Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

Jefatura del Estado
«BOE» núm. 76, de 30 de marzo de 2022
Referencia: BOE-A-2022-4973

ÍNDICE

TEXTO CONSOLIDADO
Última modificación: 20 de diciembre de 2023

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 integrar computación en la red, permitir crear redes virtuales, ofrecer baja latencia 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 y servicios 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, abierta y desagregada, y de 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 en el borde (*edge computing*) o la virtualización 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 este real decreto-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, ni con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

La materia regulada requiere una norma con rango de ley, ya que establece algunas obligaciones a empresas 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 y servicios 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.

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 de 2019, 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 usuarios específicos o funciones restringidas de las redes donde no puedan actuar suministradores calificados como de alto riesgo o de riesgo medio.

Para crear 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.

El presente real decreto-ley establece 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 de 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 este real decreto-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 este real decreto-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».

El artículo 86 de la Constitución permite al Gobierno dictar decretos-leyes «en caso de extraordinaria y urgente necesidad», siempre que no afecten al ordenamiento de las instituciones básicas del Estado, a los derechos, deberes y libertades de los ciudadanos regulados en el título I de la Constitución, al régimen de las Comunidades Autónomas ni al Derecho electoral general.

El Tribunal Constitucional ha declarado que la situación de extraordinaria y urgente necesidad que exige, como presupuesto habilitante, el artículo 86.1 de la Constitución Española, puede deducirse «de una pluralidad de elementos», entre ellos, «los que quedan reflejados en la exposición de motivos de la norma» (STC 6/1983, de 4 de febrero),

En este sentido, la STC 61/2018, de 7 de junio (FJ 4), exige, por un lado, «la presentación explícita y razonada de los motivos que han sido tenidos en cuenta por el Gobierno para su aprobación», y por otro, «la existencia de una necesaria conexión entre la situación de urgencia definida y la medida concreta adoptada para subvenir a ella».

En todo caso, el Tribunal Constitucional exige para la utilización de este tipo de norma que la situación que se pretenda regular se ajuste al «juicio político o de oportunidad que corresponde al Gobierno» (STC 182/1997, de 30 de octubre).

Por todo ello, de acuerdo con la jurisprudencia del Tribunal Constitucional, a continuación, se concretan las razones que justifican la extraordinaria y urgente necesidad de incorporar al ordenamiento jurídico español, mediante real decreto-ley, las recomendaciones contenidas en la «caja de herramientas» de la Unión Europea en materia

de Ciberseguridad 5G, a través de la aprobación del presente real decreto-ley sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

El 24 de febrero de 2022, las fuerzas armadas rusas iniciaron una agresión a gran escala de Ucrania desde Rusia, desde Bielorrusia y desde zonas no controladas por el Gobierno de Ucrania. Como consecuencia de ello, importantes zonas del territorio ucraniano se han convertido en zonas de conflicto armado.

El Consejo Europeo condenó con la máxima firmeza en sus Conclusiones de 24 de febrero de 2022 la agresión militar de Rusia contra Ucrania e hizo hincapié en que supone una grave violación del Derecho internacional y de los principios de la Carta de las Naciones Unidas. El Consejo Europeo exigió a Rusia que respetase plenamente la integridad territorial, la soberanía y la independencia de Ucrania dentro de sus fronteras reconocidas internacionalmente, lo que incluye el derecho de Ucrania a elegir su propio destino. En solidaridad con Ucrania, el Consejo Europeo acordó sanciones adicionales, pidió que prosiguiera la labor relativa a la preparación en todos los niveles e invitó a la Comisión Europea a que presentara medidas de emergencia.

Como consecuencia, el conflicto está provocando importantes implicaciones para la Unión Europea, entre las que se encuentra el incremento considerable del riesgo de ciberataques por motivos geoestratégicos, al que ya se refería el informe «Panorama de amenazas 2021», publicado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en octubre de 2021.

Los días 14 de enero, 15 de febrero y 23 de febrero de 2022, se han constatado ciberataques que han afectado gravemente a servicios gubernamentales y bancarios de Ucrania. Asimismo, en las últimas semanas, se han recibido diversas alertas de la Agencia de Ciberseguridad e Infraestructuras (CISA) de Estados Unidos, que destacan la necesidad de reforzar la protección de los países europeos frente a posibles ciberamenazas.

En consecuencia, teniendo en cuenta la situación de conflicto internacional derivada de la agresión contra Ucrania y el elevado riesgo de ciberataques contra redes y servicios 5G ya desplegadas en nuestro país o con despliegue previsto para los próximos meses, dentro de ese «juicio político o de oportunidad» que, de acuerdo con la citada STC 182/1997, de 30 de octubre, corresponde al Gobierno, se considera que concurren las razones de extraordinaria y urgente necesidad a las que se refiere el artículo 86 de la Constitución Española para la tramitación del presente proyecto como real decreto-ley.

Ello permitirá garantizar la entrada en vigor con celeridad de aquellas medidas que permiten prohibir o limitar la actividad en el mercado de suministradores que hayan sido considerados de alto riesgo o riesgo medio por el Gobierno, en base a criterios técnicos y aspectos estratégicos que pueden tener impacto en la seguridad, como el nivel de exposición a injerencias de terceros países, pudiendo llegar a identificarse usuarios específicos o funciones restringidas de las redes donde no puedan actuar estos suministradores calificados como de alto riesgo o riesgo medio.

En conclusión, se considera que el importante incremento del riesgo de ciberataques contra redes 5G desplegadas o a punto de ser desplegadas en nuestro país justifica la extraordinaria y urgente necesidad de adoptar cuanto antes medidas que, de acuerdo con lo establecido en la citada caja de herramientas, garanticen la ciberseguridad de la tecnología 5G y el refuerzo de la autonomía y soberanía tecnológica de la Unión Europea.

La aprobación de la llamada «Ley de Ciberseguridad 5G» (con la que identifica este real decreto-ley) está incluida como una de las reformas (Reforma C15R2) de la Componente 15 del Plan de Recuperación, Transformación y Resiliencia dedicado a «Conectividad digital, impulso de la ciberseguridad y despliegue del 5G», estando, en concreto, prevista como Hito CID 235 «la entrada en vigor de la Ley de Ciberseguridad 5G».

Se cumple el principio de necesidad, pues este real decreto-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 y servicios 5G y sus riesgos. Se respeta el principio de transparencia ya que los interesados han podido participar en el procedimiento de elaboración de un borrador de anteproyecto de ley previo. 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.

En su virtud, haciendo uso de la autorización contenida en el artículo 86 de la Constitución Española, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, y previa deliberación del Consejo de Ministros en su reunión del día 29 de marzo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Este real decreto-ley establece requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G).

Artículo 2. *Objetivos.*

Este real decreto-ley persigue los siguientes objetivos:

a) Impulsar una seguridad integral del ecosistema generado por la tecnología 5G.

b) Reforzar la seguridad en la instalación y operación de las redes de comunicaciones electrónicas 5G y en la prestación de los servicios de comunicaciones móviles e inalámbricas que se apoyen en las redes 5G.

c) Promover un mercado de suministradores en las redes y servicios de comunicaciones electrónicas 5G suficientemente diversificado en aras de garantizar la seguridad basada en razones técnicas, estratégicas y operativas y evitar, por dichas razones, la presencia de suministradores con una calificación de alto riesgo o de riesgo medio en determinados elementos de red o ámbitos.

d) Reforzar la protección de la seguridad nacional.

e) Fortalecer la industria y fomentar las actividades de I+D+i nacionales en ciberseguridad relacionadas con la tecnología 5G.

Artículo 3. *Definiciones.*

1. A los efectos de este real decreto-ley, se entenderá por:

a) «Operador 5G»: la persona física o jurídica que instala, despliega o explota redes públicas 5G o presta servicios 5G disponibles al público a través, total o parcialmente, de las redes 5G, disponga de red 5G propia o no, y ha notificado al Registro de operadores el inicio de su actividad o está inscrita en el Registro de operadores.

b) «Redes 5G» o «redes basadas en la tecnología 5G»: el conjunto integrado de elementos o infraestructuras de red, ya sean *hardware* o *software*, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, incluidos los recursos asociados e infraestructuras digitales, que permitan el transporte de señales con los que proporcionar conectividad móvil e inalámbrica y, a través de ella, prestar servicios de comunicaciones electrónicas e inalámbricas 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, o en el estándar técnico de la organización 3GPP (*3rd Generation Partnership Project*: Proyecto de Colaboración para la Tercera Generación).

Estas características avanzadas son, entre otras, la computación integrada en la red, 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 los elementos de red, infraestructuras, recursos y funciones de las redes empleadas para ofrecer servicios con las

capacidades señaladas, aun cuando también sean usados en las redes y servicios de comunicaciones electrónicas de generaciones móviles precedentes.

c) «Riesgo»: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y servicios 5G.

d) «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.

e) «Servicios 5G»: los servicios de comunicaciones electrónicas e inalámbricas, en los términos definidos en la Directiva 2018/1972, de 11 de diciembre de 2018, del Parlamento Europeo y del Consejo, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, sus servicios asociados y otros servicios conexos dirigidos a proporcionar funcionalidades y operatividad a los anteriores, como el almacenamiento en la nube (*cloud computing*) o la computación en el borde (*edge computing*), en cuya prestación se emplean redes 5G.

f) «Suministrador 5G»: el fabricante, el representante autorizado, el importador, el distribuidor, el prestador de servicios logísticos o cualquier otra persona física o jurídica sujeta a obligaciones en relación con la fabricación de productos, su comercialización o su puesta en servicio en materia de equipos de telecomunicación, los suministradores de *hardware* y *software* y los proveedores de servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G.

g) «Usuario corporativo 5G»: la persona física o jurídica que instala, despliega o explota redes privadas 5G o presta servicios 5G a través, total o parcialmente, de las redes 5G, para fines profesionales o en autoprestación.

2. Serán de aplicación, asimismo, las definiciones establecidas en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y en el Código Europeo de las Comunicaciones.

Artículo 4. *Ámbito de aplicación.*

Este real decreto-ley se aplica a:

a) Los operadores 5G.

b) Los suministradores 5G.

c) Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación.

Artículo 5. *Tratamiento integral de la seguridad.*

1. Los sujetos previstos en el artículo 4 deberán llevar a cabo un tratamiento integral de la seguridad de las redes, elementos, infraestructuras, recursos, facilidades y servicios de los que sean responsables, para lo cual deberán llevar a cabo, mediante un método holístico, un análisis de las vulnerabilidades, amenazas y riesgos que les afecten como agentes económicos y de los componentes anteriormente relacionados, así como una gestión adecuada e integral de dichos riesgos mediante la utilización de las técnicas y medidas que sean adecuadas para lograr su mitigación o eliminación y alcanzar el objetivo final de una explotación y operación seguras de las redes y servicios 5G.

A tal efecto, los sujetos previstos en el artículo 4 deberán dar debido cumplimiento a lo dispuesto en este real decreto-ley, a lo que se establezca en el Esquema Nacional de Seguridad de redes y servicios 5G y a los actos que se dicten en ejecución de ambas disposiciones.

2. Para alcanzar este tratamiento integral de la seguridad, los sujetos previstos en el artículo 4 deberán proporcionar la información que sea necesaria en virtud de lo dispuesto en este real decreto-ley o en el Esquema Nacional de Seguridad de redes y servicios 5G o la que le sea requerida por el Ministerio de Asuntos Económicos y Transformación Digital en ejercicio de las funciones que se les asignan en este ámbito.

Dicha información tiene la consideración de confidencial, de forma que la misma no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y

obligaciones establecidas en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

3. El Esquema Nacional de Seguridad de redes y servicios 5G llevará a cabo igualmente un tratamiento integral de la seguridad de las redes y servicios 5G, considerando al efecto las aportaciones al alcance de cada agente de la cadena de valor de 5G, así como la normativa, las recomendaciones y los estándares técnicos de la Unión Europea, de la Unión Internacional de Telecomunicaciones (UIT) y de otras organizaciones internacionales, con el fin de garantizar el objetivo último de una explotación y operación seguras de las redes y servicios 5G en nuestro país.

CAPÍTULO II

Análisis de riesgos

Artículo 6. *Análisis de riesgos por los operadores 5G.*

1. Los operadores 5G deberán analizar los riesgos de las redes y servicios 5G, detectando vulnerabilidades y amenazas que les afecten tanto como agente económico como por los elementos de red, infraestructuras, recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes 5G o en la prestación de servicios 5G.

2. Los operadores 5G que sean titulares o gestionen elementos de red de una red pública 5G, en su análisis de riesgos, deberán llevar a cabo un estudio pormenorizado e individualizado de las amenazas y vulnerabilidades que afecten, al menos, a los siguientes elementos, infraestructuras y recursos de una red pública 5G:

a) Los relativos a las funciones del núcleo de la red.
b) Las funciones de transporte y transmisión.
c) La red de acceso.
d) Los sistemas de control y gestión y los servicios de apoyo.
e) Las funciones de computación en el borde, virtualización de red y gestión de sus componentes.
f) Los relativos a intercambios de tráfico con redes externas e Internet.
g) Otros componentes y funciones que, a tal efecto, se determinen en el Esquema Nacional de Seguridad de redes y servicios 5G.

3. Son elementos críticos de una red pública 5G:

a) Los relativos a las funciones del núcleo de la red.
b) Los sistemas de control y gestión y los servicios de apoyo.
c) La red de acceso en aquellas zonas geográficas y ubicaciones que se determine.

4. El análisis de riesgos que lleve a cabo un operador 5G deberá tener en cuenta, al menos, los siguientes factores:

a) Parametrización y configuración de elementos y funciones de red.
b) Políticas de integridad y actualización de los programas informáticos.
c) Estrategias de permisos de acceso a activos físicos y lógicos.
d) Dependencias de determinados suministradores en elementos críticos de la red 5G.
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.

5. A fin de llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G, el operador 5G deberá recabar de sus suministradores las prácticas y medidas de seguridad que se han adoptado en los productos y servicios que les han suministrado, teniendo en cuenta los factores de riesgo indicados en este capítulo y el perfil de riesgo del suministrador. Esta información deberá ser proporcionada por los suministradores y su tratamiento será confidencial, de manera que sólo podrá ser utilizada por los operadores 5G para efectuar un análisis y gestión de riesgos y por el Ministerio de Asuntos Económicos y

Transformación Digital y los demás organismos públicos competentes para la aplicación de lo dispuesto en este real decreto-ley a los exclusivos fines del mismo.

6. El análisis de riesgos del operador 5G deberá incluir una priorización y jerarquía de los riesgos en función de los siguientes parámetros:

a) Afectación a un elemento crítico de la red pública 5G.
b) Tipo de recurso, infraestructura y servicio que pueda verse afectado.
c) Afectación a la integridad y mantenimiento técnico de la red o a la continuidad del servicio.
d) Capacidad de detección y recuperación.
e) Número y tipo de usuarios afectados.
f) Tipo de información cuya integridad haya podido verse comprometida.

7. El análisis de riesgos por el operador 5G debe ser llevado a cabo cada dos años y ser remitido al Ministerio de Asuntos Económicos y Transformación Digital.

Artículo 7. *Análisis de riesgos por los suministradores 5G.*

1. Los suministradores 5G deben analizar los riesgos de los equipos de telecomunicación, *hardware* y *software* y servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G, detectando vulnerabilidades y amenazas que le afecten tanto a la gestión de la empresa como a dichos equipos, *hardware*, *software* y servicios.

2. Los suministradores 5G deberán aportar este análisis de riesgos al Ministerio de Asuntos Económicos y Transformación Digital, cuando sea requerido para ello.

3. No obstante lo dispuesto en el apartado anterior, los suministradores 5G que hayan sido calificados de alto riesgo o de riesgo medio deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital un análisis de riesgos de sus equipos, productos o servicios involucrados en las redes y servicios 5G en el plazo de seis meses a contar desde que hayan sido calificados de alto riesgo o de riesgo medio.

4. Los suministradores 5G que sean calificados de alto riesgo o de riesgo medio deberán llevar a cabo el análisis de riesgos cada dos años y remitirlo al Ministerio de Asuntos Económicos y Transformación Digital.

Artículo 8. *Análisis de riesgos por los usuarios corporativos 5G.*

1. Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación deberán analizar los riesgos de las redes y servicios 5G, detectando vulnerabilidades y amenazas que afecten a los elementos de red, infraestructuras, recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes privadas 5G o en la prestación de servicios 5G en autoprestación.

2. Los usuarios corporativos 5G mencionados en el apartado 1 deberán aportar este análisis de riesgos al Ministerio de Asuntos Económicos y Transformación Digital, cuando sea requerido para ello.

Artículo 9. *Factores de riesgo a analizar por los sujetos previstos en el artículo 4.*

El Esquema Nacional de Seguridad de redes y servicios 5G deberá identificar los factores de riesgo a analizar por los sujetos previstos en el artículo 4 en función de la evolución tecnológica, la incorporación de nuevos avances, funcionalidades y estándares tecnológicos, la situación del mercado de comunicaciones electrónicas y del de suministros y de la aparición de nuevas amenazas y vulnerabilidades.

Artículo 10. *Confidencialidad de la información sobre análisis de riesgos.*

El Ministerio de Asuntos Económicos y Transformación Digital podrá recabar de los sujetos previstos en el artículo 4 la información necesaria para el análisis de riesgos.

La información que los referidos sujetos proporcionen sobre el análisis de riesgos tiene la consideración de confidencial, de forma que la misma no podrá ser utilizada para una

finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

CAPÍTULO III

Gestión de los riesgos

Artículo 11. *Deber de gestionar los riesgos de seguridad.*

Los sujetos previstos en el artículo 4 deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G, con base en lo establecido en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 12. *Gestión de seguridad por los operadores 5G.*

1. Los operadores 5G deberán garantizar la instalación, despliegue y explotación seguros de redes públicas 5G y la prestación segura de servicios 5G disponibles al público mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de redes y servicios 5G, así como el cumplimiento de lo establecido en este real decreto-ley.

2. Los operadores 5G tienen las siguientes obligaciones de seguridad dirigidas a mitigar riesgos:

a) Adoptar medidas técnicas y operativas para garantizar la integridad física y lógica de las redes 5G o cualesquiera de sus elementos, infraestructuras y recursos, así como la continuidad en la prestación de servicios 5G.

b) Adoptar planes y medidas de contingencia específicas para asegurar la continuidad de otros servicios esenciales para la sociedad que dependan de las redes y servicios 5G.

c) Seleccionar e identificar a las personas que puedan acceder a los activos físicos y lógicos de la red, y realizar el mantenimiento de registros de acceso.

d) Mantener las credenciales de usuario para el acceso a la red en posesión del operador.

e) Utilizar únicamente productos, recursos, servicios o sistemas certificados para la operación de las redes 5G, o en alguna de sus partes o elementos.

f) Cumplir las normas o especificaciones técnicas aplicables a redes y sistemas de información.

g) Cumplir con los esquemas europeos de certificación de productos, servicios o sistemas, sean o no específicos de la tecnología 5G, que se empleen en la operación o explotación de redes y servicios 5G.

h) Someterse, a su costa, a una auditoría de seguridad realizada por una entidad pública o una entidad privada acreditada a estos efectos.

i) Exigir a sus suministradores el cumplimiento de estándares de seguridad, desde el diseño de los productos y servicios hasta su puesta en funcionamiento.

j) Controlar su propia cadena de suministro y la estrategia de diversificación que haya diseñado.

3. En particular, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G tienen adicionalmente las siguientes obligaciones:

a) Deberán diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales en una red pública 5G, de forma que dichos equipos, sistemas o recursos sean proporcionados, como mínimo, por dos suministradores diferentes en la red de acceso. En el núcleo de la red y en los sistemas de control y gestión y los servicios de apoyo, el suministrador podrá ser único.

A estos efectos, se considera que los suministradores no son diferentes si todos ellos pertenecen al mismo grupo de empresas, conforme a los criterios establecidos en el artículo 42 del Código de Comercio.

b) No podrán utilizar en los elementos críticos de red equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo.

c) No podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo, en aquellas estaciones radioeléctricas con las que se proporcione cobertura a centrales nucleares, centros vinculados a la Defensa Nacional y las ubicaciones, áreas y centros que, por su vinculación a la seguridad nacional o al mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, sean determinados por el Consejo de Seguridad Nacional, previo informe del Ministerio de Transformación Digital. La determinación y difusión de estas ubicaciones serán tratadas como materias clasificadas conforme a la regulación establecida en la Ley 9/1968, de 5 de abril, sobre secretos oficiales.

d) Deberán solicitar y obtener del Ministerio de Transformación Digital autorización para la instalación, modificación o adaptación de estaciones radioeléctricas que proporcionen cobertura a estas ubicaciones, áreas y centros previamente determinados conforme a lo dispuesto en el párrafo anterior, habida cuenta de su vinculación con la seguridad nacional o el mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos. En el otorgamiento de esta autorización, el Ministerio de Transformación Digital tendrá en cuenta los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales, hardware, software o servicios auxiliares a instalar, las condiciones técnicas en el uso del dominio público radioeléctrico y las características intrínsecas y fines a proteger en esas ubicaciones, áreas y centros previamente determinados.

El plazo para el otorgamiento de estas autorizaciones es de tres meses, entendiéndose desestimada la solicitud en caso de ausencia de resolución expresa. La resolución, expresa o presunta, pone fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra el mismo un recurso de reposición con carácter previo al recurso contencioso-administrativo.

e) Deberán ubicar los elementos críticos de una red pública 5G dentro del territorio nacional. No obstante, determinados elementos, funciones y sistemas tanto del núcleo de la red como de los sistemas de control y gestión y los servicios de apoyo podrán ubicarse fuera del territorio nacional, siempre y cuando el Ministerio de Transformación Digital pueda ejercer las facultades que le atribuye este real decreto-ley, en particular, las facultades de inspección y régimen sancionador previstas en el capítulo V, de manera que pueda efectuar una verificación integral sobre el funcionamiento, operatividad y condiciones de uso de dichos elementos críticos de una red 5G y, en su caso, poder adoptar medidas, cautelares o definitivas, sobre dichos elementos, funciones y sistemas o el equipamiento utilizado en el ejercicio de estas facultades.

4. En el caso de que como consecuencia de operaciones de concentración empresarial, se redujera el número de suministradores incluidos en la estrategia de diversificación en la cadena de suministro que implicara que no se cumpliera el límite mínimo de dos suministradores diferentes establecido en el apartado 3.a) de este artículo, el operador 5G deberá comunicárselo al Ministerio de Asuntos Económicos y Transformación Digital, que impulsará que el Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previa audiencia de los operadores 5G y suministradores 5G afectados, decida si resulta posible mantener un suministrador único, teniendo en cuenta las condiciones concretas de la operación de concentración empresarial, la situación del mercado de los suministradores, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G, la calificación del suministrador como de alto riesgo, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, la migración de las redes 5G no autónomas a autónomas, así como su impacto económico.

5. Los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital la

estrategia de diversificación en la cadena de suministro en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley.

Asimismo, la estrategia de diversificación en la cadena de suministro deberá ser remitida al Ministerio de Asuntos Económicos y Transformación Digital cada vez que sea objeto de modificación.

Igualmente, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital información cada año sobre el estado de ejecución de la estrategia de diversificación en la cadena de suministro.

6. El Ministerio de Transformación Digital, si considera que no queda garantizada la continuidad en la prestación de los servicios 5G, la integridad física o lógica de la red 5G, que existe una amplia exposición al equipamiento instalado por un suministrador que en determinadas circunstancias puede poner en peligro la funcionalidad y operatividad de la red 5G o para garantizar la seguridad en la provisión de servicios utilizados por los servicios de Seguridad Nacional, Defensa Nacional o por distintas Administraciones Públicas, y teniendo en cuenta si existe calificación de suministradores de alto riesgo, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G, y los ciclos de actualización de equipos, podrá modificar la estrategia de diversificación en la cadena de suministro de un operador 5G.

Antes de aprobar la modificación, se deberá efectuar un trámite de audiencia con el operador 5G y suministrador o suministradores 5G afectados por un plazo de 15 días hábiles. La resolución pon fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra la misma un recurso de reposición con carácter previo al recurso contencioso-administrativo.

7. Los operadores 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital cada dos años una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos.

Artículo 13. *Gestión de seguridad por los suministradores 5G.*

1. Los suministradores 5G deberán garantizar la seguridad de los equipos de telecomunicación, *hardware*, *software* o servicios auxiliares que proporcionen y que sean objeto de uso por las redes y servicios 5G.

2. Los suministradores 5G tienen las siguientes obligaciones de seguridad dirigidas a mitigar riesgos, las cuales serán objeto de concreción y desarrollo en el Esquema Nacional de Seguridad de redes y servicios 5G:

a) Cumplir estándares de seguridad desde el diseño de los equipos, productos y servicios hasta su puesta en funcionamiento.

b) Reforzar la integridad del *software*, actualización y gestión de parches.

c) Acreditar la certificación de productos y servicios de tecnologías de la información que se usen en las redes y servicios 5G.

d) Garantizar la aplicación de medidas de seguridad técnicas y organizativas estándar a través de un sistema de certificación.

e) Efectuar una auditoría de seguridad de sus equipos, productos y servicios.

f) Proporcionar información sobre posibles injerencias de terceros en el diseño, operación y funcionamiento de sus equipos, productos y servicios.

g) Colaborar con los operadores 5G y usuarios corporativos 5G proporcionando información y acreditando el cumplimiento de estándares de seguridad de equipos, productos y servicios que suministren.

3. Los suministradores 5G deberán aportar al Ministerio de Asuntos Económicos y Transformación Digital una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

4. No obstante lo dispuesto en el apartado anterior, los suministradores 5G que hayan sido calificados de alto riesgo o de riesgo medio deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital un informe de las medidas técnicas y organizativas

diseñadas y aplicadas para gestionar y mitigar los riesgos en el plazo de seis meses a contar desde que hayan sido calificados de alto riesgo o de riesgo medio.

5. Los suministradores 5G de alto riesgo y de riesgo medio deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital cada dos años una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos.

Artículo 14. *Suministradores 5G de alto riesgo y de riesgo medio.*

1. El Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previo informe del Consejo de Seguridad Nacional y previa audiencia de los operadores 5G y suministradores 5G afectados por un plazo de 15 días hábiles, podrá calificar que determinados suministradores 5G son de alto riesgo.

A tal efecto, el Gobierno analizará tanto las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios como su exposición a injerencias externas.

2. En relación con el análisis de las medidas técnicas y las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios se valorará 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 entidades independientes.

3. En relación con el análisis de las medidas estratégicas y exposición a injerencias externas, se valorarán 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 de la legislación y la política de ciberdefensa y el respeto al derecho internacional y a las resoluciones y acuerdos de la Organización de las Naciones Unidas 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 la normativa del tercer Estado sobre protección de datos personales a la de España, al Reglamento General de Protección de Datos aprobado por 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 datos y por el que se deroga la Directiva 95/46/CE, adoptada por la Unión Europea y a cualquier otra normativa aplicable en materia de seguridad de las redes y sistemas de información y de telecomunicaciones.

4. El acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como suministradores de alto riesgo determinará el plazo en que lo operadores 5G deberán llevar a cabo la sustitución de los equipos, productos y servicios proporcionados por dicho suministrador en la red y servicios del operador 5G, cuando ello fuera necesario, para lo cual deberá tener en cuenta la situación del mercado de los suministradores, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G y en función de cuáles son en concreto los elementos críticos afectados, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, la migración de las redes 5G no autónomas a autónomas, así como su impacto económico, si bien, en ningún caso, este plazo podrá ser inferior a un año.

5. El acuerdo del Consejo de Ministros por el que se califique que determinados suministradores 5G son de alto riesgo pone fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra el mismo un recurso de reposición con carácter previo al recurso contencioso-administrativo.

6. Los suministradores de alto riesgo cuyos equipos de telecomunicación, *hardware*, *software* o servicios auxiliares proporcionados sean utilizados única y exclusivamente en redes privadas 5G o para la prestación de servicios 5G en régimen de autoprestación son calificados como suministradores de riesgo medio.

Artículo 15. *Gestión de seguridad por los usuarios corporativos 5G.*

1. Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación deberán garantizar la instalación, despliegue y explotación seguros de redes privadas 5G y prestación segura de servicios 5G en autoprestación mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de las redes y servicios 5G.

2. Los usuarios corporativos 5G mencionados deberán aportar al Ministerio de Asuntos Económicos y Transformación Digital una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

Artículo 16. *Condiciones de cumplimiento de las obligaciones.*

En el cumplimiento de las obligaciones establecidas en los artículos anteriores, los sujetos previstos en el artículo 4 tendrán en cuenta y aplicarán lo establecido en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 17. *Gestión de seguridad por las Administraciones públicas.*

1. Las administraciones públicas deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G.

2. En particular, las administraciones públicas que quieran llevar a cabo la instalación, despliegue y explotación de redes 5G, ya sean públicas o privadas, o la prestación de servicios 5G, disponibles al público o en autoprestación, no podrán, por razones de seguridad nacional, utilizar equipos, productos y servicios proporcionados por suministradores de alto riesgo o riesgo medio.

Artículo 18. *Cumplimiento de la normativa sobre inversiones extranjeras y sobre competencia.*

Las obligaciones establecidas en los artículos anteriores se entienden sin perjuicio de la aplicación de los instrumentos de control sobre inversiones extranjeras directas en los sujetos previstos en el artículo 4 que sean de nacionalidad española, así como de la aplicación de la normativa en materia de defensa de la competencia.

Artículo 19. *Confidencialidad de la información sobre gestión de riesgos.*

El Ministerio de Asuntos Económicos y Transformación Digital podrá recabar de los sujetos previstos en el artículo 4 la información necesaria para la gestión de riesgos.

La información que los referidos sujetos proporcionen sobre sobre la gestión de riesgos tiene la consideración de confidencial, de forma que la misma no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

CAPÍTULO IV

Esquema Nacional de Seguridad de redes y servicios 5G

Artículo 20. *Contenido del Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Esquema Nacional de Seguridad de redes y servicios 5G llevará a cabo un tratamiento integral y global de 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 5G.

2. En el Esquema Nacional de Seguridad de redes y servicios 5G se efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G así como identificará, concretará y desarrollará medidas a nivel nacional para mitigar y gestionar los riesgos analizados.

Artículo 21. *Aprobación y revisión del Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Gobierno aprobará, mediante real decreto, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital, previo informe del Consejo de Seguridad Nacional, un Esquema Nacional de Seguridad de redes y servicios 5G.

2. El Esquema Nacional de Seguridad de redes y servicios 5G se revisará al menos cada cuatro años o cuando las circunstancias lo aconsejen.

Artículo 22. *Análisis de riesgos en el Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Esquema Nacional de Seguridad de redes y servicios 5G efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G.

2. En este análisis de riesgos nacional se identificarán, entre otros, los siguientes aspectos:

a) El análisis general de los riesgos de las redes y servicios 5G, tomando en consideración la información recabada de los sujetos previstos en el artículo 4.

b) El examen de las vulnerabilidades ligadas a la cadena de suministro de las redes y servicios 5G.

c) La evaluación del grado de dependencia de los suministradores del conjunto de las redes y servicios 5G en España teniendo en cuenta los análisis de riesgos y las estrategias de diversificación de suministradores remitidos por los operadores 5G, así como el riesgo de interrupción del suministro por circunstancias económicas, societarias o comerciales que afecten a los suministradores.

d) La evaluación de la eficacia 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. El Esquema Nacional de Seguridad de redes y servicios 5G establecerá una jerarquía de riesgos en función de los análisis de riesgos llevados a cabo por los sujetos previstos en el artículo 4 y en función de las deficiencias apreciadas en la evaluación de la eficacia de las medidas aplicadas.

Artículo 23. *Gestión de riesgos en el Esquema Nacional de Seguridad de redes y servicios 5G.*

1. En el Esquema Nacional de Seguridad de redes y servicios 5G se establecerán, concretarán y desarrollarán criterios, requisitos, condiciones y plazos para que los sujetos previstos en el artículo 4 puedan dar cumplimiento a las obligaciones que a cada una de estas categorías de agentes económicos les impone este real decreto-ley.

Para ello, se tendrá en cuenta el análisis de riesgos nacional que incorpora la propia Estrategia Nacional y la evaluación de la eficacia de las medidas aplicadas con anterioridad por los sujetos previstos en el artículo 4 para mitigar y gestionar los riesgos en las redes y servicios 5G.

2. En el Esquema Nacional de Seguridad de redes y servicios 5G se podrá supeditar la utilización de un equipo, programa o servicio en concreto por un operador 5G, suministrador 5G o usuario corporativo 5G previsto en el artículo 4 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.

3. El Esquema Nacional de Seguridad de redes y servicios 5G, al margen de las estrategias de diversificación de la cadena de suministro que puedan tener los operadores 5G, podrá llevar a cabo un análisis específico y podrá proponer objetivos de diversificación de suministradores 5G en la cadena de suministro en las redes y servicios 5G para el conjunto del Estado, para lo cual podrá arbitrar medidas objetivas, proporcionadas y no discriminatorias dirigidas al cumplimiento de estos objetivos, siempre dentro del marco establecido en este real decreto-ley.

4. El Esquema Nacional de Seguridad de redes y servicios 5G también contendrá medidas para mitigar o gestionar los riesgos derivados del mercado de equipos terminales y dispositivos conectados.

La fabricación, importación, distribución, puesta en el mercado y comercialización de equipos terminales y dispositivos para conectarse a una red 5G y poder prestar servicios 5G, estará condicionado al cumplimiento de los requisitos esenciales aplicables relacionados con la ciberseguridad, adoptados conforme a la normativa europea, en particular, en relación con la protección de los datos personales, la privacidad, y la protección contra el fraude.

Artículo 24. *Deber de colaboración en la aprobación y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G.*

Todos los sujetos previstos en el artículo 4, así como los fabricantes, importadores, distribuidores y quienes pongan en el mercado y comercialicen equipos terminales y dispositivos para conectarse a una red 5G y poder prestar servicios 5G deberán prestar la colaboración y remitir la información que le sea requerida para la elaboración, aprobación y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G.

Artículo 25. *Cooperación internacional.*

1. El Gobierno cooperará estrechamente con otros Estados miembros de la Unión Europea y con las instituciones de la Unión Europea en la definición y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G y, en general, colaborará con las distintas organizaciones internacionales especializadas para poder llevar a cabo un tratamiento integral y global de la seguridad de las redes y servicios 5G.

2. En particular, el Gobierno y el Ministerio de Asuntos Económicos y Transformación Digital podrán compartir información relacionada con los análisis que realicen las instituciones de la Unión Europea 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 las instituciones de la Unión Europea para su realización. Igualmente, podrá llevar a cabo estos análisis de forma conjunta con otros Estados miembros de la Unión Europea.

Artículo 26. *Apoyo a la I+D+i en ciberseguridad 5G.*

El Esquema Nacional de Seguridad de 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 y servicios 5G y para la formación de personal especializado.

Artículo 27. *Impulso a la interoperabilidad.*

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

Artículo 28. *Facultades para la aplicación del Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Ministerio de Asuntos Económicos y Transformación Digital será el departamento competente para aplicar el Esquema Nacional de Seguridad de redes y servicios 5G y ejercer las demás funciones que le atribuye este real decreto-ley.

2. El Ministerio de Asuntos Económicos y Transformación Digital se coordinará con los demás órganos competentes en materia de ciberseguridad e infraestructuras críticas para garantizar una aplicación coherente del Esquema Nacional de Seguridad de redes y servicios 5G.

3. El Ministerio de Asuntos Económicos y Transformación Digital, en el ejercicio de las funciones que le asigna este real decreto-ley, podrá ejercer, entre otras, las siguientes facultades:

a) Desarrollar, concretar y detallar el contenido del Esquema Nacional de Seguridad de redes y servicios 5G.

b) Formular requerimientos de información a los sujetos previstos en el artículo 4, que deberán ser respondidos en el plazo de 15 días hábiles a contar desde el día siguiente al de su notificación, a efecto de poder ejercer las funciones que le asigna este real decreto-ley y su normativa de desarrollo y, en concreto, para verificar y controlar el cumplimiento de las respectivas obligaciones que este real decreto-ley y su normativa de desarrollo impone a los sujetos previstos en el artículo 4.

c) Realizar auditorías u ordenar su realización para verificar y controlar el cumplimiento de las respectivas obligaciones que este real decreto-ley y su normativa de desarrollo impone a los sujetos previstos en el artículo 4.

d) Realizar inspecciones por los funcionarios destinados en la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y ejercer la potestad sancionadora en los términos indicados en el capítulo siguiente.

e) Conceder ayudas públicas.

f) Ejercer las demás funciones que le correspondan según la legislación aplicable.

CAPÍTULO V

Inspección y régimen sancionador

Artículo 29. *Facultades de inspección.*

El Ministerio de Asuntos Económicos y Transformación Digital ejercerá en la aplicación y supervisión de lo establecido en este real decreto-ley todas las potestades de la función inspectora previstas en el título VIII de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Artículo 30. *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 este real decreto-ley.

2. Adicionalmente, se tipifican las siguientes infracciones clasificadas como muy graves, graves y leves.

3. Es infracción muy grave el incumplimiento por los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G de las obligaciones establecidas en el artículo 12.3.

4. Son infracciones graves:

a) El incumplimiento por los operadores 5G de las obligaciones establecidas en el artículo 12, excepto las contempladas en el artículo 12.3, que son infracciones calificadas como muy graves.

b) El incumplimiento por los suministradores 5G de las obligaciones establecidas en el artículo 13.

c) El incumplimiento por los usuarios corporativos 5G previstos en el artículo 4 de las obligaciones establecidas en el artículo 15.

d) El incumplimiento por las administraciones públicas de las obligaciones establecidas en el artículo 17.

e) El incumplimiento de estipulaciones establecidas en el Esquema Nacional de Seguridad de redes y servicios 5G cuando sean directamente exigibles.

f) El incumplimiento de los requerimientos de información formulados conforme al artículo 27.3.b) cuando haya pasado un mes desde la finalización del plazo dado para su cumplimiento.

5. Son infracciones leves los cumplimientos defectuosos o incumplimientos parciales de las conductas clasificadas como infracciones graves.

6. Las sanciones a aplicar son las establecidas en el artículo 79 de la Ley 9/2014, de 9 de mayo.

7. Los criterios para la determinación de la cuantía de la sanción son los establecidos en el artículo 80 de la Ley 9/2014, de 9 de mayo.

8. El ejercicio de la potestad sancionadora corresponde a la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

9. Se podrán aplicar las medidas previas y las medidas cautelares establecidas en los artículos 81 y 82 de la Ley 9/2014, de 9 de mayo, cuando sea oportuno conforme a la regulación contenida en dichos artículos.

Artículo 31. *Inspección y régimen sancionador de la Ley General de Telecomunicaciones.*

En lo no previsto en este real decreto-ley, será de aplicación lo establecido en la regulación contenida en materia de inspección y régimen sancionador del título VIII de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Disposición adicional primera. *Remisión al Ministerio de Asuntos Económicos y Transformación Digital de los análisis de riesgos de los operadores 5G y de las medidas técnicas y organizativas para mitigarlos.*

Los operadores 5G deberán remitir en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley 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 diseñadas y aplicadas para gestionar y mitigar los riesgos.

Disposición adicional segunda. *Remisión al Ministerio de Asuntos Económicos y Transformación Digital de las estrategias de diversificación en la cadena de suministro.*

Los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital la estrategia de diversificación en la cadena de suministro en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley.

Disposición adicional tercera. *Declaración de suministradores de alto riesgo.*

En el plazo de tres meses a contar desde la entrada en vigor de este real decreto-ley, el Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previo informe del Consejo de Seguridad Nacional y previa audiencia de los operadores 5G y suministradores 5G afectados por un plazo de 15 días hábiles, podrá calificar que determinados suministradores 5G son de alto riesgo.

A tal efecto, el Gobierno analizará tanto las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios como su exposición a injerencias externas en los términos indicados en el artículo 14.

Disposición adicional cuarta. *Determinación de centros y ubicaciones en los que no se podrán utilizar equipos, productos o servicios de suministradores de alto riesgo.*

En el plazo de tres meses a contar desde la entrada en vigor de este real decreto-ley, el Consejo de Seguridad Nacional, previo informe del Ministerio de Asuntos Económicos y Transformación Digital, determinará las ubicaciones y centros en los que, en virtud de lo establecido en el artículo 12.3.c), por su vinculación a la seguridad nacional o al

mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G no podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, *hardware*, *software* o servicios auxiliares de suministradores de alto riesgo.

Disposición adicional quinta. *Aplicación del real decreto-ley a las sucesivas generaciones de comunicaciones electrónicas.*

Este real decreto-ley es 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 única. *Sustitución de equipos, productos o servicios proporcionados por suministradores 5G declarados de alto riesgo.*

Si se produce la declaración de suministradores de alto riesgo en los términos indicados en la disposición adicional cuarta y ello trae como consecuencia que los operadores 5G tienen que sustituir los equipos, productos o servicios proporcionados por dichos suministradores 5G, los operadores 5G dispondrán de un plazo de cinco años a contar desde que los suministradores 5G hayan sido calificados de alto riesgo para llevar a cabo dicha sustitución en los elementos críticos de red relativos a las funciones del núcleo de la red y a los sistemas de control y gestión y los servicios de apoyo, así como de un plazo de dos años a contar desde que los suministradores 5G hayan sido calificados de alto riesgo para llevar a cabo dicha sustitución en los elementos críticos de red relativos a la red de acceso en aquellas zonas geográficas y ubicaciones conforme a lo establecido en el artículo 12.3.c).

Disposición final primera. *Título competencial.*

Este real decreto-ley se dicta al amparo de lo previsto en el artículo 149.1.21.ª y en el artículo 149.1.29.ª de la Constitución, que atribuyen al Estado, respectivamente, competencia exclusiva en materia de régimen general de telecomunicaciones y en materia de seguridad pública.

Disposición final segunda. *Aplicación supletoria de la normativa sobre seguridad e integridad de las redes de comunicaciones electrónicas.*

1. En todo lo que no esté regulado en este real decreto-ley, será de aplicación supletoria lo dispuesto en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y su normativa de desarrollo.

2. En lo no regulado en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y su normativa de desarrollo, será aplicación supletoria el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, así como su respectiva normativa de desarrollo.

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

1. Se habilita al Gobierno para desarrollar reglamentariamente lo previsto en este real decreto-ley y, en particular, para aprobar el Esquema Nacional de Seguridad de redes y servicios 5G.

2. El primer Esquema Nacional de Seguridad de redes y servicios 5G deberá ser aprobado en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley.

Disposición final cuarta. *Entrada en vigor.*

1. Este real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

2. Las obligaciones contenidas en los artículos, 12, 13, 15, 16 y 17 entrarán en vigor en el plazo de un mes a contar desde el día de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid, el 29 de marzo de 2022.

FELIPE R.

El Presidente del Gobierno,
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN

Información relacionada

- El Real Decreto-ley 7/2022, de 29 de marzo, ha sido convalidado por Acuerdo del Congreso de los Diputados, publicado por Resolución de 28 de abril de 2022. Ref. BOE-A-2022-7313