

CONSULTA PÚBLICA PREVIA A LA ELABORACIÓN DE UNA NORMA SOBRE SEGURIDAD DE LAS REDES Y SERVICIOS 5G

Se procede a la apertura de una consulta pública para recabar aportaciones de cualquier persona o entidad en relación con la elaboración de normas sobre la seguridad de las redes y servicios de comunicaciones móviles de quinta generación o 5G. Esas normas deberán tener en cuenta la hoja de ruta y los objetivos establecidos en la Recomendación (UE) 2019/534, de 26 de marzo de 2019, de la Comisión europea, sobre la ciberseguridad de las redes 5G.

Forma y plazo de presentación

Al inicio de la aportación el remitente deberá señalar su identificación mediante su nombre o denominación social y sus datos de contacto.

Se ruega contesten a las preguntas que se formulan, en aquéllos puntos en los que se quiera realizar una aportación, haciéndolo siempre a través de **respuestas razonadas**.

Las aportaciones a realizar en el marco de esta consulta pública podrán remitirse hasta el día 13 de diciembre de 2019 a la siguiente dirección de correo electrónico: consulta5G@mineco.es

Sólo serán consideradas aquellas respuestas en las que el remitente esté identificado y su aportación se realice dentro del marco de la presente consulta. Con carácter general, las respuestas y aportaciones recibidas se considerarán susceptibles de difusión pública. Las partes de la información remitida que, a juicio del interesado, deban ser tratadas con carácter confidencial y, en consecuencia, no proceda su libre difusión, deberán ser específicamente señaladas en el propio texto, debiendo justificarse de manera motivada las razones por las que se solicita su tratamiento confidencial. No se tendrán en cuenta, a estos efectos, los mensajes genéricos de confidencialidad de la información.

El potencial transformador de la tecnología 5G ha llevado a la Unión Europea y a España a planificar el rápido despliegue de las infraestructuras de red necesarias para su aprovechamiento. En el ámbito de la Unión Europea, la Comisión propugnó un plan ambicioso para implantar la tecnología 5G en la UE desde finales de 2020 en su Comunicación “La 5G para Europa: un plan de acción” de 14 de septiembre de 2016 (COM(2016) 588 final). El Consejo y el Parlamento europeo hicieron suyo el reto y fijaron un calendario para comenzar la explotación comercial a gran escala de la tecnología 5G a partir de julio de 2020 mediante la Decisión (UE) 2017/899 del Parlamento europeo y del Consejo, de 17 de mayo de 2017, sobre el uso de la banda de frecuencia de 470-790 MHz en la Unión.

En España, se aprobó el Plan Nacional 5G 2018-2020, de 1 de diciembre de 2017, con el objetivo de cumplir con ese calendario. En ejecución del Plan Nacional, el Gobierno está subvencionando la realización de proyectos piloto con la tecnología 5G¹, y se han adjudicado ya

¹ Los 2 primeros proyectos piloto ya están en marcha (bases reguladoras aprobadas por la Orden ECE/1016/2018, de 28 de septiembre, y resolución del Director General de Red.es de 30 abril de 2019). Próximamente, se convocará una licitación para seleccionar 11 más (acuerdo del Consejo de Ministros de 4 de octubre de 2019).

las primeras concesiones demaniales para la explotación de redes 5G². Así mismo, se ha aprobado el Plan Técnico Nacional de la Televisión Digital Terrestre (Real Decreto 391/2019, de 21 de junio), para la liberación de la banda de frecuencias de 694-790 MHz que se utilizará para desplegar las redes 5G, en línea con la Decisión (UE) 2017/899 del Parlamento europeo y del Consejo, de 17 de mayo de 2017.

Las redes 5G facilitarán banda ancha móvil de muy alta velocidad y capacidad; comunicaciones ultra-fiables y de baja latencia y comunicaciones máquina a máquina. Estas características convierten al 5G en un potente catalizador de cambios tecnológicos en múltiples ámbitos más allá de la telefonía móvil. Así, permitirá ofrecer experiencias de realidad virtual; fomentar el vehículo autónomo, la telemedicina o los sistemas de seguridad y control en tiempo real de la fabricación industrial, y abrirá las puertas al Internet de las cosas y al crecimiento de los servicios de “big data”. Según datos de la Comisión europea³, la introducción de 5G en cuatro sectores (automoción, salud, transporte y servicios públicos) reportaría unos beneficios anuales crecientes que alcanzarían los 62.500 millones de euros en 2025. Algunas de las promesas del 5G son contribuir a la transformación digital de la producción (la industria 4.0), al transporte y los territorios inteligentes y al desarrollo optimizado de aplicaciones multimedia de utilidad para el ocio, la educación, la gestión medioambiental, etc. Si esas promesas se cumplen, las redes 5G tendrán, por tanto, un efecto transversal sobre el conjunto de la economía y sociedad.

Es necesario garantizar que no haya incidentes de seguridad en las redes 5G o que éstas se recuperen rápidamente de un incidente para que no repercuta negativamente en el funcionamiento de los servicios y actividades de cualquier sector económico dependientes de la tecnología 5G. Entre ellos, podrían encontrarse servicios esenciales como el suministro de agua potable, la sanidad, el transporte o la energía.

Para ello, deben reforzarse las medidas de seguridad aplicables a las comunicaciones móviles 5G, en especial, por lo que respecta a la ciberseguridad de equipos, sistemas y programas informáticos conectados entre sí o a otras redes de comunicación en las redes 5G.

En este contexto, la Comisión europea aprobó el 26 de marzo la Recomendación (UE) 2019/534 sobre ciberseguridad de las redes 5G, en la que, por una parte, aconseja a los Estados examinar los riesgos de seguridad de las redes 5G, valorar la adecuación y suficiencia de los métodos de gestión del riesgo existentes y actualizarlos en concordancia. Por otra parte, promueve un análisis conjunto de los riesgos que afecten a las redes 5G en toda la Unión y la recopilación de las mejores prácticas en cada país en un documento que debería publicarse antes del 31 de diciembre de 2019.

En aplicación de dicha Recomendación, durante el mes de octubre se han publicado un resumen de los riesgos identificados por los Estados miembros y la Agencia para la seguridad de las redes y la información (ENISA) sobre los activos de red y las amenazas que afectan a cada uno de éstos. Entre los riesgos, destacan los derivados de las singularidades de las redes 5G frente a las redes de generaciones anteriores, que, entre otras consecuencias, dan lugar al aumento del número de agentes involucrados en su operación o que pueden influir en ella

² Orden ECE/1161/2018, de 29 de octubre, por la que se resuelve la subasta convocada por Orden ETU/531/2018, de 25 de mayo, para el otorgamiento de concesiones de uso privativo de dominio público radioeléctrico en la banda 3600-3800 Mhz.

³ Estudio SMART 2014/0008: "Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe".

(operadores de redes, suministradores, subcontratistas, fabricantes de objetos conectados...). La cadena de suministro se perfila como clave para mantener la seguridad de la red, en tanto que la amenaza principal provendría de ataques orquestados por Estados, tal vez utilizando a empresas involucrados en la gestión de las redes. La Recomendación (UE) 2019/534 alude a este tipo de amenaza como un riesgo no tecnológico u “otros factores” de riesgo.

Siguiendo lo previsto en la Recomendación (UE) 2019/534, el Gobierno elaboró y remitió a ENISA su análisis de riesgos nacional y se dispone a iniciar con esta consulta previa un proceso normativo para incorporar a nuestro Ordenamiento jurídico las recomendaciones de la Comisión y las acordadas entre los Estados miembros para afrontar los riesgos de las redes 5G.

a) Problemas que se pretende solucionar con la iniciativa:

El resumen de riesgos elaborado por los Estados miembros afirma que éstos pueden afectar a todas las dimensiones de la seguridad (confidencialidad, disponibilidad e integridad) no solo de las comunicaciones móviles sino también de otros servicios que utilicen las redes y servicios 5G para su prestación. Se describen, así mismo, diversas vulnerabilidades y situaciones de riesgo en que aquellas pueden ser explotadas, así como, en su caso, los sujetos que podrían aprovecharlas.

Los operadores, fabricantes de equipos y otros agentes del sector de las tecnologías de la información están sujetos a diversas normas sobre la gestión de riesgos de seguridad. Cabe citar el artículo 44 de la Ley 9/2014, de 9 de mayo, general de telecomunicaciones, sobre integridad y seguridad de las redes y servicios de comunicaciones electrónicas; la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas; el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y los artículos en los capítulos III y V del título III de la Ley 9/2014, de 9 de mayo, relativos al secreto de las comunicaciones y protección de datos personales en las comunicaciones electrónicas.

Sin embargo, se considera que sería necesario disponer de una norma que tratara los riesgos específicos de las redes y servicios 5G, teniendo presente la variedad de actores y de situaciones de riesgo que pueden alterar la seguridad de las redes 5G. Esa norma podría ser desarrollada por reglamentos más técnicos.

Por ello, el problema que el gobierno quiere solucionar es la ausencia de un marco jurídico apropiado para proteger la seguridad de las redes y servicios 5G y de unas reglas para su supervisión por la Administración que ofrezcan seguridad jurídica a todos los intervinientes.

1. ¿Está de acuerdo con (a) los análisis de los Estados miembros y de ENISA en cuanto a los riesgos de la tecnología 5G y (b) la posibilidad de que un incidente de seguridad en las redes y servicios 5G afecte a la prestación de servicios esenciales para la sociedad distintos de las telecomunicaciones?
2. ¿Qué opinión le merecen los que la Recomendación (UE) 2019/534 llama riesgos no tecnológicos u “otros factores” de riesgo y cómo cree que deben abordarse?
3. ¿Cree que la regulación que, en su caso, se adopte debe extenderse a las redes y servicios de comunicaciones móviles de segunda, tercera o cuarta generación?
4. ¿A qué operadores de redes y prestadores de servicios de comunicaciones móviles (operadores críticos, operadores virtuales...) debería aplicarse esa norma?

5. ¿Cómo debería enfocarse la relación entre los operadores de redes 5G y los agentes que intervienen en la gestión de la red o pueden afectar a su seguridad (fabricantes de equipos o programas para redes, fabricantes de objetos conectados, subcontratistas...)? En particular, ¿deberían ser responsables ante la Administración o ante el operador de la red o del servicio 5G?
6. ¿Cómo cree que debe regularse la seguridad de las redes y servicios 5G sin aumentar innecesariamente la carga administrativa de los sujetos obligados?

b) Necesidad y oportunidad de la aprobación de una norma:

La elaboración de una norma específica sobre la seguridad de las redes 5G se justifica por la complejidad tecnológica y el mayor impacto potencial sobre otros sectores económicos que el que puede tener una mera interrupción del servicio de comunicaciones móviles o una interceptación ilegal de una comunicación privada.

A este respecto, la Comisión europea ha recomendado a los Estados miembros que actualicen los requisitos de seguridad aplicables a las redes 5G y ha impulsado varias acciones para identificar entre todos los Estados miembros los riesgos y las medidas de gestión más adecuadas. La Recomendación (UE) 2019/534 señala que este análisis conjunto servirá para informar ulteriores propuestas de la Comisión para elevar el nivel de seguridad en las redes 5G. A nuestro juicio, deberían incorporarse al Ordenamiento jurídico español las buenas prácticas que resulten del análisis conjunto de los EE.MM. sin esperar a que la Comisión presente nuevas medidas ya que no se sabe cuánto tardará en hacerlo ni si consistirán en una propuesta normativa u otro tipo de actuación.

Ahora es el momento idóneo para elaborar una norma nacional ya que la tecnología 5G comenzará a comercializarse a gran escala a partir del segundo semestre de 2020. Las empresas e instituciones públicas no se arriesgarán a invertir dinero en nuevas aplicaciones para 5G si la seguridad del servicio es endeble y los riesgos no compensan sus beneficios.

1. ¿Está de acuerdo con la necesidad de una norma específica para la seguridad de la tecnología 5G y los motivos esgrimidos para dictarla?
2. ¿Cree que sería mejor esperar a que la Comisión europea propusiera, en su caso, medidas más concretas como resultado de la aplicación de la Recomendación (EU) 2019/534?

c) Objetivos de la norma:

El objetivo que se persigue es afianzar la confianza de los usuarios de la fiabilidad de los servicios 5G, la cual, en parte, depende de la aplicación de una política de seguridad adecuada y convenientemente actualizada. De esta manera, será más fácil conseguir la rápida adopción de 5G por las empresas y entidades para el desarrollo de aplicaciones en movilidad para su propio ámbito de actividad. El pleno aprovechamiento de las características 5G puede hacer más competitiva a España en la economía digital y ofrecer a los ciudadanos servicios de gran valor añadido para su salud y su seguridad.

Algunos Estados miembros, como Francia, Alemania o Italia, han aprobado o están tramitando normas para implementar la Recomendación (UE) 2019/534, que incluyen medidas como la certificación de equipos, su autorización administrativa o el otorgamiento de un poder de veto al gobierno sobre la adquisición de equipos o la contratación de servicios que tengan como destino la explotación de redes 5G.

1. ¿Qué papel desempeña, a su juicio, la seguridad en el buen funcionamiento de las redes 5G para promover el desarrollo de aplicaciones y servicios IoT, “big data”, realidad aumentada o emisión de contenidos en ultra alta definición, etc. que no serían posibles o lo serían en mucha menor medida sin esta tecnología?
2. ¿Hay otros factores (compartición de emplazamientos, disponibilidad de espectro radioeléctrico o de equipos...) pueden influir en el desarrollo de la tecnología 5G y en su aplicación a distintas actividades económicas o sociales, que requieran o puedan beneficiarse de una regulación específica?
3. ¿Cree necesario establecer medidas de veto, autorización previa o certificación de componentes o sistemas para alcanzar el objetivo de seguridad expresado? En caso afirmativo, ¿la impondría para todos los componentes o sistemas o solo para los suministrados por empresas de terceros países?

d) Las posibles soluciones alternativas regulatorias y no regulatorias:

En este documento, se ha razonado la necesidad de una norma heterónoma para alcanzar un nivel de seguridad alto para la operación de las redes y la prestación de servicios basados en la tecnología 5G que esté alineado con los principios acordados en el ámbito comunitario y sea fiscalizable por la Administración.

No obstante, cabría imaginar métodos alternativos, como la corregulación con el sector, con principios establecidos por ley o reglamento y normas de desarrollo pactadas con la industria. Otro enfoque es la autorregulación, apoyado en códigos, estándares y buenas prácticas internacionales, y supervisado por el propio sector.

1. ¿Cuál cree que sería el enfoque adecuado (regulación, corregulación o autorregulación) para abordar la ciberseguridad en las redes y servicios 5G?
2. Si opina que las mejores alternativas son la corregulación o la autorregulación, ¿cómo propone resolver las discrepancias que puede haber entre operadores, usuarios y fabricantes a la hora de establecer obligaciones salvaguardando el interés general en la seguridad de las redes y servicios 5G?
3. ¿De qué modo y con qué frecuencia debería actualizarse la norma (o código de conducta) que se elaborara para que siga siendo eficaz en la mejora de la ciberseguridad de las redes y servicios 5G?
4. A la vista de la Recomendación (UE) 2019/534 y de las síntesis de riesgos y medidas de gestión acordadas por los Estados miembros, ¿piensa que alguna de las medidas susceptibles de adopción o de las facultades de control por la Administración deberían figurar en una norma con rango de ley?