toolbox of risk mitigating measures](#), acordado por el Grupo de Cooperación SRI.

⁵ [Conclusiones](#) de la reunión extraordinaria del Consejo Europeo de los días 1 y 2 de octubre de 2020, EUCO 13/20.

8. RECUERDA el requisito enunciado por la Comisión en su Comunicación «Configurar el futuro digital de Europa»⁶ consistente en que toda empresa que preste servicios a los ciudadanos de la UE debe aceptar y respetar las normas de la UE.
9. TOMA NOTA de las conclusiones y las recomendaciones del Informe Especial y RECONOCE en particular que:
- no todos los Estados miembros hacen referencia a los objetivos de la Comisión en sus estrategias nacionales de 5G ni en sus planes de banda ancha;
 - el Código Europeo de las Comunicaciones Electrónicas (CECE)⁷ aún no se ha transpuesto en todos los Estados miembros;
 - la asignación del espectro para las redes 5G no se ha realizado en todos los Estados miembros o se ha realizado parcialmente;
 - la probabilidad de que un proveedor sea objeto de intromisiones por parte del Gobierno de un país no perteneciente a la UE es un factor importante que en el conjunto de instrumentos se define como determinante de su perfil de riesgo; los criterios para evaluar estas posibles intromisiones incluyen las características del marco jurídico del tercer país, también si este garantiza un nivel suficiente de protección de datos.
10. TOMA NOTA de las respuestas de la Comisión que acompañan al Informe Especial⁸ y de la aceptación de las recomendaciones del Informe Especial por parte de la Comisión.
11. INVITA a los Estados miembros y a la Comisión a que presten atención a las recomendaciones del Informe Especial y los anima a que tengan en cuenta dichas recomendaciones a la hora de elaborar sus políticas sobre el desarrollo de sus redes 5G, garantizando al mismo tiempo la seguridad de dichas redes mediante la aplicación y el posterior desarrollo del conjunto de instrumentos para la ciberseguridad de las redes 5G a la luz de los nuevos problemas de seguridad derivados de las tendencias tecnológicas y de la evolución de la cadena de suministro de la 5G.

⁶ [Comunicación «Configurar el futuro digital de Europa» \(europa.eu\)](#)

⁷ Directiva (UE) 2018/1972.

⁸ [COM-Replies-SR-22-03_ES.pdf \(europa.eu\)](#)

12. INVITA a la Comisión a que colabore con los Estados miembros para recomendar políticas y medidas encaminadas a alcanzar los objetivos europeos de conectividad y la cobertura 5G en todas las zonas pobladas de la Unión de aquí a 2030, teniendo en cuenta al mismo tiempo factores geopolíticos y económicos fundamentales —como la agresión de la Federación de Rusia contra Ucrania— que pueden obstaculizar el progreso hacia la consecución de dichos objetivos y tener consecuencias significativas en términos de coordinación transfronteriza de los Estados miembros con países no pertenecientes a la UE.

 13. INVITA a la Comisión, con el apoyo de la ENISA, y a los Estados miembros, a que prosigan la cooperación coordinada de la UE en materia de medidas para la seguridad de las redes 5G y el seguimiento de la aplicación del conjunto de instrumentos para la ciberseguridad de las redes 5G, y a que evalúen la necesidad de un enfoque más homogéneo respecto al uso de sus elementos.
-