BORRADOR DE ANTEPROYECTO DE LEY SOBRE REQUISITOS PARA GARANTIZAR LA SEGURIDAD DE LAS REDES Y SERVICIOS DE COMUNICACIONES ELECTRÓNICAS DE QUINTA GENERACIÓN

Desde su introducción generalizada a finales de los años 90 del Siglo XX, las redes móviles han sido un pilar del progreso de las telecomunicaciones y base para la introducción de las tecnologías de la información en todos los ámbitos de la sociedad, gracias tanto a la gradual extensión de su cobertura como, muy fundamentalmente, al desarrollo de nuevas capacidades que han incorporado las sucesivas generaciones de servicios móviles.

La más reciente de ellas, conocida como quinta generación o 5G, puede dar a las comunicaciones móviles e inalámbricas una nueva dimensión al permitir crear redes virtuales más versátiles, implantar servicios y aplicaciones de inteligencia artificial y prestar servicios de enorme valor añadido para la sociedad en ámbitos como el de la medicina, el transporte y la energía. Por eso, la Unión Europea y España impulsan el rápido despliegue de redes y la realización de proyectos demostrativos de su utilidad para distintos sectores.

La prestación de servicios avanzados para la población y la industria con apoyo en la tecnología se irá conformando como una realidad a lo largo de los próximos cinco o diez años. Pero, para que las redes 5G desarrollen el potencial que encierran es preciso generar la confianza necesaria en su funcionamiento continuado y en su protección frente a fugas o manipulaciones de datos o comunicaciones. Sin esa confianza, las personas y entidades que pueden aprovechar las oportunidades que ofrecen las redes 5G no harán uso de ellas, y la tecnología 5G no producirá los beneficios que se esperan de ella.

Las redes 5G poseen ventajas comparativas en seguridad respecto a las de generaciones precedentes. Pero presentan también riesgos específicos derivados por ejemplo de su arquitectura de red más compleja, su capacidad para transportar ingentes volúmenes de información y permitir la interacción simultánea de múltiples personas y cosas. Su interconexión con otras redes y el carácter transnacional de muchas de las amenazas inciden en su seguridad, y el previsible empleo generalizado de estas redes para funciones esenciales para la economía y la sociedad, incrementará el impacto potencial de los incidentes de seguridad que sufran.

Los equipos y programas informáticos cobran una importancia singular en las redes 5G pues sus prestaciones características, como la computación periférica o la segmentación múltiple de redes (*network slicing*), se orientan hacia paradigmas propios de la informática y los servicios de computación en nube, apartándose del enfoque tradicional de las arquitecturas de las redes de comunicaciones electrónicas. El funcionamiento de estas redes dependerá en gran medida de sistemas informáticos y de servicios proporcionados por proveedores externos a los operadores (designados colectivamente en esta ley como "suministradores"), creándose una dependencia de éstos que podría aumentar el nivel de riesgo al que se está expuesto.

La arquitectura de las redes 5G anteriormente descrita y los nuevos requisitos de seguridad, conllevan la necesaria evolución de las estrategias tradicionales, que se basaban en garantizar su disponibilidad, confidencialidad e integridad frente a ataques provenientes del exterior.

La complejidad técnica y el nuevo paradigma tecnológico que implica la inclusión y generalización en el mercado de las telecomunicaciones y en otros muchos sectores económicos de la tecnología 5G, hace que los retos de seguridad que se plantean alrededor de las redes 5G no puedan

abordarse en su totalidad con las normas sobre seguridad e integridad de las redes de comunicaciones electrónicas contenidas en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, ni con el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La materia regulada requiere una norma con rango de ley, ya que establece algunas limitaciones a la libertad de empresa y potestades administrativas que deben establecerse por ley. Justifican esas limitaciones y potestades la importancia para la sociedad de la garantía del funcionamiento ordinario de servicios esenciales que podrían depender en un futuro de las redes 5G. La apertura de la red a multitud de usos y aplicaciones aumenta los puntos de ataque a la red, y la importancia del papel de los suministradores en su arquitectura y gestión aconseja tomar precauciones para evitar posibles incidentes atribuibles a su actuación.

Así, las obligaciones previstas se refieren, entre otros aspectos, a los permisos de acceso a los programas y equipos que sustentan las redes 5G, a la segmentación o compartición de los recursos de red según su finalidad, a la interdependencia de las redes 5G y otros servicios esenciales y a la cadena de suministro.

A este respecto, se somete a los suministradores a estrictos controles de seguridad para garantizar su fiabilidad técnica y su independencia de injerencias externas, lo que da lugar a análisis de riesgos y medidas que realizarán los operadores y el Gobierno.

En el aspecto técnico, se da preeminencia a la aplicación de estándares internacionales y europeos y a los esquemas de certificación europeos que resulten de la ejecución del Reglamento (UE) 2019/881 del Parlamento europeo y del Consejo, de 17 de abril, sobre Ciberseguridad. Además, los operadores deberán poner en marcha una estrategia de

diversificación de suministradores para minimizar los riesgos e impacto de contingencias que les afecten.

En el ámbito estratégico, se examinará el perfil de riesgo de los suministradores más importantes de los operadores de redes y servicios 5G en España, en particular, desde el punto de vista de su protección frente a ataques y de su exposición a injerencias externas; pudiendo llegar a identificarse áreas, usuarios específicos o funciones restringidas de las redes donde no puedan actuar suministradores calificados como de *alto riesgo*, considerando la existencia de alternativas.

Para crearlas y reforzar la industria de 5G en España, se impulsará la investigación, desarrollo e innovación en torno a la tecnología 5G, también en lo que a la ciberseguridad 5G se refiere.

La presente ley establece solo normas especiales o adicionales a las existentes en otras leyes aplicables en materia de seguridad, incluidas la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, la Ley 36/2015, de 28 de septiembre, de seguridad nacional, el Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (Reglamento General sobre protección de datos personales), la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales o el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes, y sistemas de información.

En la elaboración de esta ley, se ha tenido en cuenta la Recomendación (UE) 2019/534, de 26 de marzo de 2019, de la Comisión europea, sobre la ciberseguridad de las redes 5G, el análisis de riesgos coordinado de los Estados miembros y la “caja de herramientas” acordada por éstos como base común para un desarrollo seguro de la tecnología 5G

en Europa. Se incluyen en esta ley las recomendaciones fundamentales que la Comunicación de 29 de enero de 2020 de la Comisión Europea "Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE" (COM/2020/50 final) realizaba a los Estados miembros sobre la utilización de la "caja de herramientas".

En este sentido, tanto los sujetos obligados por esta ley como los órganos competentes para su aplicación seguirán, en la mayor medida posible, las recomendaciones y la información sobre buenas prácticas referentes a la explotación y uso de la tecnología 5G que emanen de las instituciones comunitarias, de la Agencia europea de ciberseguridad (ENISA), y del grupo de cooperación establecido por el artículo 11 de la 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 Europea y la información sobre buenas prácticas recopiladas por dicho grupo y la red de CSIRT, regulado en el artículo 12 de aquélla.

Asimismo, se han tenido en cuenta los criterios y recomendaciones recogidas en la Estrategia Nacional de Ciberseguridad 2019 (orden PCI/487/2019 de 26 de abril) aprobada por el Consejo de Seguridad Nacional.

Se atribuye Gobierno la capacidad de detallar, mediante Real Decreto, las obligaciones se fijan en la ley, tanto para la propia administración como para operadores y suministradores, y la necesidad de que el instrumento para ello (el Esquema de seguridad para las redes y servicios 5G) se revise cada seis años al menos o cuando las circunstancias lo aconsejen. Entre estas circunstancias, sin duda, cabe entender las futuras revisiones o recomendaciones conjuntas de la Unión Europea sobre los riesgos relacionados con las infraestructuras del ecosistema digital y en particular, las redes 5G.

Cabe, finalmente, destacar el papel coordinador que asume el departamento de Asuntos Económicos y Transformación Digital tanto en las tareas de impulso a la I+D en materia de Ciberseguridad como en las de inspección, control de las auditorías y análisis de riesgos o en la potestad sancionadora previstas esta norma.

Se cumple el principio de necesidad pues esta ley se dicta para garantizar un bien de interés general, como es la seguridad y confianza en las comunicaciones electrónicas; es conforme con el principio de proporcionalidad ya que las medidas son adecuadas a los riesgos identificados en cada caso; se ajusta al principio de seguridad jurídica porque se reconoce el marco normativo vigente en materia de seguridad y solo se añaden requisitos y controles adecuados a la singularidad de las redes 5G y sus riesgos. Se respeta el principio de transparencia ya que los interesados han podido participar en el procedimiento de elaboración de esta ley. Por último, cumple el principio de eficiencia pues se han limitado las cargas administrativas al mínimo imprescindible para conseguir el fin perseguido de la seguridad.

Capítulo I

Disposiciones generales

Artículo 1. *Objeto.*

Esta ley establece requisitos de seguridad para el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas basados en la tecnología 5G.

Artículo 2. *Fines*.

Esta ley persigue los siguientes objetivos:

a) Reforzar la seguridad en la operación de las redes 5G, y en la prestación de los servicios de comunicaciones móviles e inalámbricas y de otros que se apoyen en las redes 5G.
b) Promover un mercado de suministradores suficientemente diversificado y evitar la dependencia de suministradores con una calificación de riesgo elevado.
c) Evitar posibles injerencias de terceros actores en la cadena de suministro.
d) Proteger la seguridad nacional.
e) Fortalecer la industria y fomentar la I+D+i nacionales en Ciberseguridad.

Artículo 3. *Definiciones.*

A los efectos de esta ley, se entenderá por:

a) "redes 5G" o "redes basadas en la tecnología 5G", el conjunto de elementos, hardware o software, de infraestructura de red que permiten dar conectividad móvil e inalámbrica y prestar servicios de valor añadido a usuarios y empresas con características avanzadas, que incorporen las funciones y capacidades y respondan a los casos de utilización recogidos en la Recomendación UIT-R M.2083, de la Unión Internacional de Telecomunicaciones.

   Estas características son, entre otras, la transmisión de grandes volúmenes de datos a alta velocidad, mínima latencia en las comunicaciones, alta fiabilidad y capacidad para conectar un número masivo de dispositivos a la red, o la provisión de servicios específicos para determinados usos o aplicaciones.

   Se considera que forman parte de las redes 5G la totalidad de funciones o partes relevantes de las redes empleadas para

ofrecer servicios con las capacidades señaladas. Por tanto, las redes 5G pueden incluir elementos de red basados en las generaciones móviles precedentes.

b) "servicios 5G", los servicios de comunicaciones electrónicas y otros servicios de la sociedad de la información en cuya prestación se emplean redes 5G.
c) "operadores", las personas físicas o jurídicas que explotan redes 5G y los prestadores de servicios de comunicaciones electrónicas basados, total o parcialmente en dichas redes 5G.
d) "suministradores", los suministradores de hardware y software y los proveedores de servicios para el funcionamiento de redes 5G o de servicios 5G.
e) "usuario corporativo", la persona física o jurídica que utiliza o solicita servicios 5G, que no están disponibles para el público, para fines profesionales.
f) "órgano competente", autoridad competente, por razón de la materia, para la aplicación y supervisión del cumplimiento de las disposiciones de la presente ley por los sujetos obligados que se identifican en el artículo siguiente.

Artículo 4. *Ámbito de aplicación.*

Esta ley se aplica a:

1. los operadores de redes y servicios de comunicaciones electrónicas basados en la tecnología 5G.
2. los suministradores.
3. los fabricantes y las personas que pongan en el mercado español equipos terminales y dispositivos conectados.

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.

Artículo 5. *Aplicación supletoria de la normativa sobre seguridad e integridad de las redes de comunicaciones electrónicas.*

En todo lo que no resulte especificado en esta ley, será de aplicación supletoria lo dispuesto en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y su normativa de desarrollo.

Capítulo II

Análisis y gestión de los riesgos

Artículo 6. *Análisis de riesgos de los operadores.*

1. Los operadores analizarán los riesgos de las redes y servicios 5G, considerando tanto los que afecten a elementos y funciones esenciales de las redes 5G como otros riesgos propios de las redes de comunicaciones electrónicas.

   Estos análisis se efectuarán, al menos, cada dos años.

2. Los análisis de riesgos considerarán de modo específico los siguientes componentes y funciones esenciales de las redes 5G:

   a) Los relativos a las funciones del núcleo de la red.
   b) La red de acceso.
   c) Las funciones de transporte y transmisión.
   d) Los sistemas de control y gestión y los servicios de apoyo.

e) Las funciones de computación periférica, virtualización de red y orquestación de sus componentes.
f) Los relativos a intercambios de tráfico con redes externas e Internet.
g) Otros componentes y funciones esenciales que, a tal efecto, se determinen en el Esquema de seguridad de las redes y servicios 5G.

3. Los análisis deberán tener en cuenta, al menos, los siguientes factores:

a) Dependencias de determinados suministradores o proveedores en elementos o funciones esenciales de la red.
b) Parametrización y configuración de elementos y funciones de red.
c) Políticas de integridad y actualización de los programas informáticos.
d) Estrategias de permisos de acceso a activos físicos y lógicos.
e) Agentes externos, incluyendo grupos organizados con capacidad para atacar la red.
f) Equipos terminales y dispositivos conectados a la red.
g) Elementos de usuarios corporativos y redes externas conectadas a la red 5G.
h) La interrelación con otros servicios esenciales para la sociedad.

Artículo 7. *Análisis de las prácticas de seguridad de los suministradores.*

Los operadores deberán 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.

Artículo 8. *Deber de gestionar los riesgos de seguridad.*

1. Los operadores deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes para las redes y servicios

5G, con base en lo establecido en esta ley y, supletoriamente, en la Ley 9/2014, de 9 de mayo, y su normativa de desarrollo.

En particular, deberán garantizar procedimientos de operación y supervisión seguros, adoptar requisitos estrictos de acceso a los elementos y funciones esenciales de la red, y que minimicen el acceso por entidades externas, así como garantizar procedimientos de operación y supervisión seguros.

2. Los operadores deberán 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.

3. Elaborarán 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.

   Al aplicar lo dispuesto en los apartados anteriores, 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.

Artículo 9. *Información al órgano competente.*

1. Los operadores deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital los resultados de los análisis de riesgo que realicen, una descripción de las medidas técnicas y organizativas para

mitigarlas, y un informe sobre las prácticas de seguridad de sus suministradores y sus modificaciones.

2. Los operadores deberán remitir su estrategia de diversificación de suministradores al citado Ministerio e informarle cada año sobre su estado de ejecución.

Capítulo III

Esquema de seguridad de las redes y servicios 5G

Artículo 10. *Esquema de seguridad para las redes y servicios 5G.*

1. El Gobierno aprobará, mediante real decreto, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital, un Esquema de seguridad para las redes y servicios 5G para abordar los riesgos que pongan de manifiesto los análisis que se efectuarán a nivel nacional.
2. Formarán parte de este análisis, entre otros aspectos:
   - El examen de las vulnerabilidades ligadas a la cadena de suministro de las redes 5G.
   - El análisis general de los riesgos de las redes y servicios, tomando en consideración la información recabada de los operadores de acuerdo con el artículo anterior.
   - La evaluación de las medidas de seguridad aplicadas hasta la aprobación de cada análisis de riesgos nacional para mitigar los riesgos puestos de manifiesto por tal análisis.
3. Todos los operadores y suministradores, los fabricantes y quienes pongan en el mercado equipos terminales y dispositivos conectados, así como los usuarios corporativos deberán prestar la colaboración que se

les requiera para realizar el análisis de riesgos nacional y la evaluación de la eficacia de las medidas de seguridad aplicadas.

4. El Gobierno cooperará estrechamente con otros Estados miembros y con la Comisión europea en todo lo relativo al Esquema de seguridad de las redes y servicios 5G, a la definición del perfil de riesgo de los suministradores y a la aplicación de las medidas de apoyo que la Comisión europea impulse.
5. El Gobierno podrá compartir información relacionada con los análisis que realice con la Comisión y con otros Estados miembros de la Unión Europea preservando, como corresponda en Derecho, la seguridad, los intereses comerciales y la confidencialidad de la información recabada en la elaboración del análisis, así como servirse de la información que le envíen otros Estados o la Unión Europea para su realización. Igualmente, podrá llevar a cabo estos análisis de forma conjunta con otros Estados miembros de la Unión Europea.
6. El Esquema de seguridad para las redes y servicios 5G será informado por el Consejo de Seguridad Nacional, y se revisará al menos cada seis años o cuando las circunstancias lo requieran.

Artículo 11. *Criterios para analizar las vulnerabilidades ligadas a la cadena de suministro.*

1. El Gobierno examinará el perfil de riesgo de los suministradores de los operadores de redes y servicios 5G en España. considerará en particular tanto las garantías técnicas de funcionamiento y su protección frente a ataques como su exposición a injerencias externas.

   Para el primero de los análisis se podrán valorar, entre otros, aspectos relativos al cumplimiento de normas o especificaciones técnicas, su

verificación mediante esquemas de certificación, o la superación de pruebas o auditorías de seguridad realizadas por partes independientes.

Para el segundo de estos análisis se valorarán, como mínimo, los siguientes aspectos:

a) Los vínculos de los suministradores y de su cadena de suministro, con los gobiernos de terceros países.

b) La composición de su capital social y la estructura de sus órganos de gobierno.

c) El poder de un tercer Estado para ejercer presión sobre la actuación o ubicación de la empresa.

d) Las características del régimen político y de su política de ciberdefensa, de ese tercer Estado.

e) Los acuerdos de cooperación en materia de seguridad, ciberseguridad, delitos cibernéticos o protección de datos firmados con el país tercero de que se trate, así como los tratados internacionales en esas materias de que sea parte dicho Estado.

f) El grado de adecuación de su normativa de protección de datos personales al Reglamento General de Protección de Datos adoptada por la Unión Europea.

2. El Gobierno, mediante Acuerdo de Consejo de Ministros, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital y previo informe del Consejo de Seguridad Nacional, calificará como bajo, medio o alto el perfil de riesgo de los suministradores según los resultados del análisis de las vulnerabilidades y especificará las consecuencias de dicha calificación.

3. El Gobierno evaluará el grado de dependencia de los suministradores del conjunto de redes y servicios 5G en España teniendo en cuenta los análisis de riesgos y las estrategias de diversificación de suministradores remitidos por los operadores, así como el riesgo de interrupción del

suministro por circunstancias económicas, societarias o comerciales que afecten a los suministradores.

Artículo 12. *Tratamiento integral de la seguridad para las redes y servicios 5G.*

El Gobierno dará un tratamiento integral a la seguridad de las redes y servicios 5G considerando las aportaciones al alcance de cada agente de la cadena de valor de 5G para garantizar un funcionamiento continuado y seguro de la red y los servicios.

De acuerdo con ello, el Esquema de seguridad para las redes y servicios 5G. contendrá una priorización de los riesgos que afectan a las redes y servicios 5G y desarrollará las medidas que han de adoptar los operadores para afrontarlos, obligaciones aplicables a suministradores, equipos terminales y dispositivos conectados, medidas para el fomento de la seguridad de las redes y servicios 5G, y requisitos para la contratación pública de comunicaciones 5G o de servicios que se basen en estas redes.

Artículo 13. *Priorización de riesgos en el Esquema de seguridad para las redes y servicios 5G.*

1. El Esquema de seguridad para las redes y servicios 5G establecerá una jerarquía de riesgos en función de los análisis de riesgos llevados a cabo por los operadores y el Gobierno, y de las deficiencias apreciadas en la evaluación de la eficacia de las medidas aplicadas.

   Asimismo, determinará y priorizará las obligaciones de seguridad que los órganos competentes exigirán para hacer frente a dichos riesgos. En concordancia con ello, podrá fijar plazos máximos de implementación y adoptar medidas de apoyo para su realización.

2. Las obligaciones establecidas en el Esquema de seguridad para las redes y servicios 5G se entienden sin perjuicio de la aplicación de los instrumentos de control sobre inversiones extranjeras directas en los operadores de redes y servicios 5G o en los suministradores españoles, y de la denuncia de conductas contrarias a la competencia en el mercado de suministros ante la Comisión europea o la Comisión Nacional de los Mercados y la Competencia, según proceda.

Artículo 14. *Obligaciones de seguridad exigibles a los operadores y suministradores.*

1. El Esquema de seguridad para las redes y servicios 5G podrá desarrollar, entre otras, las siguientes obligaciones exigibles a los operadores:
   a) Criterios para seleccionar e identificar a las personas que puedan acceder a los activos físicos y lógicos de la red, y mantenimiento de registros de acceso.
   b) Mantenimiento de las credenciales de usuario para el acceso a la red en posesión del operador.
   c) Condiciones, restricciones o prohibiciones para utilizar equipos, programas o servicios de suministradores de una determinada calificación de riesgo, incluyendo el establecimiento de cuotas o porcentajes de utilización, así como plazos para su eliminación de las redes.
   d) Condiciones, restricciones o prohibiciones para el acceso por el personal de los suministradores a los elementos o funciones de la red 5G esenciales para su correcto funcionamiento.
   e) Obligación de utilizar únicamente productos, servicios o sistemas certificados para la operación de las redes 5G, o en alguna de sus partes.

f) Restricciones en cuanto a la ubicación de los centros de gestión de la red y de seguridad, así como de los elementos que les den soporte.
g) Separación de emplazamientos y limitación de la compartición de recursos en función de la importancia de la función de red o del servicio a que van destinados.
h) Obligación de adoptar planes y medidas de contingencia específicas para asegurar la continuidad de otros servicios esenciales para la sociedad que dependan de las redes 5G, así como asegurar su propia continuidad ante incidencias en los servicios esenciales en los que se apoya la explotación de las redes 5G.

2. El Esquema de seguridad para las redes y servicios 5G podrá imponer, entre otras, las siguientes obligaciones de seguridad, según proceda, a los operadores y a sus suministradores:

a) Cumplimiento de normas o especificaciones técnicas aplicables a redes y sistemas de información.
b) Cumplimiento de esquemas europeos de certificación de productos, servicios o sistemas, sean o no específicos de la tecnología 5G, que se empleen en la explotación de redes 5G.
c) Sometimiento de los equipos y programas utilizados para la operación de las redes 5G a una auditoría o control externo por una entidad u organismo acreditado.
d) Sometimiento del operador o del suministrador, a su costa, a una auditoría de seguridad realizada por una autoridad pública o una entidad u organismo acreditado.
e) Superación de una auditoría por una entidad externa, solvente e independiente, u obtención de una certificación europea de seguridad para permitir la actuación en España de suministradores extranjeros.

3. El Esquema de seguridad para las redes y servicios 5G podrá fijar objetivos de diversificación de suministradores en la cadena de suministro de los operadores y para el conjunto del Estado, en función del cual podrán imponerse obligaciones de sustitución o ampliación del número de suministradores para toda la red, para componentes importantes de éstas, para determinados clientes, o en determinadas partes del territorio.
4. El Esquema de seguridad para las redes y servicios 5G podrá prever plazos transitorios para el cumplimiento de las obligaciones para los operadores, suministradores, fabricantes o quienes pongan en el mercado equipos terminales y dispositivos conectados y para los usuarios corporativos en función, entre otros aspectos, de la alta dependencia previa de proveedores considerados de alto riesgo, los ciclos de actualización de equipos o la migración de las redes 5G no autónomas a autónomas.

Artículo 15. *Certificación en elementos de redes 5G y requisitos esenciales para equipos terminales y dispositivos conectados.*

1. El Gobierno podrá supeditar la utilización de un equipo, programa o servicio externo en la gestión de las redes 5G a la previa obtención de una certificación establecida en virtud del Reglamento (UE) 2019/881, del Parlamento europeo y del Consejo, de 17 de abril de 2019, sobre la ciberseguridad.
2. La puesta en el mercado o el uso de equipos terminales y dispositivos conectados en relación con las redes 5G, estará condicionado al cumplimiento de los requisitos esenciales aplicables relacionados con la ciberseguridad, adoptados conforme a la normativa comunitaria, en particular en relación con la protección datos personales, privacidad, y la protección contra el fraude.

Artículo 16. *Aplicación adaptada a cada riesgo.*

Los órganos competentes podrán aplicar las obligaciones de seguridad previstas en el Esquema de seguridad para las redes y servicios 5G y en sus normas de desarrollo a todos los operadores, suministradores, fabricantes de equipos terminales y dispositivos conectados o a quienes los pongan en el mercado y a todos los usuarios corporativos por igual. Pero, también podrán aplicarlas de manera diferenciada y en distintos plazos o fases en supuestos debidamente justificados como:

a) La designación como operador crítico de un operador.
b) La importancia de un componente de red para la adecuada prestación del servicio.
c) El grado de dependencia de la tecnología 5G de un servicio o la gravedad del impacto que una disfunción en el funcionamiento de las redes podría ocasionar en ese servicio.
d) La atribución de una determinada calificación de riesgo a un suministrador.

Así mismo, podrán adoptarse medidas específicas respecto de determinadas redes y lugares si hay razones demográficas, sociales, económicas y de seguridad que así lo justifiquen.

Artículo 17. *Apoyo a la I+D+i en Ciberseguridad 5G*

1. El Esquema de seguridad para las redes y servicios 5G incluirá las líneas generales y prioridades de las ayudas públicas que pudieran ser convocadas para fomentar la investigación y el desarrollo en materia de seguridad en las redes 5G y en los servicios que dependan de ellas, y para la formación de personal especializado.

2. El Esquema de seguridad para las redes y servicios 5G impulsará la interoperabilidad de los equipos y programas ligados a la gestión de redes 5G, así como la participación de actores públicos y privados en la elaboración de estándares internacionales sobre el funcionamiento de las redes y servicios 5G.

Artículo 18. *Redes* y servicios *5G en la contratación pública.*

Cuando la Administración licite un contrato de comunicaciones o de servicios que hagan uso de la tecnología 5G, se exigirá para su adjudicación, cuando sea procedente, la posesión de una certificación derivada de un esquema de certificación europeo aprobado conforme al Reglamento (UE) 2019/881 del Parlamento europeo y del Consejo, de 17 de abril de 2019, sobre la ciberseguridad, que sea pertinente según el objeto del contrato.

De modo motivado, podrá imponerse la condición de excluir el uso de suministradores que tengan una determinada calificación de riesgo de un contrato público.

Capítulo IV

Potestades administrativas de control y sanción

Artículo 19. *Competencia para la aplicación del Esquema de seguridad para las redes y servicios 5G.*

1. El Ministerio de Asuntos Económicos y Transformación Digital será competente para aplicar el Esquema de seguridad para las redes y servicios 5G a los operadores, suministradores y fabricantes de equipos terminales y dispositivos conectados o a quienes los pongan en el

mercado. En todo lo que afecte a los suministradores de alto riesgo, actuará bajo la coordinación del Consejo de Seguridad Nacional.

Los demás departamentos ministeriales aplicarán las obligaciones de seguridad referidas a los usuarios corporativos que contenga el Esquema de seguridad para las redes y servicios 5G.

El Ministerio de Asuntos Económicos y Transformación Digital se coordinará con los demás órganos competentes para garantizar una aplicación coherente del Esquema de seguridad para las redes y servicios 5G, lo menos onerosa posible para los sujetos obligados.

Los órganos competentes modularán el alcance e intensidad de las obligaciones de seguridad en función de la prioridad otorgada por el Esquema de seguridad para las redes y servicios 5G al riesgo de que se trate, y de sus posibles repercusiones sobre el ritmo y coste del despliegue de red y el acceso de los usuarios a los servicios.

2. Los órganos competentes podrán ejercer las siguientes potestades para la aplicación de esta ley:

   a) Dictar órdenes ministeriales, instrucciones técnicas y guías orientativas para detallar el contenido del Esquema de seguridad para las redes y servicios 5G
   b) Dictar resoluciones para especificar las obligaciones que incumban a cada operador o suministrador, fabricante o quien ponga en el mercado equipos terminales o dispositivos conectados o usuario corporativo, o a cada categoría de ellos, que serán vinculantes para sus destinatarios.
   c) Formular requerimientos de información.
   d) Dirigir requerimientos de actuación u omisión a los sujetos obligados por esta ley para subsanar deficiencias detectadas.
   e) Realizar inspecciones y auditorías u ordenar su realización.

f) Realizar inspecciones de equipos terminales y dispositivos conectados.
g) Ejercer la potestad sancionadora.
h) Conceder ayudas públicas.
i) Ejercer las demás potestades que le correspondan según el Derecho administrativo.

Artículo 20. *Audiencia previa a la adopción de instrucciones técnicas, guías orientativas y resoluciones.*

Los órganos competentes darán audiencia a los titulares de derechos e intereses legítimos que resulten afectados por las instrucciones técnicas, guías orientativas y resoluciones que dicten. Se fomentará la participación de los ciudadanos y empresas en el procedimiento de elaboración de instrucciones técnicas.

Artículo 21. *Potestades de inspección.*

1. El Ministerio de Asuntos Económicos y Transformación Digital ejercerá en la aplicación y supervisión de lo establecido en esta ley todas las potestades de la función inspectora previstas en el Título VIII de la Ley 9/2014, de 9 de mayo.
2. En particular, los fabricantes de equipos terminales y dispositivos conectados o quienes los pongan en el mercado y los usuarios corporativos de las redes y servicios 5G podrán ser requeridos para proporcionar información y colaborar en la realización de inspecciones sobre los operadores y suministradores sometidos a esta ley.
3. Para garantizar la seguridad de la cadena de suministro de las redes y servicios 5G, el Ministerio de Asuntos Económicos y Transformación Digital podrá, además, requerir de los operadores información acerca de

sus suministradores, así como sobre los productos o servicios que tengan contratados con ellos.

Los operadores informarán al Ministerio sobre cualquier circunstancia o dato que pueda ser relevante para este análisis. Así mismo, les comunicarán los cambios importantes que tengan previsto realizar con sus suministradores, o en relación con ellos.

Artículo 22. *Régimen sancionador.*

1. Será de aplicación el régimen sancionador establecido en el Título VIII de la Ley 9/2014, de 9 de mayo, a excepción de las especialidades establecidas en el presente artículo.
2. Adicionalmente, se tipifican las siguientes infracciones:
    a) El incumplimiento de las obligaciones establecidas en el Esquema de seguridad para las redes y servicios 5G cuando sean directamente exigibles, lo que constituirá una infracción grave
    b) El incumplimiento de las resoluciones dictadas por órganos competentes, lo que constituirá una infracción grave.
    c) El incumplimiento de los requerimientos de información y de colaboración dictados por los órganos competentes, lo que será una infracción leve.

    Constituirá una infracción grave cuando el requerimiento se dirija a los operadores o a los suministradores y haya pasado un mes desde la finalización del plazo para su cumplimiento.
3. Las sanciones correspondientes a las infracciones aplicables a los operadores, suministradores y, en su caso, a los 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, serán las siguientes:

a) Por la comisión de infracciones muy graves, multa de hasta 20.000.000 euros. También podrá comportar la prohibición para contratar prevista en el art. 71 de la Ley 9/2017 de Contratos del Sector Público.
b) Por la comisión de infracciones graves, multa de hasta 2.000.000 euros.
c) Por la comisión de infracciones leves, amonestación o multa hasta 50.000 euros.

En el caso de que se acredite fehacientemente que el perjuicio causado o el beneficio obtenido con las prácticas sancionadas, supera estas cuantías, la sanción se incrementará hasta dicho importe.

4. Los órganos competentes para la aplicación del Esquema de seguridad para las redes y servicios 5G lo son también para la aplicación del régimen sancionador a los sujetos a los que, respectivamente, supervisen.

Disposición adicional primera. *Remisión al Ministerio de Asuntos Económicos y Transformación Digital de los análisis de riesgo de los operadores y prácticas de seguridad de los suministradores.*

1. Los operadores de redes deberán remitir en el plazo de 4 meses desde la aprobación de esta ley:
   a) Un análisis de riesgos de sus redes y servicios 5G o de los que vayan a desplegar en los próximos dos años y un informe de las medidas técnicas y organizativas para mitigarlos.
   b) Si ya prestan servicios 5G o han firmado contratos con vistas a ello, un informe sobre los suministradores que trabajan o trabajarán con ellos, los productos o servicios que les suministran o prestan o tienen previsto suministrar o prestar, y sobre las prácticas de seguridad de sus suministradores.

2. Los operadores de redes deberán remitir las actualizaciones periódicas de los informes considerados en el apartado anterior en el plazo de 4 meses desde su realización.

Disposición adicional segunda. *Aplicación de la ley a las sucesivas generaciones comunicaciones electrónicas.*

La presente ley será de aplicación para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de generaciones posteriores a la quinta generación mientras no exista norma específica para las mismas.

Disposición transitoria. *Obligaciones relacionadas con el perfil de riesgo de los suministradores.*

Hasta la aprobación del Esquema de seguridad para las redes y servicios 5G, se habilita al titular del Ministerio de Asuntos Económicos y Transformación Digital, previo informe del Consejo de Seguridad Nacional, a establecer las obligaciones relacionadas con el perfil de riesgo de los suministradores que se consideran en el artículo 14.

Disposición final primera. *Título competencial.*

Esta ley se dicta al amparo de lo previsto en el artículo 149.1. 21.ª de la Constitución, que atribuye al Estado competencia exclusiva en materia de régimen general de telecomunicaciones.

Disposición final segunda. *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno para desarrollar reglamentariamente lo previsto en esta ley.

Disposición final tercera. *Entrada en vigor.*

Esta ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».