COMISIÓN
EUROPEA

Bruselas, 29.1.2020
COM(2020) 50 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE

1. Introducción

La quinta generación (5G) de redes de telecomunicaciones desempeñará un papel fundamental en el desarrollo de la sociedad y la economía europeas. De ellas se espera que ofrezcan enormes oportunidades económicas y ofrezcan un importante punto de partida para la transformación digital y ecológica en ámbitos tales como los de transportes, energía, fabricación, sanidad, agricultura y medios de comunicación.

La 5G, pues, podría repercutir en prácticamente todos los aspectos de la vida de los ciudadanos de la UE. De ahí que la ciberseguridad de las redes 5G sea primordial no solo para proteger nuestras economías, sociedades y procesos democráticos, sino también para garantizar una transformación digital que se desarrolle en un clima de confianza y beneficie conjunto de la ciudadanía de la UE.

Por depender muchos servicios esenciales de las redes 5G, cualquier perturbación sistémica y generalizada tendría consecuencias especialmente graves y, dado el carácter interconectado de los ecosistemas digitales, repercusiones que podrían ser significativas más allá de las fronteras nacionales. Por tanto, garantizar la ciberseguridad de las redes 5G es cuestión de importancia estratégica para la Unión en un momento en el que los ciberataques van en aumento, son más sofisticados que nunca y vienen de toda clase de agentes, en particular de agentes de Estados no miembros de la UE o que cuentan con su respaldo. En materia de seguridad de infraestructuras críticas tales como la 5G, el planteamiento elegido consiste en definir por primera vez un enfoque europeo común. Este enfoque respeta plenamente el carácter abierto del mercado interior de la UE a condición de que a su vez se respeten sus requisitos de seguridad basados en los riesgos.

El Consejo Europeo de 22 de marzo de 2019 abogaba por un enfoque concertado en materia de seguridad de las redes 5G. El 26 de marzo de 2019, la Comisión adoptó la Recomendación (UE) 2019/534 sobre ciberseguridad de las redes 5G[1]. En ella se insta a los Estados miembros a completar sus evaluaciones nacionales de riesgos y revisar las medidas nacionales, a trabajar conjuntamente en la UE sobre una evaluación de riesgos coordinada y a elaborar una caja de herramientas compuesta por posibles medidas de mitigación. La presente Comunicación forma parte integrante de la estrategia europea global de la Comisión para el sector digital por la que abogaba el Consejo Europeo.

2. Despliegue de la 5G en la UE

Para la estrategia industrial y la competitividad europeas, el despliegue de la infraestructura de red 5G en Europa es fundamental. La Comisión ha reconocido el despliegue de las tecnologías de red en la 5G como factor importante para el futuro de los servicios digitales. En 2016, la Comisión adoptó el Plan de Acción 5G para garantizar que a partir de 2020 la Unión contara con la infraestructura de conectividad necesaria para su transformación digital y para desplegarla de modo general en las zonas urbanas y las principales vías de transporte hasta 2025[2]. La Comunicación relativa a la sociedad del Gigabit declara la ambición de

[1] Recomendación (UE) 2019/534, relativa a la ciberseguridad de las redes 5G, DO L 88 de 29.3.2019, p. 42-47.
[2] COM (2016) 588, de 14 de junio de 2016, sobre la 5G para Europa: un plan de acción.

garantizar el acceso a la conectividad de datos móviles en todas partes[3], incluso en zonas rurales y remotas.

En cuanto a la asignación de frecuencias, los Estados miembros han asignado el 16 % de las bandas pioneras de 5G[4]. Dada la obligación legal de permitir el uso de todas las bandas pioneras 5G antes de que termine el año, en los próximos meses se espera celebrar consultas sobre una serie de procedimientos de asignación.

Europa es una de las regiones más avanzadas del mundo por lo que a lanzamiento comercial de servicios 5G se refiere[5]. En estos momentos se prevé que a finales de 2020 estén disponibles en 138 ciudades europeas los primeros servicios 5G. Las primeras redes 5G se basan en la actual cuarta generación (4G) de tecnologías de redes, y los servicios de 5G se prestan principalmente al público en general, ya sea en forma de mejora de la 4G en cuanto a capacidad y velocidad o como alternativa inalámbrica rentable a las redes fijas[6].

Por lo que se refiere a las oportunidades de nuevos servicios de empresa a empresa —en sectores como los de energía, alimentación y agricultura, sanidad, fabricación o transportes—, Europa avanza a buen paso gracias a una inversión del orden de 1 000 millones de euros, que incluye fondos europeos por valor de 300 millones de euros dentro de la asociación público privada para la 5G englobada en Horizonte 2020. Esta inversión incluye más de 160 pruebas de 5G a gran escala en Europa, incluidos diez corredores transfronterizos en autopistas transfronterizas para ensayos a gran escala de servicios de movilidad conectada y automatizada basados en la 5G. Las pruebas incluyen aplicaciones basadas en la 5G en sectores que van desde una sanidad sostenible y una agricultura automatizada y con un uso eficiente de recursos móviles hasta unas redes eléctricas inteligentes y la Industria 4.0. Además, el BEI, con el apoyo del Fondo Europeo para Inversiones Estratégicas, ha facilitado préstamos para acelerar la investigación y el desarrollo de la tecnología 5G.

El Código Europeo de las Comunicaciones Electrónicas («el Código»)[7], que se aplicará a partir del 21 de diciembre de 2020, es una base importante a la hora de crear un entorno favorable a la inversión para las redes de 5G y posteriores. Pero, para apoyar el futuro despliegue de redes 5G, también serán esenciales programas de financiación pública tales como el Mecanismo «Conectar Europa» – Sector digital»[8] o los Fondos Estructurales y de Inversión Europeos en particular, al conectar las comunidades a servicios posibilitados por la 5G tales como escuelas, hospitales, ciudades y administraciones locales.

Dadas las oportunidades estratégicas de Europa en cuanto a servicios de 5G para diversas industrias, será de vital importancia que los operadores y proveedores de servicios inviertan

[3] COM(2016) 587 «La conectividad para un mercado único digital competitivo - hacia una sociedad europea del Gigabit».

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Algunas de las nuevas funcionalidades de la 5G se introducirán por etapas. En una primera fase (a corto o muy corto plazo), el despliegue de la 5G consistirá principalmente en redes «autónomas» en las que solo se actualizará a la tecnología 5G la red de acceso radio, pero que, por lo demás, seguirán dependiendo de las redes básicas de 4G y ofrecerán a los usuarios finales un mejor rendimiento de la banda ancha móvil. En las fases siguientes (a corto o medio plazo hasta a largo plazo), el despliegue de redes 5G «autónomas», incluidas las funciones de la red básica 5G, requerirá y, con el tiempo, implicará un cambio mucho más amplio de la arquitectura de red.

[7] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas (texto refundido).

[8] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el Mecanismo «Conectar Europa» y se derogan los Reglamentos (UE) n.º 1316/2013 y (UE) n.º 283/2014

en redes y servicios avanzados de 5G. Estos no solo requerirán nuevas redes de radio 5G, sino también nuevas redes de 5G «autónomas» que ofrezcan funcionalidades avanzadas de 5G tales como fragmentación de la red[9] y computación en el borde[10].

La Comisión seguirá apoyando el despliegue de la 5G en la UE, en particular mediante la colaboración con los Estados miembros y las partes interesadas a fin de aprovechar las oportunidades que ofrece la 5G. Se tendrán debidamente en cuenta los aspectos relacionados con la salud, basándose en el principio de precaución[11] y en cooperación con las organizaciones internacionales correspondientes y la comunidad científica.

3. La evaluación coordinada por la UE de los riesgos en materia de ciberseguridad en las redes 5G

Trabajando conjuntamente en el Grupo de Cooperación para la Seguridad de las Redes y Sistemas de Información (SRI)[12], cada uno de los Estados miembros ha completado su propia evaluación nacional de riesgos para sus infraestructuras de red 5G, cuyos resultados transmitió a principios de julio de 2019 a la Comisión y la ENISA (Agencia de la Unión Europea para la Ciberseguridad).

A partir de las evaluaciones nacionales de riesgos, el 9 de octubre de 2019, el Grupo de Cooperación en materia de SRI —formado por representantes de los Estados miembros, la Comisión y la ENISA— publicó un informe de evaluación de riesgos coordinada en la UE para la ciberseguridad en las redes 5G[13]. El informe enumera las principales amenazas y agentes de riesgo, los activos más delicados y los principales puntos vulnerables (tanto técnicos como de otro tipo) que afectan a las redes 5G. Partiendo de esta base, el informe establece una serie de categorías de riesgos de importancia estratégica desde el punto de vista de la UE, ilustradas por escenarios de riesgo concretos que reflejan combinaciones de los distintos parámetros (vulnerabilidades, amenazas y agentes de riesgo) en relación con los distintos activos (véase el apéndice).

Para complementar este informe y como nuevo componente de la caja de herramientas, la ENISA elaboró un panorama específico de amenazas[14] que recoge un análisis detallado de una serie de aspectos técnicos y se centra en los activos de red y las amenazas que sobre ellos penden.

El informe de evaluación de riesgos coordinada en la UE se centra en una serie de aspectos importantes para las redes 5G. Concretamente:

---

[9] La fragmentación de la red 5G permite un alto grado de separación entre las distintas capas de servicio en una misma red física, lo que aumenta las posibilidades de ofrecer servicios diferenciados en toda la red.

[10] La computación en el borde es un paradigma de computación distribuida que acerca la computación y el almacenamiento de datos al lugar donde se necesitan a fin de mejorar los tiempos de respuesta y ahorrar ancho de banda.

[11] Recomendación del Consejo, de 12 de julio de 1999, relativa a la exposición del público en general a campos electromagnéticos (0 Hz a 300 GHz) (1999/519/CE).

[12] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión («Directiva SRI»). Para garantizar la cooperación estratégica y el intercambio de información sobre ciberseguridad entre los Estados miembros de la UE, la Directiva SRI estableció el Grupo de Cooperación en materia de SRI.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[14] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

a) Los cambios tecnológicos introducidos por la 5G aumentarán la superficie de ataque en general y el número de posibles puntos de entrada para los atacantes:

- Una funcionalidad mejorada en el borde de la red y una arquitectura menos centralizada que en generaciones anteriores de redes móviles implica que algunas funciones de las redes básicas pueden integrarse en otras partes de las redes, lo que hace más sensibles los equipos correspondientes (por ejemplo, estaciones base o funciones MANO);

- El mayor papel del software en los equipos 5G implica un aumento de los riesgos ligados a los procesos de desarrollo y actualización de software, crea nuevos riesgos de errores de configuración y da un papel más importante dentro del análisis de seguridad a las opciones elegidas por cada operador de redes móviles en la fase de despliegue de la red.

b) Estas nuevas características tecnológicas darán mayor relevancia a la confianza de los operadores de redes móviles en los proveedores terceros y a su papel dentro de la cadena de suministro de la 5G.

Esto, a su vez, incrementará el número de vías de ataque que podrán aprovechar los agentes de riesgo y, en particular, los agentes de Estados no miembros de la UE o que cuenten con su respaldo debido a su capacidad (intención y recursos) de atentar contra las redes de telecomunicaciones de los Estados miembros de la UE y a la potencial gravedad de las consecuencias de tales atentados.

En este contexto de mayor exposición a atentados facilitados por proveedores terceros, será especialmente importante el perfil de riesgo de cada proveedor, en particular si tiene una presencia significativa en determinadas redes o zonas.

c) Una gran dependencia de un único proveedor aumenta la exposición y las consecuencias de un posible fallo del mismo. También agrava el efecto potencial de los puntos débiles o vulnerables y su posible aprovechamiento por agentes de riesgo, en particular en caso de dependencia de un proveedor que presente un alto grado de riesgo.

d) Si algunos de los nuevos casos de uso de la 5G previstos llegan a buen puerto, las redes 5G terminarán siendo una parte importante de la cadena de suministro de muchas aplicaciones informáticas críticas, lo que no solo afectará a los requisitos de confidencialidad y privacidad, sino que, además, convertirá la integridad y disponibilidad de esas redes en cuestión primordial de seguridad nacional y en un gran reto de seguridad para la UE.

Fuente: Evaluación de riesgos coordinada en la UE

Por lo demás, el informe de evaluación de riesgos coordinada en la UE concluye que estos retos crean un nuevo paradigma de seguridad que hace necesario reevaluar el actual marco político y de seguridad aplicable al sector de la 5G y a su ecosistema, para lo cual es fundamental que los Estados miembros adopten las medidas de mitigación necesarias.

Para abordar eficazmente los riesgos detectados y reforzar la seguridad y resistencia de las redes 5G se requiere un enfoque amplio, lo que implica tomar una serie de medidas clave y medidas de apoyo asociadas para abordar los riesgos al mismo tiempo. La evaluación de

riesgos coordinada en la UE sienta la base para determinar las medidas de mitigación que pueden aplicarse en los ámbitos nacional y europeo.

Las Conclusiones del Consejo de 3 de diciembre de 2019 corroboran las conclusiones de la evaluación coordinada de riesgos y subrayan «la importancia de un enfoque coordinado y de la aplicación efectiva de la Recomendación, para evitar la fragmentación del mercado único»[15]. A tal fin, el Consejo insta a los Estados miembros, la Comisión y la ENISA a tomar «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 [a seguir] consolidando un planteamiento coordinado para atender los problemas de seguridad de las tecnologías 5G».

4. La caja de herramientas de la UE sobre ciberseguridad de la 5G

El 29 de enero de 2020, el Grupo de Cooperación en materia de SRI publicó la caja de herramientas de la UE para medidas de reducción del riesgo[16]. En ella se abordan todos los riesgos enumerados en el informe de evaluación coordinada de riesgos.

La caja de herramientas de la UE enumera y describe una serie de medidas estratégicas y técnicas acompañadas de medidas de apoyo destinadas a reforzar su eficacia a la hora de mitigar los riesgos observados. Las **medidas estratégicas** incluyen medidas para dotar a las administraciones de mayores competencias reglamentarias para supervisar la contratación y el despliegue de las redes, medidas específicas para abordar los riesgos relacionados con vulnerabilidades no técnicas y posibles iniciativas para impulsar una cadena de valor y suministro de 5G sostenible y diversa y evitar riesgos sistémicos de dependencia a largo plazo. Las **medidas técnicas** incluyen medidas para reforzar la seguridad de las redes y equipos de 5G abordando los riesgos derivados de las tecnologías, los procesos y los factores humanos y físicos. Además, en cada una de las áreas de riesgo señaladas en la evaluación de riesgos coordinada en la UE se contemplan **planes de mitigación del riesgo** basados en las medidas de mayor eficacia.

Entre ellas, las conclusiones de la caja de herramientas de la UE acordadas por el Grupo de Cooperación en materia de SRI recomiendan un conjunto de **medidas clave** que deberán aplicar todos los Estados miembros y la Comisión:

Conclusiones de la caja de herramientas de la UE

La caja de herramientas de la UE contempla una serie de medidas y acciones que, si se combinan de forma adecuada y se aplican con eficacia, son la base de un enfoque coordinado en este campo. Y es que, dada la gran variedad de áreas de riesgo descritas en la evaluación de riesgos coordinada en la UE y su diversa naturaleza, para atender a todas las áreas de riesgo clave no bastará con un único tipo de medidas, sino que será necesaria toda una serie de medidas aplicadas en una combinación adecuada.

Basándose en la evaluación de los posibles planes de mitigación y la lista de medidas más eficaces, en la caja de herramientas se recomienda:

[15] Conclusiones del Consejo sobre la importancia de la 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G. 3 de diciembre de 2019 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

[16] Ciberseguridad de las redes 5G - Caja de herramientas de la UE: medidas de mitigación de riesgos, 29 de enero de 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

1. Todos los Estados miembros deben asegurarse de contar con medidas (incluidas competencias para las administraciones nacionales) que les permitan responder de forma adecuada y proporcionada a los riesgos actuales y futuros y, en particular, asegurarse de poder restringir, prohibir o imponer requisitos o condiciones específicos al suministro, despliegue y explotación de equipos de red 5G en función de una serie de motivos de seguridad y según un enfoque basado en el riesgo.

En particular, deben:

- *reforzar los **requisitos de seguridad** para los operadores de redes móviles (por ejemplo, controles de acceso estrictos, normas de funcionamiento y supervisión seguros, límites a la externalización de determinadas funciones, etc.);*

- *evaluar el perfil de riesgo de los proveedores y, en consecuencia, **aplicar las restricciones que correspondan a los proveedores considerados de alto riesgo, incluidas las exclusiones necesarias para reducir eficazmente los riesgos 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);*

- *velar por que todo operador cuente con una estrategia adecuada y basada en múltiples proveedores que permita **evitar o limitar cualquier dependencia importante** respecto de un único proveedor (o proveedores con perfiles de riesgo similares), garantizar un adecuado equilibrio entre proveedores nacionales y **evitar la dependencia de proveedores considerados de alto riesgo**; esto requiere asimismo evitar situaciones de cautividad con respecto a un único proveedor, entre otras cosas, fomentando una mayor interoperabilidad de los equipos.*

2. La Comisión Europea, conjuntamente con los Estados miembros, debe contribuir a:

- *mantener una **cadena de suministro de la 5G diversa y sostenible** a fin de evitar situaciones de dependencia a largo plazo, para lo cual, entre otras cosas:*

  *o se hará pleno uso de las herramientas e instrumentos de la UE existentes, en particular, mediante el control de las potenciales **inversiones extranjeras directas** que afecten a los activos clave de la 5G y evitando **falseamientos** del mercado de suministro de la 5G debidos a posibles prácticas de dumping o subvenciones; y*

  *o se reforzarán las **capacidades de la UE en tecnologías de 5G y posteriores a la 5G** utilizando los programas y la financiación de la UE que correspondan.*

- *facilitar la coordinación entre los Estados miembros en materia de **normalización** para alcanzar objetivos de seguridad específicos y desarrollar **el sistema o sistemas de certificación pertinentes para toda la UE** con vistas a impulsar productos y procesos más seguros.*

3. Para garantizar que este enfoque coordinado supere la prueba del tiempo, deberá ampliarse el mandato del Grupo de Cooperación en materia de SRI y la cooperación con otros organismos y entidades pertinentes, en particular, a fin de:

- *revisar periódicamente, con el apoyo de la Comisión y de la ENISA, las **evaluaciones de riesgos nacionales y de la UE** sobre la seguridad de las redes 5G y posteriores a la 5G elaborando y ajustando la metodología de evaluación seguida y adaptándola a la evolución de la tecnología 5G;*

- *efectuar un **seguimiento y una evaluación detallados y periódicos de la aplicación** de la caja de herramientas basados en informes estructurados por parte de los Estados miembros;*

- *coordinar y apoyar la aplicación de las **medidas de apoyo** que requieran cooperación dentro de la UE, sobre todo a la hora de elaborar orientaciones e intercambiar mejores prácticas sobre las diversas medidas;*

- *apoyar una posible coordinación ulterior dentro de la UE, en particular para lograr una mayor convergencia en torno a los **requisitos de seguridad técnica y organizativa para los operadores de redes**.*

Fuente: Caja de herramientas de la UE.

Las conclusiones de la caja de herramientas demuestran la firme disposición de los Estados miembros a responder en común a los retos de seguridad para las redes 5G. Esto es fundamental para la seguridad dentro de los Estados miembros y en toda la UE, para las economías nacionales y para el mercado interior de la UE y la soberanía tecnológica de Europa. Tanto la evaluación de riesgos coordinada en la UE como la caja de herramientas son prueba del gran valor del trabajo colectivo realizado en el Grupo de Cooperación en materia de SRI y de la intensa colaboración desarrollada entre los representantes de todos los Estados miembros, la Comisión y la ENISA.

La caja de herramientas permite un enfoque común de la UE en materia de ciberseguridad de la 5G que favorece la coherencia en todo el mercado interior a través de las políticas y la coordinación europeas y facilita el ejercicio de las competencias de los Estados miembros, en particular por lo a seguridad nacional se refiere. Las medidas y planes de mitigación que contiene hacen posible una respuesta adecuada, eficaz y proporcionada de la UE ante los retos comunes de ciberseguridad de la 5G.

La Comisión saluda la publicación de la caja de herramientas de la UE sobre ciberseguridad de 5G y apoya plenamente todas las conclusiones en ella recogidas y anteriormente enumeradas.

La Comisión insta a los Estados miembros y a las instituciones, agencias y demás organismos de la Unión a:

i) garantizar la rápida aplicación en toda la UE de estrategias eficaces y adecuadas de reducción del riesgo acordes con la caja de herramientas de la UE, y

ii) adoptar cuantas medidas adicionales sean necesarias para garantizar la coordinación dentro de la Unión, entre otras cosas, prosiguiendo los trabajos del Grupo de Cooperación en materia de SRI y estableciendo un mecanismo sólido para supervisar la aplicación de la caja de herramientas de la UE a fin de garantizar la eficacia de las medidas y el buen funcionamiento del mercado interior.

5. Aplicación de la caja de herramientas

Para un enfoque europeo creíble y eficaz en materia de seguridad de la 5G es fundamental la determinación de los Estados miembros a hacer pleno uso de la caja de herramientas. Si bien serán los Estados miembros quienes decidan, en función de sus circunstancias nacionales, si cada medida concreta es adecuada, es absolutamente fundamental aplicar **en el ámbito de cada Estado miembro —y, en algunos casos, el europeo— una serie de medidas clave recomendadas por el Grupo de Cooperación en materia de SRI (véanse las conclusiones de la caja de herramientas)** a fin de atender a los riesgos observados.

La Comisión está dispuesta a seguir prestando todo su apoyo durante las siguientes fases e insta a los Estados miembros:

- a tomar **a más tardar el 30 de abril de 2020** medidas concretas y cuantificables para aplicar el conjunto de medidas clave recomendadas en las conclusiones de la caja de herramientas de la UE;

- a elaborar **a más tardar el 30 de junio de 2020** un informe del Grupo de Cooperación en materia de SRI sobre el estado de aplicación de dichas medidas clave en cada Estado miembro, basado en los informes y la supervisión periódicos efectuados, en particular, en el Grupo de Cooperación en materia de SRI y con el apoyo de la Comisión y la ENISA.

5.1. Un enfoque concertado y basado en los riesgos para los proveedores de 5G

Dado el objetivo último de garantizar la seguridad y la resistencia de las redes 5G y su sostenibilidad, los Estados miembros coinciden en la necesidad de evaluar el perfil de riesgo de cada proveedor y, en consecuencia, de aplicar las restricciones pertinentes a los proveedores considerados de alto riesgo, incluidas las exclusiones necesarias a fin de mitigar eficazmente los riesgos para los activos clave, tal como se indica en la caja de herramientas. La Comisión está dispuesta a apoyar a los Estados miembros a la hora de aplicar estas medidas.

Para apoyar su aplicación en toda la Unión, la evaluación de riesgos coordinada en la UE y la caja de herramientas de la UE ofrecen orientaciones sobre 1) la evaluación del perfil de riesgo de los proveedores[17] y 2) la sensibilidad de los elementos y funciones de red[18], así como otros activos. Tanto la evaluación de riesgos coordinada en la UE como las medidas de la caja de herramientas contemplan los riesgos relacionados con los proveedores de equipos y servicios de red 5G. No incluyen los demás productos o servicios que estos u otros proveedores puedan suministrar.

Tal como se indica en el punto 2.37 de la evaluación de riesgos coordinada en la UE, los perfiles de riesgo de los proveedores individuales pueden evaluarse a partir de diversos factores.

La evaluación de los perfiles de riesgo de los proveedores únicamente debe obedecer a motivos de seguridad y basarse en criterios objetivos. Para facilitar un enfoque coordinado de la aplicación de estas medidas, en la caja de herramientas se recomienda que los Estados miembros intercambien información sobre enfoques y mejores prácticas nacionales. La Comisión considera además que esta debe ser una de las primeras prioridades de la próxima fase de los trabajos del Grupo de Cooperación en materia de SRI desarrollados conjuntamente con la Comisión y la ENISA.

Es importante introducir de manera oportuna restricciones a los proveedores considerados de alto riesgo —incluidas las exclusiones necesarias para reducir eficazmente los riesgos— y medidas destinadas a evitar la dependencia respecto de estos proveedores. Hacerlo cuanto

[17] Punto 2.37 de la evaluación de riesgos coordinada en la UE.

[18] El punto 2.21 de la evaluación de riesgos coordinada en la UE presenta las principales categorías de elementos y funciones, con su nivel general de sensibilidad, y enumera una serie de elementos clave determinados en cada categoría por los Estados miembros, mientras que en los puntos 2.28 y 2.29 se enumeran otros tipos de activos o áreas sensibles (por ejemplo, entidades o áreas geográficas específicas).

antes, en particular y a ser posible en el caso de los procesos de concesión de licencias de frecuencias 5G, también aumentará la previsibilidad para los operadores del mercado, lo que contribuirá a un despliegue rápido y garantizará la seguridad a largo plazo de las redes 5G, así como la resiliencia de la cadena de suministro de la 5G.

Al mismo tiempo, en casos necesarios y justificados, al aplicarse estas medidas en el ámbito nacional podrán fijarse plazos diferentes, sobre todo si existe un alto grado de dependencia respecto de proveedores de equipos o servicios considerados de alto riesgo (por ejemplo, teniendo en cuenta los ciclos de actualización de equipos y, en particular, la migración de las redes 5G «no autónomas» a las «autónomas»). Los Estados miembros podrían plantearse la posibilidad de definir planes de aplicación que incluyan períodos de transición adecuados para los operadores de redes afectados. En ese caso, los períodos de transición deben definirse de manera que se preserven, o incluso se refuercen, los incentivos para invertir en equipos de red modernos, lo que incluye acelerar el despliegue de redes básicas completas («autónomas») de 5G y la sustitución de los equipos 4G existentes en otras partes de las redes (por ejemplo, en la red de acceso radioeléctrico), en consonancia con los objetivos del Plan de Acción 5G[19].

Además, y dada la complejidad de las redes 5G, los operadores de telecomunicaciones podrían recurrir cada vez más a entidades terceras para realizar determinadas tareas tales como las de mantenimiento y mejora de las redes y programas informáticos 5G y a otros servicios externalizados, además del suministro de equipos de red. Tal como se explica en la evaluación de riesgos coordinada de la UE, se trata de una fuente de graves riesgos para la seguridad, por lo que debe prestarse especial atención a este aspecto. Es fundamental hacer una evaluación de seguridad exhaustiva del perfil de riesgo de los proveedores responsables de estos servicios, sobre todo cuando las tareas en cuestión no se lleven a cabo en la UE. A fin de preservar la integridad a largo plazo de la infraestructura 5G, deben tomarse las medidas adecuadas, incluidas restricciones, sobre todo, en partes sensibles de las redes 5G, o la exclusión obligatoria de las entidades de alto riesgo, en consonancia con las medidas de mitigación contempladas en la caja de herramientas.

5.2. El papel de la Comisión en el apoyo a la aplicación de la caja de herramientas

La Comisión seguirá apoyando la aplicación del enfoque de la UE en materia de ciberseguridad de la 5G en general y emprendiendo iniciativas específicas en relación con las medidas y objetivos de la caja de herramientas que puedan aportar un valor añadido. Para atender a las cuestiones de seguridad observadas y en la medida necesaria, la Comisión hará pleno uso de sus competencias e instrumentos pertinentes. De esta manera, y actuando conjuntamente con los Estados miembros y el sector privado, la Comisión quiere impulsar medidas estratégicas que contribuyan a garantizar la soberanía y el liderazgo tecnológico de la UE en el futuro desarrollo de las tecnologías de red, las tecnologías de ciberseguridad y todos los componentes de que dependen nuestra economía y nuestra seguridad.

Más concretamente, y para garantizar la aplicación en sus ámbitos de competencia de las correspondientes medidas de mitigación de la caja de herramientas, la Comisión tomará las siguientes medidas:

Salvaguardia de la ciberseguridad de las redes 5G y de una cadena de valor diversificada para la 5G:

[19] COM (2016) 588, de 14 de septiembre de 2016, sobre la 5G para Europa: un plan de acción.

- **Cooperación en materia de ciberseguridad**: seguir prestando apoyo a los Estados miembros para la aplicación efectiva, coordinada y oportuna de las medidas nacionales a través del Grupo de Cooperación en materia de SRI.

- **Normas sobre telecomunicaciones y ciberseguridad**: prestar 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 estudiar 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.

- **Normalización**: tomar medidas para mantener y, en su caso, aumentar la participación europea en los respectivos organismos de normalización a fin de alcanzar los objetivos de seguridad e interoperabilidad de Europa. En particular, la Comisión, junto con los Estados miembros, evaluará e impulsará normas y especificaciones técnicas que permitan la interoperabilidad entre los proveedores de equipos de 5G en diferentes partes de la red, incluidas las redes ya existentes, a fin de hacer posible un verdadero entorno de proveedores múltiples, por ejemplo, mediante interfaces abiertas e interoperables.

- **Certificación**: apoyar el desarrollo de regímenes de certificación de la 5G que aborden las necesidades de las redes 5G dentro del marco europeo de certificación de la ciberseguridad.

- **Control de las inversiones extranjeras directas (IED)**: apoyar la aplicación del marco de control de la UE haciendo inventario de la cadena de valor de la 5G —incluidos los activos de red sensibles— y con un seguimiento periódico de las IED a lo largo de la cadena de valor. Con arreglo al calendario de control de las IED (en octubre de 2020), la Comisión estudiará las inversiones extranjeras en el ámbito de la 5G a la luz de las directrices establecidas en el Reglamento (CE) n.º EU2019/452 y teniendo en cuenta la evaluación de riesgos coordinada en la UE y la caja de herramientas de la UE.

- **Instrumentos de defensa comercial**: supervisar todas las novedades de interés en los mercados de la UE y de terceros países y proteger a los operadores de la UE en el mercado europeo de la 5G a través de medidas de defensa comercial contra posibles prácticas de distorsión del comercio (dumping o subvenciones), incluso, en su caso, poniendo en marcha investigaciones preliminares.

- **Normas de competencia:** supervisar el funcionamiento de los mercados de suministro de hardware y software de 5G para garantizar que produzcan resultados competitivos, sobre todo en relación con posibles situaciones de cautividad contractual o técnica.

- **Programas de financiación europeos**: garantizar que la participación en los programas de financiación de la UE en los ámbitos tecnológicos pertinentes se supedite al cumplimiento de requisitos de seguridad, utilizando plenamente y aplicando condiciones de seguridad en los programas de I + D, en particular Horizonte Europa, el programa Europa Digital y el Mecanismo «Conectar Europa» 2, los Fondos Estructurales y de Inversión Europeos y otros programas pertinentes. Debe adoptarse un enfoque similar en los programas de financiación exterior y los instrumentos financieros de la UE, en particular por lo que se refiere a la financiación a través de las instituciones financieras internacionales.

- **Contratación pública:** impulsar la contratación pública en el área de las redes 5G para apoyar los objetivos de seguridad establecidos, la diversidad de proveedores y la sostenibilidad a largo plazo de las redes 5G; en particular, tratar de garantizar que se preste la debida atención a los aspectos de seguridad a la hora de adjudicar contratos públicos en el área de las redes 5G, de acuerdo con las normas de contratación pública de la UE.

- **Respuesta a incidentes y gestión de crisis (Plan director) y ejercicios de ciberseguridad**: aprovechar plenamente el desarrollo del Plan director de la UE[20] para la respuesta coordinada a incidentes de ciberseguridad a gran escala; además, y conjuntamente con la ENISA, estudiar la posibilidad de efectuar un ejercicio de ciberseguridad de la 5G tan pronto como la madurez del mercado lo permita.

Y, bajo la responsabilidad del alto representante de la Unión para Asuntos Exteriores y Política de Seguridad y Vicepresidente de la Comisión, así como del Consejo:

- **Marco para la respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»)[21]:** para prevenir actividades informáticas malintencionadas que amenacen a la integridad y la seguridad de la UE, se anima a los Estados miembros a aplicar las medidas pertinentes de política exterior y de seguridad común contempladas en el conjunto de instrumentos de ciberdiplomacia (incluidas, en su caso, medidas restrictivas) para fomentar la cooperación, facilitar la mitigación de amenazas e influir en el comportamiento de los potenciales agresores.

Por otra parte, una serie de programas contribuirá a alcanzar los objetivos de evitar o limitar el riesgo de dependencia a largo plazo promoviendo un mercado diversificado y sostenible para la 5G, en particular manteniendo las capacidades de la UE en la cadena de valor de la 5G e invirtiendo en innovación, de acuerdo con las obligaciones internacionales de la UE.

Promover la innovación e invertir en ciberseguridad y tecnologías de infraestructura de red:

- **Programas** de financiación de la UE: aumentar las inversiones en investigación, innovación y despliegue de tecnologías de red y de sus componentes básicos. Dentro del próximo presupuesto de la UE para 2021-2027, la Comisión ha propuesto destinar cerca de 3 000 millones de euros a inversiones en tecnologías de ciberseguridad. Esto incluye la investigación y la innovación, a través de Horizonte Europa, y el apoyo a las capacidades de ciberseguridad, a través del programa Europa Digital. InvestEU también puede prestar apoyo financiero a la investigación y el desarrollo en el ámbito de la 5G y ayudar a su despliegue.

[20] Recomendación de la Comisión relativa a una respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (UE 2017/1584).
[21] Conclusiones del Consejo de 20 de junio de 2017, 9916/17.

Además, y en el marco del próximo programa Horizonte Europa[22], la Comisión ha propuesto establecer en la UE una asociación institucionalizada en materia de nueva generación de internet y 6G («Redes y servicios inteligentes») en colaboración con la industria y en coordinación con los Estados miembros para completar el despliegue de la 5G y, sobre todo, para **preparar la 6G**, próxima generación de tecnología móvil. Para esta iniciativa se han propuesto más de 2 500 millones de euros de inversiones de la UE con cargo a su presupuesto 2021-2027, a los que se añadirá un mínimo de 7 500 millones de euros en inversiones privadas.

- **Desarrollo y despliegue industrial**: evaluar las posibles deficiencias o fallos del mercado a lo largo de la cadena de valor de la 5G que justificarían intervenciones específicas en el marco del próximo presupuesto a largo plazo o un posible PIICE (Proyecto Importante de Interés Común Europeo) sobre ciberseguridad, siguiendo las sugerencias del foro de alto nivel sobre los PIICE. La decisión de elaborar y aplicar PIICE corresponde a los Estados miembros y las empresas. Las normas de la UE crean el marco propicio, y la Comisión está dispuesta a facilitar los contactos necesarios y ofrecer orientaciones.

[22] También puede facilitarse financiación a través del Mecanismo «Conectar Europa» (MCE) 2.0 y el programa Europa Digital.

6. Conclusión

Las redes 5G auguran toda clase de oportunidades para los ciudadanos, la sociedad y la economía europeas. Por tanto, es fundamental garantizar su seguridad y resistencia. Al mismo tiempo, las amenazas a la ciberseguridad (incluido el riesgo de intromisión de agentes de Estados no miembros de la UE o que cuenten con su respaldo) son un reto en constante evolución y cuya importancia aumenta al ritmo de la creciente dependencia de la tecnología y los datos. No atender a la ciberseguridad socavaría la confianza en el desarrollo de la economía y la sociedad digitales e impediría a la UE aprovechar todas sus ventajas. De ahí la necesidad de una respuesta más enérgica y flexible.

Para que la UE garantice su soberanía tecnológica y mantenga y desarrolle sus capacidades industriales, es fundamental que exista en la Unión un enfoque coordinado y coherente en materia de ciberseguridad de las tecnologías y redes críticas. La Comisión apoyará plenamente la aplicación del enfoque de la UE en materia de ciberseguridad de las redes 5G y garantizará al mismo tiempo la apertura de los mercados de la UE a productos y servicios que atiendan a la evolución de los requisitos sobre ciberseguridad y confianza.

Para ello es importante que se mantenga el firme compromiso de todas las partes interesadas con la seguridad de la 5G y será preciso mantener la colaboración entre los Estados miembros, la Comisión y la ENISA.

Como próxima e inmediata medida, tal como se ha señalado, la Comisión insta a los Estados miembros a aplicar sin demora y de manera efectiva y objetiva las medidas acordadas dentro de la caja de herramientas y a seguir trabajando conjuntamente, con el apoyo de la Comisión y de la ENISA, para garantizar la coordinación dentro de la UE. Paralelamente y dentro de sus competencias, la Comisión tomará todas las medidas necesarias para apoyar la aplicación de la caja de herramientas por los Estados miembros y reforzar su impacto.

Apéndice: Categorías de riesgo (fuente: evaluación de riesgos coordinada en la UE).

	Categorías de riesgos
Escenarios de riesgo relacionados con medidas de seguridad insuficientes	*R1: Fallos de configuración de las redes*
	R2: Controles de acceso insuficientes
Escenarios de riesgo relacionados con la cadena de suministro de la 5G	*R3: Productos de baja calidad*
	R4: Dependencia de un único proveedor en determinadas redes o falta de diversidad a nivel nacional
Escenarios de riesgo relacionados con el modus operandi de los principales agentes de riesgo	*R5: Intromisiones por parte de Estados a través de la cadena de suministro de la 5G*
	R6: Aprovechamiento de las redes 5G por parte de la delincuencia organizada o de grupos de delincuentes organizados para atacar a usuarios finales
Escenarios de riesgo relacionados con interdependencias entre las redes 5G y otros sistemas críticos	*R7: Daños significativos a infraestructuras o servicios esenciales*
	R8: Caída general de las redes debido a la interrupción del suministro eléctrico u otros sistemas de soporte
Escenarios de riesgo relacionados con dispositivos de los usuarios finales	*R9: Utilización abusiva del internet de las cosas (IdC)*