RESPUESTAS DE LA COMISIÓN EUROPEA AL INFORME ESPECIAL DEL TRIBUNAL DE CUENTAS EUROPEO: «DESPLIEGUE DE LA TECNOLOGÍA 5G EN LA UE: RETRASOS EN EL DESPLIEGUE DE REDES Y PROBLEMAS DE SEGURIDAD QUE SIGUEN SIN RESOLVERSE»

RESUMEN

Observaciones preliminares de la Comisión

I. El despliegue rápido y seguro de las redes 5G es una prioridad fundamental para la Comisión Europea. La protección de las redes 5G contra las ciberamenazas consiste en evaluar y mitigar las amenazas y los riesgos. Estos riesgos y amenazas han sido identificados y evaluados conjuntamente por los Estados miembros, con el apoyo de la Comisión y la ENISA, y sobre esta base se ha identificado una serie de medidas globales para mitigar dichos riesgos. Aunque el proceso todavía continúa en algunos Estados miembros, una gran mayoría de ellos ya ha endurecido o están endureciendo los requisitos de seguridad de las redes 5G sobre la base de la caja de herramientas de la UE.

La caja de herramientas de la UE ha sido admitida como marco global para abordar los riesgos de seguridad de la 5G.

La acción coordinada sobre ciberseguridad de la 5G a nivel de la UE y la caja de herramientas de la UE se insertan en un marco europeo más amplio de protección de las redes de comunicaciones electrónicas y otras infraestructuras críticas, y complementan las medidas existentes, como el Código Europeo de las Comunicaciones Electrónicas, el Marco de las Telecomunicaciones, el Reglamento de Ciberseguridad y la Directiva sobre la seguridad de las redes y los sistemas de información (Directiva SRI) y, en su caso, las normas sobre libre circulación establecidas en el Tratado y en la Carta de los Derechos Fundamentales de la UE.

III. La 5G desempeñará un papel clave en nuestra economía y sociedad digitales en los próximos años. Debemos garantizar que las redes 5G sean ciberseguras y resilientes frente a las crecientes amenazas e incidentes cibernéticos. Esta es la razón por la que la Comisión y los Estados miembros han puesto en marcha un proceso de coordinación destinado a definir y aplicar un marco de seguridad 5G global, en forma de una caja de herramientas de reducción del riesgo acordada en enero de 2020, con el fin de hacer frente, de forma eficaz y coordinada, a los principales riesgos para las redes 5G, como el intrusismo informático delictivo, el espionaje y el sabotaje. Aunque el proceso todavía continúa en algunos Estados miembros, una gran mayoría de ellos ya ha endurecido o están endureciendo los requisitos de seguridad de las redes 5G sobre la base de la caja de herramientas de la UE.

VII. La caja de herramientas de la UE proporciona un marco para promover la coherencia en el mercado interior, respetando las competencias de seguridad nacional en este ámbito.

En cuanto al enfoque de los Estados miembros con respecto a los proveedores de alto riesgo, la Comisión considera que solo será posible realizar una evaluación concluyente cuando se disponga de más información.

Aunque la ejecución siga en curso, la Comisión está trabajando con los Estados miembros en el Grupo de cooperación en materia de SRI para promover la armonización y la convergencia entre los enfoques nacionales.

IX. Primer guion: la Comisión acepta la recomendación.

Segundo guion: la Comisión acepta la recomendación.

Tercer guion: la Comisión acepta la recomendación.

La Comisión llevará a cabo la evaluación teniendo en cuenta las competencias nacionales.

INTRODUCCIÓN

04. La Comisión reconoce la existencia de riesgos de seguridad en la 5G, pero señala que la tecnología y las normas de las redes 5G también pueden aportar mejoras de seguridad en comparación con generaciones anteriores.

OBSERVACIONES

30. Si bien la 4G ya puede abarcar una amplia gama de servicios, la 5G debe constituir un gran avance, un cambio importante en comparación con la 4G, por lo que el principal reto consiste en la transición de la 4G a la 5G, desplegando la 5G en toda la UE. El riesgo de brecha digital siempre existe, pero está previsto abordarlo como prioridad en el programa de política «Itinerario hacia la Década Digital» en relación con las trayectorias hacia el objetivo en materia de 5G de una cobertura del 100 % de todas las zonas pobladas de aquí a 2030, apoyando así a los Estados miembros para que tomen medidas en este ámbito, especialmente en lo que se refiere al acceso a las zonas rurales.

32. El Observatorio 5G viene siendo una fuente fiable para supervisar el despliegue de la 5G en la UE y fuera de ella, a pesar de que se hayan producido algunas deficiencias. Los servicios de la Comisión esperan disponer de información más actualizada con el nuevo contratista.

Respuesta conjunta de la Comisión a los apartados 48 y 49:

La Comisión considera que la elección del instrumento (recomendación) y el enfoque de colaboración con los Estados miembros para identificar los riesgos y las medidas de mitigación son la actuación más adecuada para hacer frente a los riesgos de seguridad de la 5G de manera rápida, eficaz y concertada.

La Comisión optó por una Recomendación y por colaborar con los Estados miembros para determinar los riesgos y las medidas de mitigación, habida cuenta de la complejidad y el carácter transversal del asunto en todas las competencias nacionales y de la UE, así como de la importante dimensión de seguridad nacional. Además, la Comisión también tuvo en cuenta el hecho de que los Estados miembros poseen contextos nacionales muy diferentes (estructura del mercado, capacidades de ciberseguridad, inteligencia sobre amenazas, etc.).

La caja de herramientas de la UE supone un instrumento ágil, basado en el riesgo, para hacer frente a los retos en materia de seguridad y que permite tratar los aspectos de ciberseguridad de la 5G de manera oportuna y eficiente.

En su Comunicación «Despliegue seguro de la 5G en la UE — Aplicación de la caja de herramientas de la UE», de enero de 2020, la Comisión anunció que prestaría apoyo a la aplicación de las medidas de la caja de herramientas relacionadas con los requisitos de seguridad, en particular por lo que respecta a las disposiciones correspondientes de la normativa europea sobre comunicaciones electrónicas, y que estudiaría el valor añadido de posibles actos de ejecución que detallen las medidas de seguridad técnicas y organizativas, a fin de complementar las normas nacionales y aumentar la eficacia y coherencia de las medidas de seguridad impuestas a los operadores.

Respuesta conjunta de la Comisión a los apartados 51 y 52:

En el contexto de la revisión de la Recomendación de la Comisión que tuvo lugar en diciembre de 2020, la Comisión entrevistó a las autoridades competentes de todos los Estados miembros. Estas calificaron de oportuna, eficaz y proporcionada la acción coordinada de Europa en materia de ciberseguridad de la 5G. Para abordar esta compleja cuestión, se consideró adecuado el enfoque de colaboración entre las autoridades nacionales, la Comisión, la ENISA y otras partes interesadas

pertinentes. Posibilitó la definición oportuna de objetivos y metodologías comunes, y permitió también a los Estados miembros adaptar las medidas a sus circunstancias nacionales.

La caja de herramientas de la UE y el informe de situación publicado por el Grupo de cooperación en materia de SRI en julio de 2020 recomiendan que se definan planes de aplicación o períodos transitorios para los operadores que actualmente utilizan equipos de proveedores de alto riesgo o que ya hayan celebrado contratos con estos antes de la adopción de la caja de herramientas de la UE (por ejemplo, teniendo en cuenta los ciclos de mejora de los equipos, en particular la migración de las redes 5G «no autónomas» a las «autónomas»).

55. La Comisión toma nota de las observaciones del Tribunal de Cuentas Europeo.

Para seguir apoyando su aplicación, los criterios de la caja de herramientas para evaluar a los proveedores de alto riesgo han sido objeto de numerosos debates entre las autoridades nacionales competentes en el seno del Grupo de cooperación en materia de SRI desde que se pactó la caja de herramientas de la UE.

56. A fin de evaluar el perfil de riesgo de los proveedores, la caja de herramientas de la UE recomienda tener en cuenta los factores de riesgo presentados en la evaluación coordinada de riesgos en la UE, así como la información específica por país (por ejemplo, la evaluación de las amenazas realizada por los servicios nacionales de seguridad, etc.).

61. La capacidad del proveedor de garantizar el suministro es uno de los criterios recomendados por la caja de herramientas de la UE a la hora de evaluar el perfil de riesgo de los proveedores. La capacidad de garantizar el suministro también podría verse afectada por las posibles sanciones comerciales a las que se enfrente un proveedor concreto, como se menciona en el escenario de riesgo relativo a la dependencia de la evaluación coordinada de riesgos en la UE.

Respuesta conjunta de la Comisión a los apartados 70 y 73:

La Comisión y los Estados miembros están compartiendo información detallada sobre la aplicación de la caja de herramientas a nivel nacional en el seno del Grupo de cooperación en materia de SRI. Por lo que se refiere a la divulgación pública de información no pública, este tema es responsabilidad de los Estados miembros.

Respuesta conjunta de la Comisión a los apartados 74 a 76 y al recuadro 5:

La caja de herramientas de la UE proporciona un marco para promover la coherencia en el mercado interior, respetando las competencias de seguridad nacional en este ámbito.

En cuanto al enfoque de los Estados miembros con respecto a los proveedores de alto riesgo, la Comisión considera que solo será posible realizar una evaluación concluyente cuando se disponga de más información.

Aunque la ejecución siga en curso, la Comisión está trabajando con los Estados miembros en el Grupo de cooperación en materia de SRI para promover la armonización y la convergencia entre los enfoques nacionales.

CONCLUSIONES Y RECOMENDACIONES

81. El despliegue rápido y seguro de las redes 5G constituye una prioridad fundamental para la Comisión. La protección de las redes 5G contra las ciberamenazas consiste en evaluar y mitigar las amenazas y los riesgos. Estos riesgos y amenazas han sido identificados y evaluados conjuntamente por los Estados miembros, con el apoyo de la Comisión y la ENISA, y sobre esta base se ha identificado una serie de medidas globales para mitigar dichos riesgos. Aunque el proceso todavía continúa en algunos Estados miembros, una gran mayoría de ellos ya ha endurecido o están endureciendo los requisitos de seguridad de las redes 5G sobre la base de la caja de herramientas de la UE.

La caja de herramientas de la UE ofrece un marco global para hacer frente a los riesgos de seguridad de la 5G.

83. La 5G constituye un gran avance, un cambio importante en comparación con la 4G, por lo que el principal reto para evitar la brecha digital es la transición de la 4G a la 5G en toda la UE.

Las especificaciones de la 5G abarcan todo un conjunto de indicadores de rendimiento, especialmente en relación con los casos verticales de uso. Esto puede implicar, entre otras cosas, requisitos de fiabilidad, la rapidez de la instanciación del servicio, la flexibilidad de la aplicación y los niveles de seguridad.

Recomendación 1 — Promover un despliegue uniforme y oportuno de las redes 5G en la UE

a) La Comisión acepta la recomendación.

La Comisión colaborará con los Estados miembros en el desarrollo de una definición común de la calidad de servicio que deben ofrecer las redes 5G. En el contexto de la Década Digital y de la propuesta de Decisión sobre el Programa de Política Digital para 2030, la Comisión tiene la intención de trabajar con los Estados miembros en un planteamiento común de la calidad del servicio de la 5G en la UE, así como para la comparabilidad de las mediciones y los datos de supervisión.

La calidad del servicio no solo implica velocidad y latencia, sino que abarca toda una gama de indicadores de rendimiento, especialmente en relación con los casos de uso vertical.

La Comisión tiene la intención de colaborar con los Estados miembros para definir dichas mediciones, así como de realizar comprobaciones anuales y recomendar políticas, medidas y acciones para lograr la cobertura total de la 5G de aquí a 2030.

El Programa de Política Digital establecerá una gobernanza sólida a través de un mecanismo de supervisión y cooperación para garantizar el progreso hacia el cumplimiento de los objetivos del Programa Político, incluido el despliegue de la 5G, y recomendará medidas correctoras a los Estados miembros a este respecto.

b) La Comisión acepta la recomendación.

c) La Comisión acepta la recomendación.

Recomendación 2 — Fomentar un planteamiento concertado sobre la seguridad de la tecnología 5G entre los Estados miembros

a) La Comisión acepta la recomendación.

La Comisión evaluará, junto con los Estados miembros, la necesidad de nuevas medidas o apoyo, por ejemplo en forma de orientaciones relativas a determinados aspectos de la caja de herramientas de la UE.

b) La Comisión acepta la recomendación.

La Comisión realizará el seguimiento y la presentación de informes, en plena colaboración con los Estados miembros y la ENISA.

c) La Comisión acepta la recomendación.

Recomendación 3 — Tener en cuenta los efectos que los enfoques divergentes de los Estados miembros con respecto a la seguridad de la tecnología 5G tienen en el funcionamiento eficaz del mercado interior

a) La Comisión acepta la recomendación.

b) La Comisión acepta la recomendación.

La Comisión llevará a cabo la evaluación teniendo en cuenta las competencias nacionales.

En el marco de la caja de herramientas de la UE, corresponde a los Estados miembros decidir el alcance exacto de las restricciones o exclusiones necesarias en el caso de los activos clave definidos como críticos y sensibles en la evaluación de riesgos coordinada en la UE (por ejemplo, funciones de red básicas, funciones de gestión y orquestación de red y funciones de red de acceso), a fin de mitigar eficazmente los riesgos identificados, teniendo también en cuenta la evaluación de las amenazas realizada por los servicios de inteligencia nacionales. Los Estados miembros tienen derecho a adoptar medidas relacionadas con la seguridad nacional, incluidas posibles restricciones o exclusiones de proveedores de alto riesgo.