ACUERDO POR EL QUE SE EMITE INFORME SOBRE EL ANTEPROYECTO DE LEY SOBRE LOS REQUISITOS PARA GARANTIZAR LA SEGURIDAD DE LAS REDES Y SERVICIOS DE COMUNICACIONES ELECTRÓNICAS DE QUINTA GENERACIÓN

IPN/CNMC/029/21 LEY CIBERSEGURIDAD 5G

CONSEJO. PLENO

Presidenta
Dª Cani Fernández Vicién

Vicepresidente
D. Ángel Torres Torres

Consejeros
Dª. María Ortiz Aguilar
D. Mariano Bacigalupo Saggese
Dª. María Pilar Canedo Arrillaga
D. Bernardo Lorenzo Almendros
D. Xabier Ormaetxea Garai
Dª. Pilar Sánchez Núñez
D. Carlos Aguilar Paredes
D. Josep María Salas Prat

Secretario
D. Miguel Bordiu García-Ovies

En Madrid, a 24 de noviembre de 2021

Vista la solicitud remitida por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales del Ministerio de Asuntos Económicos y Transformación Digital, en el ejercicio de las competencias que le atribuye el artículo 5.2 de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, el Pleno acuerda emitir el siguiente Informe relativo al Anteproyecto de Ley sobre los requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

I OBJETO DEL INFORME Y HABILITACIÓN COMPETENCIAL

I.1 Objeto del informe

Con fecha 29 de julio de 2021 tuvo entrada, en el Registro de la Comisión Nacional de los Mercados y la Competencia (en adelante, CNMC), escrito del Director General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual solicitando informe respecto al borrador de Anteproyecto de Ley sobre los requisitos para garantizar la seguridad de las

redes y servicios de comunicaciones electrónicas de quinta generación (en adelante, APL). El citado escrito venía acompañado de la pertinente Memoria de Análisis de Impacto Normativo (MAIN).

El presente informe tiene por objeto analizar la propuesta remitida y manifestar el parecer de la CNMC sobre la misma.

I.2 Habilitación competencial

El artículo 5.2.a) de la Ley 3/2013, de 4 de junio, de creación de la CNMC establece que este Organismo participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en los sectores sometidos a su supervisión.

En este mismo sentido, el artículo 70.2.l) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en lo sucesivo, LGTel), establece que, entre otras funciones, la CNMC será consultada por el Gobierno y el Ministerio de Industria, Energía y Turismo[1] en materia de comunicaciones electrónicas, particularmente en aquellas materias que puedan afectar al desarrollo libre y competitivo del mercado. Asimismo, se precisa que, en el ejercicio de esta función, la CNMC participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en materia de comunicaciones electrónicas.

El artículo 20 de la Ley 3/2013, de 4 de junio, de creación de la CNMC atribuye al Consejo de la CNMC la adopción de estos informes.

En consecuencia, en aplicación de los anteriores preceptos, el Consejo de la CNMC es competente para elaborar el presente informe sobre el Anteproyecto de Ley sobre los requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (5G), por afectar a sus competencias en materia de comunicaciones electrónicas.

II ANTECEDENTES

II.1 Contexto relativo a la tecnología 5G

Las características técnicas inherentes a la tecnología 5G -transmisión de grandes volúmenes de datos a alta velocidad (eMBB[2]), baja latencia y alta fiabilidad (URLLC[3]), y capacidad para conectar un número masivo de

1 Actualmente Ministerio de Asuntos Económicos y Transformación Digital, de conformidad con el Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los departamentos ministeriales.
2 Enhanced Mobile BroadBand
3 Ultra Reliable Low Latency Communication

dispositivos a la red (mMTC[4])-, abren un nuevo horizonte de posibilidades que sobrepasan el ámbito de la conectividad móvil personal de las generaciones tecnológicas anteriores (2G, 3G, 4G).

La arquitectura 5G incorpora además tecnologías propias del ámbito informático de tratamiento, almacenamiento y gestión de la información, en un proceso de convergencia cada vez más generalizado de las redes de telecomunicaciones y los sistemas informáticos. De este modo, las funciones de virtualización, computación en el borde y segmentación de la red en distintas capas, presentes en las redes 5G, en combinación con el uso de tecnologías complementarias de Big Data, Internet de las cosas, Inteligencia Artificial, robótica, realidad virtual o ultra alta definición habilitarán la transformación digital de las empresas en múltiples sectores económicos y sociales -tales como industria, logística, energía, salud, emergencias, transporte o automoción-.

El desarrollo de la tecnología 5G constituye una prioridad para la estrategia industrial y la competitividad europeas, puesta de manifiesto en el ámbito de las políticas sectoriales de la Unión Europea e, igualmente, del Gobierno de España.

Así, la Comisión Europea adoptó, en abril de 2016, el Plan de Acción 5G[5] que establece una hoja de ruta común para incentivar el desarrollo de pilotos y alcanzar un despliegue temprano de redes con tecnología 5G en todos los países miembros de la Unión Europea. Este Plan estableció hitos de lanzamiento de servicios comerciales 5G en el período 2020-2025[6], que han sido ampliados en la comunicación de la Brújula Digital -Digital Compass[7]- de forma que para 2030 todas las áreas pobladas de Europa deberían disponer de cobertura 5G.

A nivel nacional, la estrategia "España Digital 2025"[8] considera las infraestructuras de telecomunicaciones clave para la transformación digital. Así, entre los planes sectoriales contemplados en dicha agenda estratégica se incluye la "Estrategia de Impulso de la tecnología 5G"[9] para promover el despliegue acelerado de redes y servicios 5G, que ha renovado el denominado "Plan Nacional 5G (2018-2020)"[10] sobre el que se basa el desarrollo de 5G en España, y que ha propiciado que nuestro país lidere el número de pilotos 5G de

[4] Massive Machine Type Communications
[5] https://ec.europa.eu/transparency/regdoc/rep/1/2016/ES/1-2016-588-ES-F1-1.PDF
[6] Primeros lanzamientos comerciales de servicios 5G en 2020 y cobertura 5G ininterrumpida en todas las áreas urbanas y corredores de transporte en 2025.
[7] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983
[8] https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx
[9] https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2020/201201_np_impulso5G.pdf
[10] https://avancedigital.mineco.gob.es/5G/Documents/plan_nacional_5g.pdf

la Unión Europea[11] y sea el segundo país europeo en número de ciudades con despliegue comercial 5G[12].

En este contexto han tomado especial relevancia los requisitos de seguridad de las redes 5G.

II.2 Marco normativo en seguridad aplicable al despliegue de redes 5G

Las obligaciones en materia de seguridad están explícitamente incluidas en el marco legislativo nacional, de acuerdo con las siguientes normas:

- La LGTel[13]: el artículo 44 establece que los operadores de redes y servicios de comunicaciones electrónicas deben gestionar adecuadamente los riesgos de seguridad e integridad de sus redes y servicios, a fin de asegurar la continuidad en la prestación de los servicios que utilizan dichas redes, y habilita a la autoridad competente para dictar instrucciones vinculantes para los operadores relativas a la seguridad e integridad 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 las infraestructuras críticas[14].

- El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, que transpuso la Directiva de seguridad de las redes y sistemas de información (Directiva SRI, también llamada por sus siglas en inglés Directiva NIS)[15], y el Real Decreto 43/2021, de 26 de enero, que lo desarrolla. Esta normativa aplica a los operadores de servicios esenciales en diferentes sectores estratégicos y los proveedores de servicios digitales.

Sectores económicos vitales para la sociedad, tales como energía, salud, banca o transporte, por mencionar solo algunos, dependen cada vez más de las

[11] Según el informe trimestral de junio de 2021 publicado por el Observatorio 5G de la UE.
[12] Según la información publicada en septiembre de 2020 por el Observatorio 5G de la UE.
[13] La LGTel va a ser objeto de revisión. El Anteproyecto de Ley General de Telecomunicaciones, sobre el cual la CNMC emitió informe el 4 de diciembre de 2020 (IPN/CNMC/034/20), propone transponer las disposiciones en la materia establecidas en los artículos 40 y 41 de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (Código Europeo). El artículo 63 de dicho Anteproyecto mantiene una redacción equivalente a la del actual artículo 44.
[14] En cumplimiento de lo estipulado en la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.
[15] 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.

tecnologías digitales para el ejercicio de sus actividades. Paralelamente, el número de ataques cibernéticos está creciendo en toda Europa. Por ello, reforzar la resiliencia de las redes de comunicaciones y de los sistemas de información se ha convertido en una prioridad de la política regulatoria europea.

Con este objetivo, el Reglamento sobre la Ciberseguridad de la UE[16] introdujo el marco de certificación de la ciberseguridad para toda la UE y reforzó el papel de la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Además, dada la especial relevancia que ha tomado la seguridad de las redes 5G, se aprobó la Recomendación de la Comisión (UE) 2019/534, de 26 de marzo de 2019, de Ciberseguridad de las redes 5G (Recomendación de ciberseguridad 5G), que identificó una serie de acciones coordinadas de los Estados miembros para analizar los riesgos de seguridad que podrían afectar a las redes 5G y aplicar así un conjunto de medidas para mitigar dichos riesgos. Fruto del trabajo conjunto de identificación de vulnerabilidades por parte de los países europeos (análisis coordinado de riesgos)[17], el Grupo de Cooperación para la Seguridad de las Redes y Sistemas de Información (Grupo de Cooperación SRI o NIS Cooperation Group)[18] publicó en enero de 2020 la caja de herramientas de la UE para medidas de reducción del riesgo en las redes 5G[19] (caja de herramientas).

Las principales vulnerabilidades de las redes 5G, puestas de manifiesto por los Estados miembros en sus respectivos análisis de riesgos, se basan en: (i) la mayor complejidad de la tecnología 5G, con una arquitectura menos centralizada, más abierta y más dependiente del software, y una mayor presencia de funciones de virtualización y computación en el borde de la red, que aumenta la superficie y el número de puntos de posible ataque cibernético, (ii) la mayor relevancia del perfil de riesgo de los proveedores utilizados en determinados equipos o funciones de las redes 5G, en particular aquellos suministradores sujetos a injerencias externas de países terceros no miembros de la UE, por la mayor exposición de la tecnología 5G a ataques de agentes externos, y (iii) la dependencia de un único proveedor, al aumentar la exposición y consecuencias ante un fallo o ataque de seguridad, especialmente si se trata de un proveedor de alto riesgo.

La caja de herramientas de la UE enumera y describe una serie de medidas estratégicas, técnicas y de apoyo, destinadas a mitigar los riesgos de seguridad observados en estos análisis.

[16] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 («Reglamento sobre la Ciberseguridad»)

[17] Según el informe de 9 de octubre de 2019 "*EU coordinated risk assessment of the cybersecurity of 5G networks - Report*".

[18] Compuesto por representantes de los Estados miembros, la Comisión Europea y la Agencia de la UE para la Ciberseguridad (ENISA).

[19] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

La Comunicación[20] de la CE de 29 de enero de 2020 insta a los Estados miembros a aplicar sin demora y de manera efectiva y objetiva las medidas acordadas dentro de esta 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.

El BEREC lleva a cabo un seguimiento de las diferentes medidas adoptadas en este ámbito[21].

El presente APL trasladaría a la normativa nacional las medidas fundamentales contenidas en dicha caja de herramientas de la UE, introduciendo medidas de seguridad adicionales a las contempladas en el marco normativo nacional.

Por último, conviene señalar que, en diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron una nueva Estrategia de Ciberseguridad para la UE, que persigue reforzar la resiliencia de Europa frente a las amenazas cibernéticas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables. Esta estrategia -actualmente en fase de debate en la UE- incorpora una serie de medidas, entre las que se encuentran la propuesta de revisión de la Directiva SRI y una nueva Directiva sobre resiliencia de las entidades críticas, y se alienta a los Estados miembros a completar la implementación de la caja de herramientas[22]. En sus conclusiones sobre la estrategia de ciberseguridad de la UE, el 22 de marzo de 2021, el Consejo de la UE ha expresado su voluntad de aplicar con prontitud la ejecución de las medidas de la caja de herramientas para las redes 5G, y de seguir esforzándose por garantizar la seguridad de las redes 5G y el desarrollo de las futuras generaciones de redes.

III DESCRIPCIÓN DEL ANTEPROYECTO DE LEY

Este APL tiene como objeto el establecimiento de requisitos de seguridad adicionales a los establecidos en el ordenamiento jurídico nacional, para el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas basados en la tecnología 5G.

Con este texto se trasladarían al marco legal español las medidas consensuadas entre los Estados miembros para mitigar los riesgos de seguridad en las redes

[20] COM(2020) 50 final. Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE.
[21] Informe BEREC BoR (20) 228 "*Report of BEREC recent activities concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)*".
[22] Para el segundo trimestre de 2021.

5G, desarrolladas en la caja de herramientas de la UE, de conformidad con la Recomendación de ciberseguridad 5G. Así se indica en el preámbulo, que se incluyen las recomendaciones fundamentales que la Comunicación de 29 de enero de 2020 de la Comisión Europea realizaba a los Estados miembros sobre la utilización de la caja de herramientas.

El APL consta de un preámbulo, 22 artículos divididos en cuatro capítulos, dos disposiciones adicionales, una disposición transitoria y tres disposiciones finales.

- Capítulo I: Disposiciones generales (artículos 1 a 5)

Este capítulo comprende el objeto de la nueva ley, sus fines, las definiciones aplicables y el ámbito de aplicación. Según estas disposiciones, los requisitos de seguridad establecidos en la norma podrán ser aplicables no solo a los operadores de redes y servicios de comunicaciones electrónicas basados en la tecnología 5G, sino también a otros agentes de la cadena de valor de las redes y servicios 5G, en concreto, los suministradores de equipos y proveedores de servicios necesarios para la explotación de redes 5G, los fabricantes de equipos terminales y dispositivos conectados a la red 5G y los usuarios corporativos que tengan derecho de uso del dominio público radioeléctrico.

- Capítulo II: Análisis y gestión de los riesgos (artículos 6 a 9)

En este capítulo se regulan los análisis de riesgos que deben efectuar los operadores, al menos, cada 2 años, y que deben focalizarse en los componentes y funciones esenciales de las redes 5G -incluye todos los elementos mencionados en la caja de herramientas- y tener en cuenta una lista de factores que incluyen, entre otros, la dependencia de determinados suministradores en elementos esenciales de la red, las estrategias de permiso de acceso a equipos o los agentes externos con capacidad para atacar la red. Incluye la obligación de que los operadores examinen las prácticas de seguridad de sus suministradores.

También se regula el deber de los operadores de gestionar sus riesgos de seguridad y los de sus suministradores, a los que deberán exigir el cumplimiento de estándares de seguridad y control de su cadena de suministro. Los operadores deben aplicar medidas técnicas y organizativas para mitigar los riesgos y adoptar una estrategia de diversificación de suministradores para limitar la dependencia de un solo suministrador o de varios que tengan una calificación de riesgo alto en elementos esenciales de la red.

Los análisis de riesgo, el informe sobre las prácticas de seguridad de los suministradores, las medidas para mitigar los riesgos y la estrategia de diversificación de suministradores deben ser remitidos al Ministerio de Asuntos Económicos y Transformación Digital (en adelante, Ministerio).

- Capítulo III: Esquema de seguridad de redes y servicios 5G (artículos 10 a 18)

Los análisis de riesgos y medidas remitidos por los operadores constituirán la base del Esquema de seguridad de las redes y servicios 5G (en adelante, Esquema de seguridad), que será aprobado por el Gobierno mediante real decreto, a propuesta del Ministerio, informado por el Consejo de Seguridad Nacional y revisado al menos cada 6 años.

El Esquema de seguridad abordará el tratamiento integral de la seguridad de las redes y servicios 5G a nivel nacional. Entre otros aspectos, dicho Esquema de seguridad contendrá una priorización de los riesgos y determinará las obligaciones de los operadores, suministradores, fabricantes de equipos y dispositivos conectados y usuarios corporativos. También podrá fijar objetivos de diversificación de suministradores en la cadena de suministro de cada operador, así como globalmente a nivel nacional.

Destaca el artículo 11, que determina los criterios que el Gobierno debe tener en cuenta para examinar el perfil de riesgo de los suministradores y calificarlos -a propuesta del Ministerio y previo informe del Consejo de Seguridad Nacional- como bajo, medio o alto. Los criterios se basan en (i) las garantías técnicas de funcionamiento y protección frente a ataques (cumplimiento de normas, certificaciones o superación de auditorías) y (ii) la exposición a injerencias externas. Para evaluar este último criterio no técnico se incluye un listado de factores -no cerrado-, entre los que se encuentra la vinculación de los suministradores y su cadena de suministro con los gobiernos de terceros países, o las características del régimen político y de la política de defensa cibernética de dichos Estados.

Se incluyen en el propio articulado del APL (artículo 14) dos listados no cerrados de obligaciones que el Esquema de seguridad puede llegar a imponer a operadores y suministradores. Entre las obligaciones de los operadores destaca la posibilidad de condicionar, restringir o prohibir el uso de equipos, programas o servicios de suministradores de una determinada calificación de riesgo, incluyendo el establecimiento de cuotas o porcentajes de uso, así como plazos para su eliminación de las redes. Asimismo, a operadores y suministradores se les podrá imponer el cumplimiento de normas o especificaciones técnicas, certificaciones o ser sometidos a auditoría por una entidad u organismo acreditado.

Se incluye la posibilidad de requerir la certificación en elementos de las redes 5G y de supeditar la comercialización o uso de equipos terminales y dispositivos conectados en las redes 5G al cumplimiento de los requisitos esenciales en ciberseguridad, conforme a la normativa comunitaria.

Todas las obligaciones del Esquema de seguridad podrán aplicarse de manera diferenciada a los distintos sujetos obligados y en distintas fases en supuestos debidamente justificados.

Se contempla la inclusión en el Esquema de Seguridad de una serie de medidas de impulso a la investigación y desarrollo en materia de seguridad, interoperabilidad y gestión de las redes 5G, así como de participación en estándares internacionales.

Por último, en la contratación pública de comunicaciones o servicios que hagan uso de la tecnología 5G, se incluye la medida de poder exigir una certificación europea conforme al Reglamento sobre la ciberseguridad de la UE, e incluso imponer la exclusión de los suministradores con una determinada calificación de riesgo.

- Capítulo IV: Potestades administrativas de control y sanción (artículos 19 a 22)

Este capítulo regula la inspección y el control de la aplicación de la ley y de la Estrategia de seguridad. El Ministerio de Asuntos Económicos y Transformación Digital será competente para aplicar el Esquema de seguridad a los operadores, suministradores y fabricantes de equipos terminales y dispositivos conectados, actuando bajo la coordinación del Consejo de Seguridad Nacional en todo lo que afecte a los suministradores de alto riesgo. Las obligaciones de seguridad del Esquema de seguridad referidas a los usuarios corporativos serán aplicadas por los demás departamentos ministeriales.

Se incluyen las potestades de inspección y el régimen sancionador, así como otras potestades administrativas que los órganos competentes podrán ejercer en la aplicación de esta ley, entre las que se encuentran la de dictar órdenes ministeriales, instrucciones técnicas y guías orientativas para detallar el contenido del Esquema de seguridad 5G.

- Disposiciones adicionales, transitoria y finales

Entre estas disposiciones destaca la obligación de los operadores de remitir sus análisis de riesgos, medidas técnicas y organizativas para mitigarlos e informes sobre sus suministradores en el plazo de 4 meses desde la aprobación de la ley. Con respecto a las obligaciones relacionadas con el perfil de riesgo de los suministradores del artículo 14 de la ley, y hasta la aprobación del Esquema de seguridad 5G, se habilita al Ministerio a establecerlas, previo informe de Seguridad Nacional.

IV VALORACION DEL ANTEPROYECTO

Esta Comisión valora positivamente el APL, ya que refuerza la seguridad de las redes basadas en tecnología 5G y, por tanto, de los nuevos servicios que serán prestados por dichas redes, lo que afianzará la transformación digital en múltiples sectores económicos y servicios esenciales para la sociedad.

Las amenazas cibernéticas pueden comprometer la disponibilidad, integridad y confidencialidad de las redes de comunicaciones y del tráfico e información vehiculado por dichas infraestructuras. Según el análisis coordinado de riesgos en las redes 5G realizado por los Estados miembros, la CE y ENISA, publicado en octubre de 2019[17], estas amenazas tienen mayor relevancia en el despliegue de las redes 5G que en las redes actuales, debido a los sectores económicos a los que la tecnología 5G dará servicio, lo que agravaría el impacto de dichos ataques.

Es significativo el aumento de la complejidad tecnológica de las redes 5G, intrínsecamente dependientes de software cada vez más abierto, con funcionalidades tales como la virtualización de funciones de red, la computación en el borde o la segmentación de la red y con multitud de usos, aplicaciones y dispositivos conectados. Por ello, las redes de los operadores serán más vulnerables a fallos de funcionamiento y ataques cibernéticos en caso de implantar medidas de seguridad insuficientes, al requerirse (i) la integración de un mayor número de proveedores terceros (de infraestructuras y servicios del ámbito TIC), (ii) personal especializado en nuevas áreas y (iii) unas políticas adecuadas de permisos y control de acceso a recursos de red y mantenimiento del software.

En el mismo análisis europeo se destaca que, entre los agentes que originan los ataques cibernéticos, las amenazas que provienen o son sustentadas por gobiernos de terceros países son consideradas las más peligrosas, por las motivaciones políticas y la capacidad de estas entidades, que pueden llegar a comprometer la seguridad en las redes 5G. Así, el análisis del perfil de riesgo de los suministradores de hardware, software o servicios de las redes 5G cobra especial relevancia, para asegurar tanto su fiabilidad técnica como su independencia respecto a injerencias externas.

En consecuencia, además de las vulnerabilidades técnicas ligadas a una política de medidas de seguridad, operación y organización potencialmente deficiente por parte de los operadores en las redes 5G, es importante considerar las vulnerabilidades asociadas a los suministradores de equipos y su cadena de suministro, así como el riesgo de dependencia de un único suministrador en partes o funciones esenciales de la red.

En base a este análisis, el APL incluye una serie de obligaciones, principalmente destinadas a los operadores y los suministradores, además de otros agentes,

que han sido elaboradas en base a las medidas propuestas en la caja de herramientas de la UE para mitigar los riesgos en seguridad de las redes 5G.

Respetando el objetivo primordial de refuerzo de la seguridad de las redes 5G, se considera adecuado incorporar medidas normativas que especifiquen tanto los criterios a valorar en la gestión de riesgos de seguridad de las redes 5G, como las medidas a adoptar para reducir dichos riesgos.

Las medidas de seguridad de la caja de herramientas, incluidas en el APL, han sido objeto de análisis y valoración por parte de las autoridades competentes nacionales en la materia, junto a la Comisión Europea, ENISA y el resto de Estados miembros. Por consiguiente, el presente informe no se centra en valorar dichas medidas, sino en analizar su aplicación en el sector de las comunicaciones electrónicas y su impacto potencial en la competencia, teniendo en cuenta los principios y objetivos del artículo 3 de la LGTel, entre los que se encuentran el fomento de la competencia, la promoción del despliegue de redes y la prestación de servicios de comunicaciones electrónicas.

Partiendo de este criterio, y sin perjuicio de la valoración general positiva del APL, se exponen a continuación una serie de comentarios generales y observaciones particulares.

IV.1 Comentarios generales

Estructura de la norma

La propuesta actual de la norma descansa en el denominado Esquema de Seguridad para las redes y servicios 5G, junto al desarrollo de otros instrumentos normativos como resoluciones, instrucciones o guías orientativas. Este Esquema y el resto de los instrumentos de desarrollo concretarán la forma de realizar la calificación del nivel de riesgo de los suministradores, el tipo de obligaciones relacionadas con la seguridad a imponer, los criterios y condiciones en los que se impondrán dichas obligaciones, y la afectación particular a cada uno de los sujetos obligados.

Dado tanto la necesidad de que se defina y apruebe el Esquema de Seguridad para que pueda continuarse el desarrollo de las redes 5G con la máxima seguridad, como la también urgente necesidad de continuar el despliegue de estas redes, es importante, tanto por las razones de seguridad que justifican su existencia, como de máximo respeto a la actividad empresarial de los agentes afectados, que su aprobación se lleve a cabo con la máxima celeridad posible.

Su rápida aprobación evitaría una suerte de incertidumbre regulatoria que se podría generar si determinadas obligaciones relacionadas con el perfil de riesgo de los suministradores, que formarán parte del Esquema de seguridad, pueden

ser aplicadas antes de la aprobación del mismo con una especificación distinta a la que resulte finalmente en el Esquema.

Afectación a la competencia

Las redes de comunicaciones móviles se caracterizan por un alto grado de innovación, que requiere de fuertes inversiones, por lo que con cada generación móvil se ha tendido a una mayor concentración de la oferta de suministradores de equipos. Como indica la Memoria de Análisis de Impacto Normativo (MAIN) que acompaña al APL, los principales suministradores de las redes 5G en la actualidad son las empresas europeas Ericsson y Nokia y las chinas Huawei y ZTE.

La norma contempla una serie de medidas regulatorias que, por un lado pueden llegar a prohibir o limitar la actividad en el mercado de suministradores considerados de alto riesgo, y por otro pueden obligar a diversificar el número de suministradores de una red. En ambos casos éstas medidas pueden alterar las condiciones de competencia en el mercado de suministradores, y por tanto, su aplicación regulatoria por razones de seguridad debería ser rigurosamente analizada y valorada con respecto a su afectación a la competencia, de forma que este factor pase a ser uno de los criterios a sopesar en el análisis de medidas de mitigación de riesgos, y en especial respecto a las restricciones vinculadas al perfil de riesgo de los suministradores, por su potencial capacidad de excluir a algunos agentes económicos del mercado.

Este posible efecto de reducción de suministradores en el mercado de redes 5G puede verse incrementado al incluir como uno de los criterios de valoración del perfil de riesgo el nivel de exposición a injerencias de terceros países, entrando a valorar aspectos geopolíticos que puedan impactar en la seguridad. Esta posible pérdida de competencia en el mercado, derivada de un menor número de agentes podría reducir los incentivos a la innovación, y aumentar el coste de prestación de servicios y la reducción de la calidad, afectando negativamente a los operadores y usuarios de servicios 5G en los mercados descendentes.

En general, se aconseja incluir criterios de valoración de las medidas de seguridad con respecto a su afectación a la competencia, en especial de aquellas medidas relacionadas con el perfil de riesgo de los suministradores.

Una vez expuestos estos comentarios generales al APL, se procede a realizar observaciones particulares a su articulado.

IV.2 Definiciones y ámbito de aplicación de la Ley (artículos 3, 4 y 5)

Definiciones de 5G y de seguridad

En primer lugar, se recomendaría que, además de la referencia a la Recomendación UIT-R M.2083, de la Unión Internacional de

Telecomunicaciones para definir la tecnología 5G en la definición 3.a), se incluyera la consideración de la organización 3GPP[23], que define las distintas generaciones de tecnología móvil y sus especificaciones.

Se propone añadir al final de la definición a) lo siguiente:

«a) […], de acuerdo con la estandarización de la organización 3GPP.

Dado que el objeto del APL es el de establecer requisitos de seguridad en el despliegue y explotación de las redes y servicios 5G, adecuados a los riesgos existentes, convendría incluir en el artículo de definiciones los términos "seguridad", y "riesgo de seguridad". Para ello, se propone añadir en el artículo 3 la siguiente redacción de tales términos basada en las definiciones del Código[24] y del RDL 12/2018:

«g) "seguridad": la capacidad de las redes y servicios 5G de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de dichas redes y servicios, de los datos almacenados, procesados o transmitidos, o de los servicios accesibles a través de ellos.

h) "riesgo": toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y servicios 5G.

Respecto al ámbito de aplicación de los requisitos de seguridad

Como se señala en su artículo 4, el APL aplica a prácticamente todos los actores de la cadena de valor en la prestación de servicios 5G: operadores, suministradores, fabricantes de dispositivos conectados y usuarios corporativos. Sin embargo, los requisitos específicos en materia de seguridad que aplican a cada sujeto obligado se encuentran distribuidos a lo largo del texto del APL, y serán objeto de mayor concreción en el Esquema de seguridad que deberá ser desarrollado con posterioridad a la aprobación del APL.

La mayoría de obligaciones de seguridad afectan a los operadores, que tienen el deber de analizar y gestionar los riesgos de seguridad asociados a las redes 5G, incluyendo el análisis de las prácticas de seguridad de sus suministradores y están obligados a adoptar medidas para mitigar los riesgos analizados, con el alcance que indique el Esquema de seguridad.

Sobre los suministradores recaen igualmente una serie de obligaciones específicas que serán determinadas en el Esquema de seguridad. Sin embargo,

[23] El 3GPP *(3rd Generation Partnership Project)* es una agrupación de siete organismos de normalización, conocidos como miembros organizativos y es el marco en que se desarrollan los estándares de comunicaciones móviles desde 1998. Los operadores y suministradores participan a través de uno de los miembros organizativos.

[24] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

otra serie de medidas afectan a los suministradores de forma indirecta, ya que serán gestionadas por los operadores. Así, los operadores deben analizar las prácticas de seguridad de sus suministradores (artículo 7), gestionar los riesgos derivados de la actuación de sus suministradores, y exigirles el cumplimiento de estándares de seguridad y el control de su cadena de suministro (artículo 8).

Sin embargo, a juicio de esta Comisión para llevarlas a cabo debería indicarse en el ámbito de aplicación que los suministradores deberán colaborar con los operadores, proporcionando la información de seguridad requerida en el APL y adoptando las medidas de seguridad determinadas por los operadores en cumplimiento de la ley que se apruebe.

Los fabricantes y comercializadores de equipos terminales y dispositivos conectados, así como los usuarios corporativos con derecho de uso del dominio público radioeléctrico, también se encuentran afectados por la norma, pero no se explicita claramente el tipo de medidas u obligaciones que pueden afectarles, más allá del deber de colaboración en el Esquema de seguridad (artículo 10.3) y del cumplimiento de requisitos esenciales -no especificados- y de certificación aplicables a los dispositivos (artículo 15). En cualquier caso, al verse afectados por las disposiciones del Esquema de seguridad, debería aclararse esta circunstancia en el ámbito de aplicación.

De acuerdo con el objetivo de incorporar aclaraciones en la estructura del APL para reflejar adecuadamente los requisitos de seguridad que aplican a cada sujeto y su condicionamiento a lo que se determine en el Esquema de seguridad, se propone incorporar un nuevo artículo en el Capítulo I, que sea posterior al artículo 4, e incorpore las aclaraciones anteriores. Una posible redacción podría ser la siguiente:

> *«**Artículo**. Requisitos de seguridad*
> *Los operadores estarán obligados a analizar y gestionar los riesgos de seguridad que afecten a la seguridad de las redes y servicios 5G, incluyendo los asociados a las prácticas de seguridad de sus suministradores.*
>
> *Los suministradores estarán obligados a colaborar con los operadores en el análisis y gestión de los riesgos de seguridad de las redes y servicios 5G, proporcionando información sobre sus prácticas de seguridad.*
>
> *Los operadores, suministradores y el resto de sujetos identificados en el artículo 4 de ámbito de aplicación de esta Ley, deberán adoptar las medidas de seguridad adecuadas y proporcionadas a los riesgos contemplados que les afecten, en cumplimiento de lo dispuesto en esta Ley, así como lo que se determine en el Esquema de seguridad de las redes y servicios 5G y su normativa de desarrollo.»*

Respecto a la calificación de operador

Los operadores de redes y servicios de comunicaciones electrónicas basados en la tecnología 5G están definidos en el artículo 3.c) como “*personas físicas o*

jurídicas que explotan redes 5G y los prestadores de servicios de comunicaciones electrónicas basados, total o parcialmente en dichas redes 5G".

Entrarían dentro de esta calificación tanto los operadores móviles con espectro radioeléctrico, como los operadores móviles virtuales (OMV) -completos y prestadores de servicio[25]-, así como cualquier otro prestador de servicios de comunicaciones electrónicas basados, total o parcialmente, en una red 5G.

Además, dado que la tecnología 5G permite la aparición de nuevos modelos de negocio en el mercado, agentes que actualmente no entran dentro de esta categoría -como los operadores de infraestructuras-, podrían evolucionar en la cadena de valor y explotar redes 5G para redes privadas en determinadas zonas.

Dado que son los equipos y funcionalidades (hardware y software) de la red 5G los que deben ser objeto de análisis de riesgos y pueden ser vulnerables a amenazas cibernéticas, el análisis coordinado de riesgos de las redes 5G ya identificaba a los operadores de red móvil como los operadores afectados, asimilando también en esta categoría de operador a los operadores de red móvil virtual y a los operadores de infraestructuras críticas que operen redes 5G para auto-prestación o por cuenta de terceros[26], debido a que serían estos agentes los que se encontrarían explotando redes 5G.

Partiendo de que los usuarios corporativos ya están incluidos en el ámbito de aplicación del APL, la calificación de operador aplicaría entonces a todos los operadores móviles con acceso radio, a los OMV Completos -por disponer de elementos de red 5G-, y también a aquellos operadores distintos de los anteriores que pudieran explotar redes 5G por cuenta de terceros, típicamente para redes privadas corporativas.

Respecto a otros prestadores de servicios que carezcan de red propia, tales como los OMV prestadores de servicios, no parece ser la intención del Ministerio su inclusión en el ámbito de aplicación, ya que la Disposición adicional primera relativa a la remisión de los análisis de riesgo al Ministerio sólo se refiere a los "operadores de redes".

No obstante, la mención a los "*prestadores de servicios de comunicaciones electrónicas basados, total o parcialmente en dichas redes 5G"* en la definición de operador podría generar alguna duda al respecto. Por tanto, convendría

[25] Los OMV completos no tienen red de acceso radio, pero explotan una red de comunicaciones, aseguran la interconexión con otros operadores y tienen numeración propia. Los OMV de tipo prestador de servicio carecen totalmente de red de comunicaciones, limitándose a revender los servicios del operador que les presta servicio.

[26] Cf. Referencia en nota al pie nº 8 del análisis coordinado de riesgos o nota al pie nº 28 de la caja de herramientas: *"Mobile virtual network operators (MVNOs) and critical infrastructure operators from another sector than telecommunications, which could operate 5G networks for their own activities or on behalf of third parties, would fall under a similar category of stakeholders."*

aclarar la mención a estos operadores, especialmente en el caso de que se les quiera aplicar las medidas que estén orientadas a la prevención de riesgos en la prestación de servicios.

Por otra parte, el mismo análisis coordinado de riesgos indica que la severidad de los escenarios que amenazan las redes 5G varía en función de un número de factores, entre ellos, el número y tipo de usuarios afectados y el tipo de servicios impactados (seguridad pública, emergencias, salud…).

De hecho, aunque prácticamente todos los Estados miembros se encuentran implementando las medidas de la caja de herramientas, hay disparidad en la concreción de las distintas medidas y países como Austria, Dinamarca o Estonia limitan su aplicación a aquellos operadores con un determinado número de usuarios.

Todos los operadores mencionados, que disponen de redes o partes de una red 5G, estarían obligados al cumplimiento de las obligaciones de seguridad previstas en el APL. Deberán analizar los riesgos de su red, gestionar los riesgos de sus suministradores, elaborar una estrategia de diversificación de suministradores, y aplicar medidas de mitigación en función del perfil de riesgo de sus suministradores.

Ahora bien, el mismo riesgo o vulnerabilidad en las redes 5G de estos operadores puede producir un impacto muy desigual para cada tipo de operador, dependiendo de la tipología de servicios afectados, el volumen de usuarios y el tipo de clientes a los que se preste servicio. Por ejemplo, la indisponibilidad de un servicio de mínima latencia en los servicios prestados a un hospital o industria logística, pueden tener una repercusión y perjuicio mayor que si la misma indisponibilidad afecta a servicios de consumidor final. De hecho, una de las razones principales para adoptar medidas de seguridad adicionales en la red 5G con respecto a las generaciones móviles anteriores se debe a que esta tecnología se utilizará en el desarrollo de servicios adaptados a la actividad de múltiples sectores económicos vitales para la sociedad. Por tanto, una incidencia de seguridad en un servicio 5G que pueda ocasionar una reducción en la velocidad de acceso a internet de los usuarios residenciales, puede representar una amenaza de menor prioridad con respecto a la posibilidad de que se vea comprometido el funcionamiento de servicios esenciales o críticos para la sociedad, como un sistema automatizado de control energético o se ponga en peligro la integridad de información confidencial, por ejemplo en el sector financiero o de la administración.

Por ello, en base a lo expuesto, se recomendaría que se aclarase y limitase el conjunto de operadores a los que sería de aplicación el APL. Asimismo, las medidas de seguridad deben ser proporcionadas a los riesgos y deberían aplicarse solo sobre aquellos operadores estrictamente necesarios en términos de seguridad, ya sea en función del volumen de usuarios potencialmente

afectados por un fallo de seguridad, o por impactar en servicios esenciales o críticos.

Respecto a los suministradores

La definición de estos agentes es muy amplia, ya que además de incluir a los proveedores de equipos (hardware y software) necesarios para la operación de las redes 5G, también se incluye a "*proveedores de servicios para el funcionamiento de redes 5G o de servicios 5G*". Esta definición podría contemplar un gran abanico de proveedores, tales como empresas de mantenimiento y gestión de red, integradores de servicios, empresas de suministro eléctrico u otros prestadores de servicios auxiliares. Además, al incluir en la definición de servicios 5G no solo los de comunicaciones electrónicas, sino también otros servicios de la sociedad de la información, la gama de suministradores se amplía considerablemente.

Se aconsejaría limitar la tipología de suministradores a los estrictamente ligados a las componentes y funciones esenciales de las redes 5G, definidos en el artículo 6.2 (núcleo de red, red de acceso, etc.).

Respecto a los fabricantes de dispositivos

No se incluye en el artículo 3 una definición de *"los fabricantes y las personas que pongan en el mercado español equipos terminales y dispositivos conectados"* mencionados en el artículo 4.3.

En el Anexo II de la LGTel los fabricantes y distribuidores de equipos y aparatos de telecomunicaciones se encuentran englobados en la definición de *"agentes económicos"*, entre los que se incluyen también a los representantes autorizados y a los importadores.

Por tanto, se considera recomendable tanto a efectos de claridad como de seguridad jurídica, modificar la definición de fabricantes en base a la definición de "agente económico" previsto en la LGTel, pero referido a los terminales y a los dispositivos conectados a la red 5G, en lugar de a los equipos de telecomunicación.

De tal forma, se sugiere incorporar un apartado i) en el artículo 3, cuyo contenido podría ser el siguiente:

> *«i) "fabricantes y otros agentes económicos": los fabricantes, representantes autorizados, importadores y distribuidores que pongan en el mercado español equipos terminales y dispositivos conectados a redes 5G».*

Asimismo, todas las menciones a *"los fabricantes de equipos terminales y dispositivos conectados o a quienes los pongan en el mercado"* dispersas a lo

largo del APL deberían adaptarse a este cambio de denominación y definición propuesto.

Respecto a los usuarios corporativos

El artículo 3.e) define como "*usuario corporativo*" a "la *persona física o jurídica que utiliza o solicita servicios 5G, que no están disponibles para el público, para fines profesionales".*

Posteriormente, el artículo 4 señala que los usuarios corporativos a los que aplica el APL serían:

> *4. los usuarios corporativos que tengan derecho de uso del dominio público radioeléctrico, el cual utilicen para explotar redes o prestar servicios en auto-prestación con capacidades específicas basadas en la tecnología 5G.*

Las personas físicas o jurídicas que explotan redes o prestan servicios basados en 5G en auto-prestación, serían usuarios de ámbito profesional -por distinguirlos de los consumidores- cuya explotación de redes o prestación de servicios de comunicaciones electrónicas no se realiza con el fin de obtener una retribución por ello.

En línea con el tipo de usuario corporativo previsto en el artículo 4 del APL, estas personas físicas o jurídicas no prestan servicios al público en general, sino que se limitan a satisfacer sus propias necesidades de comunicación o la de los usuarios vinculados con el servicio principal que estos prestan con carácter profesional (ej. empresas de energía que pueden llegar a explotar una red 5G para mejorar la operativa de su red de distribución y su funcionamiento[27]).

A la vista de ambas previsiones se señala que el término "*usuario corporativo*" implica la existencia de una organización o empresa, lo que excluye de su propia definición a las personas físicas. Además, la citada definición de *"usuario corporativo"* no contempla la posibilidad de que este tipo de usuarios exploten redes de comunicaciones electrónicas que permitan la prestación de servicios con capacidades propias de la tecnología 5G, como sí contempla el artículo 4.4.

Sin perjuicio de lo indicado para su consideración sobre la exclusión de las personas físicas, se propone modificar el texto del apartado 3.e) para alinearlo en mayor medida con el artículo 4.4:

> *«e) "usuario corporativo": la persona física o jurídica que explota redes, utiliza o solicita servicios con tecnología 5G, que no están disponibles para el público».*

Respecto a las obligaciones del APL aplicables a los usuarios corporativos se señala que éstos explotan redes 5G para prestar servicios en auto-prestación

[27] Sirva de ejemplo: https://www.endesa.com/es/prensa/sala-de-prensa/noticias/transicion-energetica/digitalizacion/endesa-participa-smart5grid-proyecto-europeo-5G-red-electrica

(un caso de usuario corporativo podría ser una autoridad portuaria con servicios de gestión de mercancías con realidad virtual), por lo que estarían sometidos a riesgos similares a los operadores. Sin embargo, el APL solo les obliga a colaborar para realizar el análisis de riesgos nacional y la evaluación de medidas de seguridad previstas en el artículo 10.3 del Esquema de seguridad.

Se recomienda especificar si existirán medidas de seguridad adicionales sobre los usuarios corporativos, que serán desarrolladas en el Esquema de seguridad, intentando reducirlas a las mínimas imprescindibles, en función de la calificación de estos agentes como operador crítico u operador de servicios esenciales.

Respecto a las normativas supletorias de seguridad

Debido a la posibilidad de afectación de la tecnología y servicios 5G sobre operadores críticos y de servicios esenciales, sería conveniente indicar en el artículo 5 del APL que, en todo lo que no resulte especificado en esta ley, será de aplicación supletoria no solo lo dispuesto en la Ley General de Telecomunicaciones, sino también en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, así como el Real Decreto 43/2021, de 26 de enero, que lo desarrolla.

Asimismo, convendría tener en cuenta a lo largo de la tramitación de esta nueva Ley aquellas posibles modificaciones a la Directiva SRI -actualmente en proceso de tramitación- que puedan impactar en la misma, así como en la LGTel[28].

IV.3 Análisis de riesgos (artículo 6)

Este artículo hace referencia a los elementos de la red 5G y los factores que deben ser tenidos en cuenta por los operadores en sus análisis de riesgos. Se considera conveniente añadir que deben aplicarse criterios de valoración de los riesgos, que permitan graduar su importancia, en función de su potencial impacto sobre los servicios prestados y su capacidad de recuperación, sobre los datos e información cuya integridad haya podido verse comprometida y sobre la cantidad y tipo de usuarios afectados.

Por otra parte, la lista de componentes y funciones esenciales de la red 5G que los operadores deben considerar en sus análisis de riesgos, según el apartado 2 del artículo 6, no es una lista cerrada, pudiendo variar en función de lo que se determine en el Esquema de seguridad. De igual forma, los factores que dichos análisis deberán tener en cuenta podrían ser determinados en el Esquema de

[28] La nueva Directiva SRI ampliaría el número de sectores esenciales y refuerza las obligaciones de seguridad, que incluirán también la seguridad de las cadenas de suministro. También pretende incorporar en su ámbito de aplicación las redes y servicios de comunicaciones electrónicas, que actualmente están en el Código Europeo, con el objetivo de armonizar todas las medidas de seguridad en una única directiva.

seguridad, al igual que los criterios de valoración de riesgos. Por consiguiente, se propone la inclusión de una referencia explícita al Esquema de seguridad que englobe todos los aspectos a considerar.

En concreto, se propone añadir un nuevo apartado 4 en el artículo 3 como sigue:

«4. Se deberán aplicar criterios de valoración de los riesgos, en función de siguientes parámetros:

- *Tipo de servicio que pueda verse afectado, y en particular, los asociados a servicios críticos o esenciales.*
- *Capacidad de detección y recuperación*
- *Número y tipo de usuarios afectados*
- *Tipo de información cuya integridad haya podido verse comprometida*

Al aplicar lo dispuesto en este apartado y en los anteriores, los operadores tendrán en cuenta y aplicarán lo que se determine en el Esquema de seguridad para las redes y servicios 5G».

IV.4 Análisis de las prácticas de seguridad de suministradores (artículo 7)

En el artículo 7 del APL se obliga a los operadores a que examinen cada dos años las prácticas de seguridad que implementen sus suministradores, sin embargo, no se detalla en qué debe consistir ese examen y si debe ser diferente en función del perfil de riesgo de los suministradores, que determine el Gobierno, conforme prevé el artículo 11 del APL.

Si bien esta Comisión entiende que la fijación de los parámetros que los operadores deberán examinar sobre sus suministradores, a efectos del cumplimiento de su obligación prevista en el artículo 7, puede realizarse a través del Esquema de Seguridad, se considera oportuno que se recoja expresamente en este texto el futuro desarrollo de dichos parámetros a través del Esquema de Seguridad.

En este sentido, se propone añadir al artículo 7 lo siguiente:

«Los criterios a examinar por los operadores sobre las prácticas de seguridad implementadas por sus suministradores, en función de su perfil de riesgo, tendrán en cuenta lo previsto, en su caso, en el Esquema de seguridad para las redes y servicios 5G».

IV.5 Medidas para gestionar los riesgos de seguridad (artículo 8)

De acuerdo con el artículo 8, una vez se apruebe el APL, los operadores estarán obligados a adoptar medidas técnicas y de organización adecuadas para mitigar los riesgos de seguridad de las redes y servicios 5G, incluyendo la gestión de los riesgos derivados de la actuación de sus suministradores.

En relación con estas obligaciones, el apartado 2 hace referencia a la aplicación de medidas de mitigación proporcionadas según se detalla en el artículo 14, que es un listado de obligaciones exigibles a los operadores que podrán desarrollarse en el Esquema de seguridad.

Adicionalmente, el apartado 3 del artículo 8 obliga a los operadores a elaborar una estrategia de diversificación de suministradores con medidas para limitar la dependencia de partes o funciones esenciales de la red de un solo suministrador o de varios que tengan una calificación de riesgo alto.

Sin embargo, no está claramente delimitado el alcance de las medidas que deberán ser aplicadas por los operadores, al mencionarse que "*los operadores tendrán en cuenta y aplicarán, en su caso, los elementos pertinentes que recojan en el análisis de riesgos nacional y el Esquema de seguridad para las redes y servicios 5G*".

Estas continuas referencias al Esquema de seguridad, que debe ser aprobado con posterioridad a esta norma, genera dos tipos de incertidumbre en relación con (i) el grado de concreción de las obligaciones y (ii) el momento a partir del cual los operadores deben adoptar las medidas de seguridad, mientras no esté aprobado el Esquema de seguridad.

Teniendo en cuenta que ya existen operadores con redes 5G en fase de despliegue y explotación comercial, la determinación de estas circunstancias es necesaria para que los operadores estén en disposición de cumplir las obligaciones establecidas en el APL. Cabe señalar al respecto, que los operadores de red están obligados, por la Disposición adicional primera, a remitir sus análisis de riesgos y un informe de las medidas técnicas y organizativas para mitigarlos a la autoridad pertinente en el plazo de 4 meses desde la aprobación de la Ley. Sin embargo, el APL no incluye ningún plazo específico que determine el momento a partir del cual los operadores deberán llevar a la práctica dichas medidas.

De hecho, el artículo 13 especifica que el Esquema de seguridad establecerá una jerarquía de riesgos y priorizará las obligaciones de seguridad que los órganos competentes exigirán para hacer frente a dichos riesgo. En el mismo artículo establece que podrá fijar plazos máximos de implementación para su realización.

Así, parecería que el Esquema de seguridad es el instrumento normativo que fijaría el plazo para aplicar las medidas de seguridad. Ahora bien, puede haber medidas técnicas y de organización que puedan ser aplicadas sin esperar a la aprobación del Esquema de seguridad (ej. adoptar requisitos estrictos de acceso a los elementos y funciones esenciales de la red), generándose cierta incertidumbre sobre qué medidas pueden y deben ser aplicadas con anterioridad al Esquema.

Por consiguiente, se recomendaría la introducción de aclaraciones en el texto del artículo 8 para concretar los plazos en que deberán ser aplicadas cada una de las medidas mencionadas en el artículo.

Por último, se ha de verificar que los requisitos de seguridad impuestos por los operadores a los suministradores -tales como el cumplimiento de estándares de seguridad- estén justificados en base al propósito perseguido de limitar los riesgos de seguridad, pero no supongan un obstáculo discriminatorio que pueda limitar la competencia entre ellos.

IV.6 Información al órgano competente (artículo 9)

Respecto a la obligación de los operadores de remitir al Ministerio los resultados de los análisis de riesgo, la descripción de medidas técnicas y organizativas para mitigarlas y el informe sobre las prácticas de seguridad de sus suministradores (artículo 9.1), convendría incluir la matización de que esta información debe remitirse al Ministerio periódicamente, por ejemplo, cada 2 años, en línea con la obligación establecida en los artículos 6 y 7.

Los operadores también deberán remitir su estrategia de diversificación de suministradores al Ministerio e informarle anualmente sobre su estado de ejecución (artículo 9.2). Sin embargo, no queda claro el momento en el que deberán comenzar a proporcionar esta información, puesto que no consta explícitamente como parte de los informes que los operadores deberán remitir al Ministerio en el plazo de 4 meses desde aprobación de la Ley, según la Disposición adicional primera. Por consiguiente, convendría incorporar aclaración al respecto.

IV.7 Valoración del perfil de riesgo de los suministradores (artículo 11)

El artículo 11 del APL incluye una lista de criterios mínimos a valorar para calificar el perfil de riesgo de los suministradores. Sin embargo, al no estar cerrada, podrían añadirse nuevos criterios, sin que se especifique en el texto si dichos criterios estarán definitivamente delimitados en el Esquema de seguridad que deberá desarrollarse.

Adicionalmente, el mismo artículo prevé tres niveles de calificación (bajo, medio alto) pero, a lo largo de la norma, las medidas condicionadas en función del perfil de riesgo solo se refieren al perfil de riesgo alto. Por tanto, se desconoce si también podrían habilitarse medidas regulatorias específicas para los suministradores con un perfil de riesgo medio.

Por ello, resulta particularmente relevante que los criterios para poder calificar a un suministrador como de riesgo alto, medio o bajo y las consecuencias de esta calificación queden claramente delimitadas en el APL y Esquema de seguridad, dada su gran relevancia e impacto en el mercado.

Además, teniendo en cuenta que el despliegue de las redes 5G ya se ha iniciado y se espera que para 2025 esta tecnología llegue al 75% de la población[29], la fijación de criterios, calificación de suministradores y aplicación de medidas deberían realizarse lo antes posible, para evitar que esta situación de incertidumbre se dilate en el tiempo, lo que perjudica al sector en general.

En este sentido, dado que se ha incluido un plazo de 4 meses para que los operadores remitan sus análisis de riesgos, informes sobre suministradores y medidas técnicas, se recomendaría también fijar el plazo máximo en el que la Administración competente efectúe la calificación del perfil de riesgo de los suministradores según lo establecido en el artículo 11.2 y establezca las obligaciones relacionadas con el perfil de riesgo del artículo 14.

Dado el impacto de la calificación del perfil de riesgo de los suministradores, se debe garantizar la transparencia de todo el procedimiento, especialmente de cara a los suministradores afectados, y dar audiencia previa a los afectados por la decisión que tome el Gobierno para evitar su indefensión.

Por otra parte, no está previsto en el APL que la calificación del perfil de riesgo, una vez realizada por el Gobierno, pueda ser revisada o modificada si determinados criterios del artículo 11.1 por el que fueron valorados hubieran variado. Convendría entonces aclarar en el APL si la calificación del perfil de riesgo de los suministradores puede ser revisada y el procedimiento para ello.

IV.8 Efectos en la competencia de las obligaciones (artículos 14 y 19)

Como se ha señalado en los comentarios generales, entre las medidas de seguridad previstas en el APL, la de mayor relevancia por su potencial impacto en el mercado y afectación a la competencia, es la posibilidad de restringir o incluso prohibir la utilización de suministradores con una determinada calificación de riesgo en las redes de los operadores.

Y, de manera particularizada, si la restricción se aplica sobre un suministrador ya presente en el despliegue de la red 5G de un determinado operador, que debe ser sustituido, este impacto podría ser significativo y afectar a la competitividad del operador en el mercado de servicios 5G. De hecho, en el cuestionario[30] de BEREC sobre las medidas de diversificación de suministradores de la caja de herramientas de la UE, los operadores señalaron que para reemplazar un

[29] Cf. “Estrategia de impulso de la tecnología 5G”. Además, en julio de 2021 se han adjudicado las concesiones de uso en la banda de 700 MHz, que llevan asociadas obligaciones de cobertura con un primer hito en 2022, y en el caso de una de las concesiones se debe alcanzar el 100% de los municipios de más de 20.000 habitantes a mitad de 2025.

[30] Informe BEREC BoR (20) 228 “*Report of BEREC recent activities concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)*”

suministrador 5G fuera del ciclo de vida habitual y sin coste significativo se necesitan más de 5 años.

Por tanto, se propone incorporar en el APL la obligación de analizar y valorar el potencial impacto desde el punto de vista competitivo de tales medidas en el mercado. Este criterio de afectación competitiva debería ser tenido en cuenta dentro de los criterios que la autoridad competente deba examinar a la hora de determinar las obligaciones de seguridad que se adecúen a la priorización de riesgos establecida por el Esquema de seguridad.

Se propone incorporar al artículo 14 relativo al detalle de las obligaciones, el requisito de que las obligaciones que puedan imponerse a operadores y suministradores sean proporcionadas, estén adaptadas a los riesgos de seguridad en función de su valoración, y no generen discriminación entre competidores. En particular, se propone incluir en el artículo 14 un apartado 5 con la siguiente redacción:

> *«5. Las obligaciones que se impongan de conformidad con este artículo deberán ser previamente analizadas en función de la valoración de los riesgos de seguridad que se pretenda mitigar, y la afectación a la competencia que puedan producir al mercado.*

Igualmente, en el artículo 19.1 se propone incluir la repercusión sobre la competencia en el párrafo que permite a los órganos competentes modular el alcance e intensidad de las obligaciones de seguridad.

IV.9 Limitaciones a la compartición de recursos (artículo 14.1.g)

Entre las obligaciones de seguridad exigibles a los operadores en el futuro Esquema de seguridad para las redes y servicios 5G, el artículo 14.1.g) del APL contempla la posibilidad de imponer la separación de emplazamientos y la limitación de la compartición de recursos en función de la importancia de la función de la red o del servicio a que van destinados.

Esta Comisión cree necesario que en el APL o en la normativa que lo desarrolle se ha de tener en cuenta el posible impacto que, dicha limitación a la compartición de recursos de red puede tener sobre el cumplimiento de las obligaciones de acceso a recursos o elementos específicos de las redes, que puedan imponerse por este organismo a los operadores, en virtud de lo dispuesto en los artículos 12, 13,14 y 15 de la LGTel, o sobre la regulación establecida en materia de compartición de infraestructuras en el Real Decreto 330/2016, de 9 de septiembre, relativo a medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de alta velocidad.

Por ello, se propone que se aclare el alcance de dicha limitación, para evitar que ésta pueda entrar en colisión con el cumplimiento de las obligaciones y el ejercicio de los derechos establecidos en la citada regulación por parte de los operadores de redes 5G.

IV.10 Diversificación de suministradores (artículos 8.3, 14.3 y 17)

Una de las principales medidas de la caja de herramientas de la UE consiste en la diversificación de suministradores a través de estrategias multi-proveedor en las redes de los operadores[31]. Esta medida ha sido incluida en el APL dentro de las obligaciones de los operadores, mediante el artículo 8.3, por el cual deben elaborar una estrategia de diversificación de suministradores con medidas para limitar la dependencia de partes o funciones esenciales de la red de un solo suministrador o de varios que tengan una calificación de riesgo alto, incluyendo plazos para restringir o excluir la presencia de suministradores de alto riesgo en dichos elementos y funciones.

Asimismo, el artículo 14.3 especifica que el Esquema de seguridad podrá fijar objetivos de diversificación de suministradores a los operadores y a nivel nacional, pudiendo imponerse obligaciones de sustitución o ampliación del número de suministradores para toda la red, para determinados componentes o clientes, o en determinadas áreas geográficas. Es decir, se incluyen estrategias multi-proveedor no solo en las redes de los operadores, sino también a nivel nacional, incorporando también la medida relativa al fortalecimiento de la resiliencia a nivel nacional[32] de la caja de herramientas de la UE.

Esta Comisión considera que la inclusión de estas obligaciones responde al objetivo de reforzar la seguridad de las redes 5G, puesto que disminuye el impacto sobre los servicios y usuarios de la red en caso de incidencia, indisponibilidad o ataque a los elementos o funciones esenciales de un determinado suministrador. Si la redundancia de equipos es uno de los requisitos habituales en los despliegues de red de los operadores, introducir requisitos de diversificación de suministradores permite una resiliencia a un nivel superior, defendiendo la integridad de la red y servicios 5G ante ataques o vulnerabilidades asociadas a un suministrador concreto, haya sido o no identificado con un perfil de riesgo.

Además de la mejora para la seguridad, añadir suministradores en las redes incrementará la competitividad y evitará el riesgo de depender excesivamente de un único suministrador en determinadas partes o elementos de la red, ya que ello puede incluso llegar a limitar el cambio de proveedor de equipos y con ello la competencia.

[31] Estrategia SM05 de la caja de herramientas.
[32] Estrategia SM06 de la caja de herramientas.

De hecho, estas ventajas fueron también puestas de manifiesto por las Autoridades de Regulación de los Estados miembros y por los operadores móviles de red en el cuestionario[33] de BEREC sobre las medidas de diversificación de suministradores de la caja de herramientas.

Esta Comisión apoya por tanto el impulso de medidas que permitan aumentar la diversidad de suministradores en la red, señalando además que incrementar el número de proveedores en funciones esenciales de la red podría asegurar la resiliencia de la red y disminuir el efecto de las amenazas vinculadas al uso de un determinado suministrador de alto riesgo. Con ello podría evitarse o limitarse la adopción de otras medidas más invasivas y restrictivas de la competencia, como la sustitución de los proveedores calificados de alto riesgo, al quedar restringido el impacto de una potencial amenaza.

Ahora bien, en el mismo cuestionario de BEREC los operadores señalaron que las principales desventajas asociadas a una estrategia multi-proveedor son las mayores dificultades para una correcta gestión de red y la interoperabilidad entre suministradores. De hecho, los operadores identificaron la necesidad de una mejor estandarización.

En este sentido, tiene especial relevancia apoyar el desarrollo de equipos 5G con arquitecturas abiertas, que permitan la aparición de un mayor número de suministradores, fomentando así la competencia.

El despliegue de equipos de red basados en estas arquitecturas abiertas supondría la incorporación de nuevos suministradores, con funcionalidades interoperables y a un menor coste a medio/largo plazo. Sin embargo, se observa que el desarrollo e implementación de soluciones de este tipo se encuentra aún en una situación de inmadurez tecnológica, y podrían no estar disponibles de forma inmediata en el mercado.

Dado el objetivo del APL de promover un mercado de suministradores suficientemente diversificado, se considera muy acertada la inclusión del artículo 17 en la norma, de apoyo a la I+D+I en ciberseguridad 5G. En este sentido, se recomienda que se apoye y fomente la investigación y desarrollo de iniciativas tecnológicas, en coordinación con la UE, que permitan diversificar el número de suministradores en las redes 5G, fortaleciendo la industria tecnológica europea, y cumpliendo con los requisitos de seguridad específicos de las redes 5G.

IV.11 Contratación pública (artículo 18)

Respecto a la posibilidad de exigir una certificación o imponerse la condición de exclusión de un determinado suministrador en un procedimiento de contratación pública de servicios que hagan uso de la tecnología 5G (artículo 18), se observa

[33] Informe BEREC BoR (20) 228 "*Report of BEREC recent activities concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)*"

una falta de concreción respecto a los casos en que dichas restricciones podrían imponerse.

Siempre que las funcionalidades de seguridad de los productos y servicios queden garantizadas, se recomienda que se utilicen procedimientos de contratación favorecedores de la competencia, evitando la imposición de restricciones en base a la seguridad que no estén adaptadas al nivel de riesgo del que se trate, limiten la concurrencia de proveedores y puedan suponer un mayor coste para la Administración. Toda restricción que pueda suponer una limitación competitiva deberá ser ponderada con respecto al riesgo de seguridad que se pretenda mitigar y ser impuesta en aquellos casos donde sea necesaria y proporcional al fin que se persigue.

IV.12 Régimen sancionador (artículo 22)

A la vista de los fines que se persiguen con la aprobación de esta Ley, se considera que el régimen sancionador que garantice el cumplimiento de dichos fines y disuada las conductas que pretendan conculcarlos, debería ser más detallado, sistemático y coherente con el régimen sancionador previsto o que se prevé regular en la LGTel, dado que el régimen sancionador de esta Ley será el régimen aplicable con carácter general. Ello también con el objeto de garantizar la seguridad jurídica a los posibles responsables por la posible comisión de infracciones tipificadas de forma similar en ambas Leyes.

En este sentido, se propone que se defina con mayor precisión los tipos infractores propuestos y que estos se gradúen y se sancionen tomando en cuenta los criterios ya establecidos en la LGTel, así como los propuestos por esta Comisión en el informe emitido sobre la revisión de esta Ley.

En primer lugar, en relación con las dos primeras infracciones[34], se propone tipificar el incumplimiento no solo grave sino también muy grave de las obligaciones establecidas en el Esquema de Seguridad (a) y de las resoluciones que dicten los órganos competentes (b). Este organismo entiende que es posible que los potenciales responsables (operadores, suministradores, fabricantes de equipos terminales y dispositivos conectados o a quienes los pongan en el mercado y a los usuarios corporativos de las redes y servicios 5G) solo se retrasen o realicen un cumplimiento defectuoso o parcial de las obligaciones o de lo dispuesto en las resoluciones, lo que debería ser tipificado con distinta graduación a su incumplimiento íntegro[35].

[34] Incumplimiento de las obligaciones establecidas en el Esquema de seguridad cuando sean directamente exigibles, lo que constituirá una infracción grave; e incumplimiento de las resoluciones dictadas por órganos competentes, lo que constituirá una infracción grave.

[35] En particular, este tipo de incumplimiento sería el grave -como ocurre en la LGTel con otros tipos de infracción, como el incumplimiento defectuoso o parcial de las resoluciones de la CNMC-, pudiendo sancionarse a través del tipo de infracción muy grave otros incumplimientos más relevantes.

Además, las respectivas infracciones grave y muy grave de las resoluciones dictadas por los órganos competentes (b) deberían especificar que (i) estas resoluciones han de ser firmes en vía administrativa y (ii) dictadas por los órganos competentes en el ejercicio de sus funciones en materia de seguridad de las redes y la prestación de servicios de comunicaciones electrónicas basados en la tecnología 5G. También, estos tipos infractores deberían incluir la posibilidad de que se incumplan las medidas provisionales que los órganos competentes puedan dictar.

Asimismo, se echa en falta la inclusión de sendos tipos infractores referentes al incumplimiento grave y muy grave de las obligaciones prevista en esa Ley por parte de los operadores, como las reguladas en los artículos 6 a 9 del Capítulo II y en la Disposición adicional primera, en relación con la realización de los análisis de riesgos y prácticas de seguridad de los suministradores en los plazos indicados de 4 meses, desde la aprobación de la Ley, y cada 2 años, así como la obligación de remitir dichos análisis de riesgos y prácticas de seguridad al MAETD.

En este mismo sentido, cabe tener en cuenta que en el artículo 7 del APL se obliga a los operadores a *"examinar las prácticas de seguridad de sus suministradores que puedan repercutir en los productos y servicios que les proporcionan, teniendo en cuenta los factores de riesgo indicados en este capítulo. Este examen debe repetirse, al menos, cada dos años".* Además, el artículo 8 del APL también les exige *"gestionar los riesgos derivados de la actuación de sus suministradores, y exigirles el cumplimiento de estándares de seguridad, desde el diseño de los productos hasta su puesta en funcionamiento, así como el control de su propia cadena de suministro. Deberán aplicar medidas de mitigación proporcionadas según se detalla en el Artículo 14, en particular en función de la calificación de riesgo que reciban los suministradores."*

Pues bien, el cumplimiento de estas obligaciones no será posible sin la debida colaboración de los suministradores en la entrega de datos sobre sus prácticas de seguridad[36] y el cumplimiento de los estándares de seguridad que les sean requeridos por los operadores. Por lo que se propone tipificar también el posible incumplimiento por parte de los suministradores de esa falta de colaboración con los operadores para el cumplimiento de sus obligaciones en materia de análisis de riesgos, en línea con la infracción prevista en el APL en relación con la falta de colaboración de los sujetos obligados por la Ley cuando esta es requerida por los órganos competentes.

En segundo lugar, en cuanto a los límites de los importes de las posibles sanciones a imponer en función de la gravedad de la infracción cometida, se indica que la previsión de una sanción por la comisión de una infracción muy grave estaría justificada si se adoptan los cambios antes propuestos, ya que atendiendo a la regulación prevista en el APL, no se prevé tipificar ninguna

[36] Como se ha señalado en los comentarios respecto al ámbito de aplicación.

infracción muy grave a la que le fuera posible imponer la sanción prevista a este tipo de infracciones (20 millones o el beneficio conseguido o perjuicio causado si su importe es mayor).

Es más, en línea con lo indicado por esta Comisión en el informe de 4 de diciembre de 2020 remitido al MAETD, sobre el APL de LGTel, se propone que la fijación de los límites máximos de las sanciones a imponer se base en el porcentaje sobre el volumen anual de negocios del operador infractor, en línea con lo previsto en otras normas como la Ley 15/2007, de 3 de julio, de Defensa de la Competencia (LDC) y el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679, de 27 de abril de 2016) (RGPD), además de que así se garantiza el efecto disuasorio exigible a un régimen sancionador.

Asimismo, en relación con el establecimiento de los límites máximos de las infracciones atendiendo al beneficio obtenido de la infracción, cabe recordar que el artículo 29.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP) prevé que *"El establecimiento de sanciones pecuniarias deberá prever que la comisión de las infracciones tipificadas no resulte más beneficioso para el infractor que el cumplimiento de las normas infringidas",* en la medida en que las sanciones han de ser disuasorias.

En esta línea, la LGTel prevé, a la hora de establecer los límites máximos de las sanciones previstas por la comisión de infracciones muy graves y graves, que se tengan en cuenta los beneficios, en caso de que estos puedan ser determinados, variando entre el tanto y el doble (infracciones graves) o el quíntuplo (infracciones muy graves) del beneficio bruto obtenido por los actos u omisiones en que consista la infracción. Por ello se propone incluir una previsión similar en el artículo 22 del APL.

Por último, sobre la vinculación del límite máximo de las sanciones a imponer a los perjuicios causados por la comisión de la infracción, se indica que atendiendo a lo dispuesto en el actual artículo 80 de la LGTel, los perjuicios causados sirven para graduar la sanción, no para determinar su límite máximo. Con el fin de garantizar la sistematización de ambas normas, se propone que se incluya en el APL un artículo similar al actual artículo 80 de la LGTel, en el que se distingan de forma específica para este tipo de infracciones, y tal y como este organismo propuso en el APL de la LGTel, por un lado, los límites máximos de las sanciones a imponer, y por otro lado, los criterios de graduación de la sanción que han de servir a la Administración competente para adecuar la sanción a imponer. Ello podría conducir a una mayor previsibilidad en la determinación de las sanciones y facilitar la motivación de su imposición.

Es más, con carácter adicional al pago de la sanción, los perjuicios causados como consecuencia de un incumplimiento deberían ser valorados a los efectos de generar el pago de una indemnización a aquellos a los que se les haya generado un daño, incluida a la propia Administración, teniendo en cuenta los fines que persigue la Ley propuesta en el APL (protección de la seguridad

nacional y fomento de la I+D+I nacionales en Ciberseguridad, entre otros) y que ambas medidas (la imposición de una sanción y de la indemnización por daños) son compatibles, al proteger intereses diferentes. Por tanto, tal y como dispone el artículo 28.2 de la LRJSP, se debería prever la posibilidad de que dichas indemnizaciones puedan ser determinadas y exigidas por los órganos competentes para sancionar las infracciones propuestas.

De hecho, aunque no sea la revisión de la LGTel el objeto de este informe, esta Comisión solicita también la inclusión de esta misma potestad administrativa, para determinar y exigir indemnizaciones por los daños generados por la comisión de una infracción, en el régimen sancionador previsto en la LGTel que se encuentra pendiente de revisión, de forma adicional al resto de propuestas ya planteadas sobre el régimen sancionador en el informe sobre el Anteproyecto de esta Ley, de 4 de diciembre de 2020[37] -algunas de ellas ya citadas en el presente informe-.

IV.13 Evaluación de la norma

También hay que referirse a que el anteproyecto no prevé mecanismos concretos de evaluación ex post. Debido a la importancia que puede tener la norma y su desarrollo en la competencia del sector, al poderse imponer restricciones a los operadores del mercado a la hora de participar en los contratos públicos y privados de desarrollo del 5G en España, sería recomendable fijar un hito a medio plazo para evaluar la eficacia de la norma, esto es, el grado de cumplimiento de los objetivos y fines de la norma y la idoneidad de las medidas adoptadas.

V CONCLUSIONES

El APL pretende incorporar a la normativa nacional las medidas de seguridad de las redes 5G acordadas a nivel europeo en la denominada caja de herramientas de la UE. Se introducen medidas de seguridad adicionales a las contempladas en el marco normativo nacional, que no solamente afectan a los operadores, sino que también impactan en los suministradores y otros agentes de la cadena de valor de redes y servicios 5G.

Se valora positivamente el Anteproyecto porque refuerza la seguridad de las redes 5G y los nuevos servicios que se desarrollarán sobre estas redes y fundamentarán la transformación digital en múltiples sectores económicos y servicios esenciales para la sociedad. Sin embargo, se considera conveniente modificar algunas de sus disposiciones, especialmente en relación con los siguientes aspectos:

[37] A raíz de la elaboración del informe emitido el pasado 15 de septiembre de 2021, sobre el Anteproyecto del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU), esta Comisión ha tenido conocimiento de la intención de incluir esta misma potestad administrativa, en supuestos de prácticas comerciales desleales, a través del artículo 51.6 del referido APL.

- Aclaración de las definiciones y ámbito de aplicación de los requisitos de seguridad.

- Aclaración del alcance, grado de concreción y momento temporal en el que comenzarán a aplicarse determinadas obligaciones, en particular, aquellas que pueden ser cumplimentadas sin esperar a la aprobación del Esquema de seguridad de las redes y servicios 5G.

- Inclusión de criterios de valoración de todos los riesgos, que permitan posteriormente determinar las medidas más adecuadas y proporcionadas con respecto a la importancia de cada riesgo.

- Incorporación de criterios de valoración de las obligaciones de seguridad con respecto a su potencial impacto en la competencia, en especial con respecto a aquellas medidas que puedan limitar o condicionar el uso de suministradores con un determinado perfil de riesgo.

- Revisión de algunos aspectos del régimen sancionador del Anteproyecto para que sea más detallado y sistemático.