MEMORIA DE ANÁLISIS DE IMPACTO NORMATIVO DEL PROYECTO DE REAL DECRETO POR EL QUE SE APRUEBA EL ESQUEMA NACIONAL DE SEGURIDAD DE REDES Y SERVICIOS 5G.

RESUMEN EJECUTIVO

Ministerio/Órgano proponente	Ministerio de Transformación Digital Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales	Fecha	diciembre de 2023
Título de la norma	PROYECTO DE REAL DECRETO POR EL QUE SE APRUEBA EL ESQUEMA NACIONAL DE SEGURIDAD DE REDES Y SERVICIOS 5G		
Tipo de Memoria	Normal ☒ Abreviada ☐		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	En desarrollo de lo establecido en el 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, en particular, en aplicación de su capítulo IV, la propuesta aprueba el Esquema Nacional de Seguridad de las redes y servicios 5G (en adelante, ENS5G), con el fin de lograr un entorno confiable para el desarrollo y adopción de las redes y servicios 5G.		
Objetivos que se persiguen	- Llevar 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. - Garantizar un funcionamiento continuado y seguro de la red y los servicios 5G. - Impulsar una seguridad integral del ecosistema generado por la tecnología 5G.		

	- 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. - 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. - Reforzar la protección de la seguridad nacional. - Fortalecer la industria y fomentar las actividades de I+D+i nacionales en ciberseguridad relacionadas con la tecnología 5G.
Principales alternativas consideradas	No existe ninguna alternativa a la aprobación de la presente norma, ya que el artículo 21 del Real Decreto-ley 7/2022, de 29 de marzo, obliga al Gobierno a aprobar, mediante real decreto, a propuesta del Ministerio de Transformación Digital, previo informe del Consejo de Seguridad Nacional, un Esquema Nacional de Seguridad de redes y servicios 5G.
CONTENIDO, ANÁLISIS JURÍDICO Y DESCRIPCIÓN DE LA TRAMITACIÓN	
Tipo de norma	Real Decreto
Estructura de la Norma	El proyecto consta de una parte expositiva, un artículo único por el que se aprueba el ENS5G, dos disposiciones adicionales y cuatro disposiciones finales. El ENS5G que se aprueba consta de treinta y tres artículos divididos en ocho capítulos y de tres anexos.
Informes a recabar	- Informe de la CNMC - Procedimiento de información en materia de normas y reglamentaciones técnicas y de reglamentos relativos a los servicios de la sociedad de la información previsto en la Directiva (UE) 2015/1535

	- Informe de la Secretaría General Técnica del Ministerio de Trasformación Digital - Informe del Consejo de Seguridad Nacional - Dictamen del Consejo de Estado	
Trámite de audiencia	De acuerdo con lo establecido en el artículo 26.2 de la Ley 50/1997, de 27 de noviembre, del Gobierno y en el artículo 133.1 de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los días 30 de mayo y 22 de junio de 2022 se ha llevado a cabo consulta pública previa, a través de la sede electrónica del Ministerio de Asuntos Económicos y Transformación Digital. Asimismo, deberá llevarse a cabo el trámite de audiencia pública, conforme a lo señalado en los artículos 26.6 de la Ley 50/1997, de 27 de noviembre y 133.2 de la Ley 39/2015, de 1 de octubre.	
ANÁLISIS DE IMPACTOS		
Adecuación al orden de competencias	El Real Decreto y el esquema que aprueba se dictan al amparo de las competencias estatales en materia de telecomunicaciones y de seguridad pública, establecidas en los artículos 149.1.21ª y 149.1.29ª de la Constitución.	
Impacto económico y presupuestario	Efectos sobre la economía en general	De acuerdo con estudios de la Comisión Europea los beneficios estimados al introducir 5G en cuatro sectores productivos (automoción, salud, transporte y utilities) aumentarían progresivamente hasta alcanzar en 2025 los 62.500 millones de euros de impacto directo anual dentro de la Unión Europea, que se elevarían a 113.000 millones de euros sumando los impactos indirectos. El mismo estudio estima que en nuestro país se obtendrían unos beneficios indirectos en los cuatro sectores analizados de 14.600 millones de euros y una importante creación de empleos.

		La confianza en la seguridad de las redes y servicios 5G es clave para extender su utilización entre ciudadanos y empresas.
	En relación con la competencia	☐ la norma no tiene efectos significativos para la competencia. ☒ la norma tiene efectos positivos sobre la competencia. ☒ la norma tiene efectos negativos sobre la competencia
	Desde el punto de vista de las cargas administrativas	☐ supone una reducción de cargas administrativas. ☐ incorpora nuevas cargas administrativas. ☒ no afecta a las cargas administrativas
	Desde el punto de vista de los presupuestos, la norma: ☒ No afecta a los presupuestos de las	☐ implica un gasto

	Administraciones Públicas ☒ No afecta a los presupuestos de la Administración del Estado	☐ implica un ingreso
Impacto de género	La norma tiene un impacto de género	Negativo ☐ Nulo ☒ Positivo ☐
Otros impactos considerados		-Impacto en la lucha contra la despoblación y el cambio climático. -Impacto en relación con la igualdad de oportunidades, la no discriminación y la accesibilidad universal de las personas con discapacidad. -Impacto en relación con la infancia la adolescencia y la familia**.**
Otras **consideraciones**		

A. OPORTUNIDAD DE LA PROPUESTA

1. Motivación.

- **Causas:**

Las comunicaciones móviles de quinta generación o 5G constituyen un nuevo paradigma de las comunicaciones electrónicas con un gran potencial transformador en beneficio de la sociedad y la economía, pues abren la posibilidad a la incorporación de nuevas funcionalidades que van a tener un gran impacto como la computación en la red y permiten crear redes virtuales, ofrecer baja latencia y prestar servicios de gran valor añadido en ámbitos como el de la medicina, el transporte y la energía.

Por ello, tanto la Unión Europea como España vienen impulsando el rápido despliegue de redes 5G y la realización de proyectos demostrativos de su utilidad para distintos sectores mediante la prestación de servicios 5G.

Las redes y servicios 5G poseen ventajas comparativas en seguridad respecto a 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 asimismo, el previsible empleo generalizado de estas redes para funciones esenciales de la economía y la sociedad incrementará el impacto potencial de los incidentes de seguridad que sufran.

Estos nuevos riesgos específicos de seguridad de las comunicaciones móviles 5G se abordaron regulatoriamente a través del 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, que incorpora en toda su extensión la Recomendación (UE) 2019/534, de 26 de marzo de 2019, de la Comisión Europea, sobre la ciberseguridad de las redes 5G, así como las recomendaciones 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 dicha «caja de herramientas».

El citado Real decreto-ley 7/2022, de 29 de marzo, prevé su desarrollo reglamentario a través del Esquema Nacional de Seguridad de redes y servicios 5G (ENS5G).

De acuerdo con el artículo 5.3 del citado Real Decreto-ley, el ENS5G llevará a cabo 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.

Por su parte, el artículo 20 del Real Decreto-ley establece que, para garantizar un funcionamiento continuado y seguro de la red y los servicios 5G, el ENS5G efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G e identificará, concretará y desarrollará medidas para mitigar y gestionar los riesgos analizados.

Por último, de acuerdo con el artículo 21 del Real Decreto-ley el ENS5G será aprobado por el Gobierno, mediante real decreto, a propuesta del Ministerio de Transformación Digital, previo informe del Consejo de Seguridad Nacional.

La presente norma aprueba el ENS5G, desarrollando las previsiones del 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.

- **Colectivos afectados:**

  La norma se aplicará a:

a) Las personas físicas o jurídicas que explotan redes 5G y a los prestadores de servicios de comunicaciones electrónicas basados, total o parcialmente en dichas redes 5G.

   Esto incluye a operadores móviles titulares de concesiones administrativas para el uso del espectro radioeléctrico y a operadores móviles virtuales, así como a los operadores que utilicen la tecnología 5G para prestar servicios de comunicaciones. También incluye a los operadores que exploten redes privadas (o corporativas) de comunicaciones electrónicas, lo cual va a ser más frecuente con 5G de lo que es ahora con la tecnología 4G.

b) Los proveedores de equipos y servicios para la operación de las redes y servicios 5G, ajenos a los operadores (designados colectivamente en la norma como “suministradores”).

   Una parte de la norma les afecta de manera directa, es decir, contiene disposiciones cuyo cumplimiento puede ser exigido, y sancionado, por las autoridades competentes. Se trata, por una parte, de las obligaciones de colaboración en las funciones de supervisión de la Administración, y, por otra, de los requisitos de certificación de productos, procesos o servicios, o de sometimiento a auditoría que la norma impone.

   Pero, además, la norma les afecta también de manera indirecta, al exigir a los operadores de redes y servicios 5G el cumplimiento de requisitos de seguridad en relación con sus

suministradores. Este grupo de normas incluye disposiciones que pueden tener repercusiones importantes sobre los suministradores. Por ejemplo: la norma prevé que pueda exigirse a los operadores prescindir total o parcialmente de ciertos suministradores que se califiquen como de alto riesgo.

c) Los usuarios corporativos de las redes 5G.

Pueden ser las entidades que gestionen una capa o segmento de la red para sus fines propios (por ejemplo: un hospital para sus aplicaciones de telemedicina). Debido a su imbricación con la red principal, pueden ser una puerta de entrada de un ataque exterior.

Además, la norma, en cuanto asegura la seguridad de las redes y servicios 5G, beneficia a todos los usuarios de estas redes y servicios, en particular a las Administraciones Públicas, que podrán utilizarlas como canal seguro y eficaz de comunicación con los ciudadanos.

- **Interés público afectado:**

El interés público afectado es el de garantizar la máxima protección de las redes y servicios de comunicaciones basadas en tecnología y redes 5G frente a ataques o incidentes de seguridad, como medio para cimentar la confianza en los nuevos servicios 5G.

El previsible empleo generalizado de estas redes en funciones esenciales para la economía y la sociedad, y la dependencia de proveedores externos, obliga a que en un momento como el actual de graves tensiones geopolíticas, la ciberseguridad de las redes 5G se convierta en un objetivo prioritario de seguridad nacional.

Además, hay derechos fundamentales implicados, como el derecho a la intimidad personal y familiar o al secreto de las comunicaciones garantizados al más alto nivel normativo por la Constitución española.

A largo plazo, se encuentra también implicado el refuerzo de la autonomía tecnológica de la Unión europea.

Asimismo, dado el potencial de esta tecnología para el crecimiento de distintos sectores económicos, se encuentra afectado el crecimiento económico y social de España y el bienestar de los ciudadanos que accedan a servicios esenciales o ejerzan su derecho a la información, a través de redes 5G.

- **Por qué es el momento apropiado para hacerlo:**

Es oportuno que los operadores adapten cuanto antes sus políticas de ciberseguridad a las medidas establecidas en la norma, a fin de que las redes y servicios de comunicaciones móviles de quinta generación sean seguros desde el primer momento.

Además, ha de tenerse en cuenta que el apartado segundo de la Disposición final tercera del Real Decreto-ley 7/2022, de 29 de marzo, establecía un plazo de seis meses a contar desde su entrada en vigor, para la aprobación del ENS5G, plazo que ya ha sido superado.

2. Objetivos.

La norma tiene por objetivo último asegurar la fiabilidad de las redes y servicios 5G, y con ello el desarrollo de servicios de valor añadido para la economía y la sociedad, en áreas tan diversas como los transportes, la sanidad, la industria, la agricultura, la logística, la energía o los medios de comunicación.

Para ello se fijan como objetivos concretos:

- Llevar 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.
- Garantizar un funcionamiento continuado y seguro de la red y los servicios 5G.
- Impulsar una seguridad integral del ecosistema generado por la tecnología 5G.
- 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.
- 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.
- Reforzar la protección de la seguridad nacional.
- Fortalecer la industria y fomentar las actividades de I+D+i nacionales en ciberseguridad relacionadas con la tecnología 5G.

3. Alternativas.

No existe ninguna alternativa a la aprobación de la presente norma, ya que el artículo 21 del Real Decreto-ley 7/2022, de 29 de marzo, obliga al Gobierno a aprobar, mediante real decreto,

a propuesta del Ministerio Transformación Digital, previo informe del Consejo de Seguridad Nacional, un Esquema Nacional de Seguridad de redes y servicios 5G.

4. Adecuación a los principios de buena regulación.

La norma cumple con los principios de buena regulación enunciados en el artículo 129 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas.

Se cumple el principio de necesidad, pues este real decreto se dicta por mandato del Real Decreto-ley 7/2022, de 29 de marzo, 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.

La norma, se ajusta al principio de seguridad jurídica en cuanto desarrolla lo establecido en el 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 y completa el marco normativo vigente en materia de seguridad, añadiendo requisitos y controles únicamente cuando la singularidad de las redes y servicios 5G y sus riesgos, así lo exigen.

Se respeta el principio de transparencia, ya que los interesados han podido participar en el procedimiento de elaboración de la norma y la misma será objeto de publicación.

Por último, se cumple el principio de eficiencia, pues se han limitado las cargas administrativas al mínimo imprescindible para conseguir el fin perseguido de garantizar la seguridad de las redes y servicios 5G.

5. Plan Anual Normativo

El Real Decreto-ley 7/2022, de 29 de marzo, se corresponde con el anteproyecto de Ley sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, previsto en el Plan Anual Normativo de la Administración General del Estado para 2022, aprobado por Acuerdo del Consejo de Ministros de 11 de enero de 2022.

El presente proyecto, por el que se desarrolla dicho Real Decreto-ley no está, sin embargo, previsto en el Plan Anual Normativo correspondiente a 2023.

B. CONTENIDO Y ANÁLISIS JURÍDICO Y DESCRIPCIÓN DE LA TRAMITACIÓN

1. Contenido.

La norma consta de una parte expositiva, un artículo único por el que se aprueba el ENS5G, dos disposiciones adicionales y cuatro disposiciones finales.

El ENS5G que se aprueba consta de treinta y tres artículos divididos en ocho capítulos y de tres anexos.

La exposición de motivos explica los motivos que impulsan la aprobación de la norma y los artículos del Real Decreto-ley que se desarrollan.

El artículo único aprueba el Esquema Nacional de Seguridad de las redes y servicios 5G.

La disposición adicional primera señala que el Gobierno, mediante real decreto, a propuesta del Ministerio de Transformación Digital, previo informe del Consejo de Seguridad Nacional, revisará el Esquema Nacional de Seguridad de redes y servicios 5G cuando las circunstancias lo aconsejen y, en todo caso, cada cuatro años.

La disposición adicional segunda señala que el Real decreto-ley 7/2022, de 29 de marzo, y el ENS5G serán de aplicación a generaciones de comunicaciones electrónicas posteriores a la quinta generación mientras no exista norma específica para las mismas.

La disposición final primera sobre título competencial señala que el real decreto y el esquema que aprueba se dictan al amparo de lo previsto en el artículo 149.1.21ª y en el artículo 149.1.29ª de la Constitución, que atribuyen al Estado, respectivamente, competencia exclusiva en materia de régimen general de telecomunicaciones y en materia de seguridad pública.

La disposición final segunda declara de aplicación supletoria la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y su normativa de desarrollo y señala que en lo no regulado en dicha normativa, 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.

La disposición final tercera sobre desarrollo reglamentario habilita a la persona titular del Ministerio de Transformación Digital para desarrollar lo previsto en este real decreto y el esquema que aprueba y para modificar mediante orden el contenido de los anexos en función de la evolución del avance tecnológico, de la aprobación de nuevos estándares técnicos y esquemas de certificación de equipos de telecomunicación y productos conectados y del desarrollo de diferentes configuraciones y parámetros técnicos de redes y servicios 5G y de venideras generaciones de comunicaciones electrónicas.

La disposición final cuarta dispone que la norma entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

En cuanto al contenido del ENS5G, que se aprueba:

El artículo 1 señala que la norma se dicta en desarrollo del Real Decreto-ley ley 7/2022, de 29 de marzo, en particular, en aplicación de su capítulo IV.

El artículo 2 se refiere a los objetivos de la norma, ya analizados.

El artículo 3 señala que se utilizarán las definiciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y en el Código Europeo de las Comunicaciones Electrónicas.

El artículo 4 determina que la norma aplicará a operadores 5G, suministradores 5G y 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.

El artículo 5 señala los elementos, infraestructuras y recursos mínimos que integran una red de comunicaciones electrónicas 5G, remitiendo su descripción detallada al Anexo I. Asimismo, establece cuáles son los elementos críticos de una red 5G, que deberán situarse, como norma general, en territorio nacional (recogiendo las posibles excepciones).

El artículo 6 se refiere al tratamiento integral de la seguridad conforme a la normativa internacional comunitaria y nacional aprobada o que pueda aprobarse, obligando a lo sujetos obligados a llevar a cabo, mediante un método holístico, un análisis de las vulnerabilidades, amenazas y riesgos que les afecten como agentes económicos y de los distintos componentes, 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.

El artículo 7 destaca que el análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada

El artículo 8 se refiere a la vigilancia continua y a la reevaluación periódica.

El artículo 9 señala que el análisis de riesgos a nivel nacional es el que figura en el anexo II y que se ha realizado teniendo en cuenta diversos elementos como la información recabada de los sujetos obligados, el examen de las vulnerabilidades ligadas a la cadena de suministro de las redes y servicios 5G, la evaluación del grado de dependencia de los suministradores, el riesgo de interrupción del suministro por circunstancias económicas, societarias o comerciales que afecten a los suministradores o la evaluación de la eficacia de las medidas de seguridad aplicadas.

El artículo 10, sobre gestión de riesgos a nivel nacional, señala que los criterios, requisitos, condiciones y plazos para que los sujetos obligados puedan diseñar e implementar técnicas y medidas de mitigación de riesgos son los que figuran en el anexo III.

El artículo 11 desarrolla lo establecido en el artículo 14 del Real Decreto-ley 7/2022, de 29 de marzo, en relación con el procedimiento y los aspectos a valorar por el Consejo de Ministros para la calificación de suministradores como de alto riesgo y los elementos a tener en cuenta a la hora de ordenar la posible sustitución de los equipos, productos y servicios proporcionados por dichos suministradores. Asimismo, conforme a lo dispuesto en el citado Real Decreto-ley se señala que 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.

El artículo 12 sobre determinación de ubicaciones en las que no se podrá instalar equipos de suministradores calificados de alto riesgo señala que el Consejo de Seguridad Nacional, previo informe del Ministerio de Transformación Digital, podrá determinar las ubicaciones, áreas y centros en las que no se podrá instalar equipos de suministradores calificados de alto riesgo. Para la instalación, modificación o adaptación de estaciones radioeléctricas que proporcionen cobertura a estas ubicaciones, áreas y centros, los operadores 5G deberán solicitar autorización al Ministerio de Transformación Digital.

El artículo 13 obliga a los operadores 5G a diseñar una estrategia de diversificación en la cadena de suministro y a contar en la red de acceso, con equipos de transmisión que sean proporcionados, como mínimo, por dos suministradores diferentes. Se proporcionan, asimismo, criterios a tener en cuenta por el Consejo de Ministros, para decidir si resulta posible mantener un suministrador único si como consecuencia de operaciones de concentración empresarial se redujera el número de suministradores. Asimismo, se señalan los supuestos y el procedimiento mediante el que el que el Ministerio de Transformación Digital, puede modificar la estrategia de diversificación en la cadena de suministro de un operador 5G.

El artículo 14 se centra en el análisis de riesgos que han de llevar a cabo los operadores 5G en relación con todos los elementos, infraestructuras y recursos de la red que figuran en el Anexo I, se listan los factores que han de tenerse en cuenta, se obliga a los operadores a recabar de sus suministradores las prácticas y medidas de seguridad adoptadas en los productos y servicios que les han suministrado y a incluir una priorización y jerarquía de los riesgos en función de determinados parámetros que también se listan. Antes del día 1 de octubre de 2024 los operadores 5G han de presentar un análisis de riesgos, y, a continuación, cada dos años.

El artículo 15 sobre análisis de riesgos por los suministradores 5G obliga a 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, y a aportar dicho análisis al Ministerio cuando así se requiera. En el caso de suministradores calificados como de

alto riesgo o de riesgo medio, el análisis de se remitirá en el plazo de seis meses a contar desde dicha calificación y posteriormente cada dos años.

El artículo 16 sobre análisis de riesgos por los usuarios corporativos 5G obliga a aportar este análisis de riesgos al Ministerio Transformación Digital, cuando dichos usuarios sean requeridos para ello.

El artículo 17 permite al Ministerio de Transformación Digital recabar de los sujetos obligados la información necesaria para el análisis de riesgo y califica como infracción grave la no aportación de dicha información en un plazo de 15 días hábiles. La información tiene la consideración de confidencial y no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en el Real decreto-ley 7/2022, de 29 de marzo, en el ENS5G y en los actos que se dicten en ejecución de ambas disposiciones.

El artículo 18 proclama el deber general de todos los sujetos obligados de gestionar los riesgos de seguridad.

El artículo 19 se centra en la gestión de seguridad por los operadores 5G, listando obligaciones para todos los operadores (como las de adoptar planes y medidas de contingencia, cumplir las normas o especificaciones técnicas y esquemas europeos de certificación, someterse, a su costa, a una auditoría de seguridad o exigir a sus suministradores el cumplimiento de estándares de seguridad) y otras adicionales para aquellos operadores que sean titulares o exploten elementos críticos de una red pública 5G (como las prohibiciones de utilización de equipamiento de suministradores de alto riesgo en los elementos críticos de red o en determinadas ubicaciones, áreas y centros). Los operadores 5G deben remitir al Ministerio de Transformación Digital una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos antes del día 1 de octubre de 2024 y, a continuación, cada dos años. Además, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Transformación Digital una estrategia de diversificación en la cadena de suministro antes del día 1 de octubre de 2024 y después cada vez que ésta sea objeto de modificación. Antes del día 1 de octubre de cada año deberán remitir información sobre el estado de ejecución de dicha estrategia.

El artículo 20 sobre gestión de seguridad por los suministradores 5G, recoge un listado de obligaciones entre las que se encuentran el efectuar una auditoría de seguridad de sus equipos, productos y servicios, proporcionar información sobre posibles injerencias de terceros en el diseño, operación y funcionamiento de sus equipos, productos y servicios o colaborar con los operadores 5G y usuarios corporativos 5G proporcionando información y acreditando el cumplimiento de estándares y certificaciones. Los suministradores 5G deben elaborar un informe de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos y aportar dicho informe al Ministerio cuando así se requiera. En el caso de suministradores calificados como de alto riesgo o de riesgo medio, el informe se remitirá en el plazo de seis meses a contar desde dicha calificación y posteriormente cada dos años.

El artículo 21, sobre gestión de seguridad por usuarios corporativos 5G, señala que éstos 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 riesgo medio y que deberán aportar al Ministerio de Transformación Digital, cuando sean requeridos para ello, una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos.

El artículo 22, sobre gestión de seguridad por las Administraciones públicas, señala que, por razones de seguridad nacional, en 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, las AP no podrán, utilizar equipos, productos y servicios proporcionados por suministradores de alto riesgo o riesgo medio.

El artículo 23 señala que, en el cumplimiento de las obligaciones establecidas en los artículos anteriores, los sujetos obligados tendrán en cuenta y aplicarán lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, en el ENS5G y en los actos que se dicten en ejecución de ambas disposiciones.

El artículo 24 permite al Ministerio de Transformación Digital recabar de los sujetos obligados la información necesaria para la gestión de riesgos y califica como infracción grave la no aportación de dicha información en un plazo de 15 días hábiles. La información tiene la consideración de confidencial y no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en el Real decreto-ley 7/2022, de 29 de marzo, en el ENS5G y en los actos que se dicten en ejecución de ambas disposiciones.

El artículo 25 señala que todos los sujetos obligados, así como las Administraciones públicas, 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 les sea requerida para la modificación y ejecución del ENS5G.

El artículo 26 señala que mediante orden de la persona titular del Ministerio de Transformación Digital se podrá supeditar la utilización de un equipo, sistema, programa o servicio en concreto por los sujetos obligados 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, o de los esquemas de certificación y normas técnicas de certificación de equipos y productos 5G que a nivel europeo o internacional puedan aprobarse.

El artículo 27 señala que la norma se aplica sin perjuicio de la normativa sobre inversiones extranjeras y sobre competencia.

El artículo 28 sobre equipos terminales dispone que 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 de seguridad para los productos digitales y 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.

El artículo 29 se refiere a la cooperación internacional a desarrollar por el Ministerio de Transformación Digital, en especial en el ámbito de la Unión europea

El artículo 30 se refiere a la competencia del Ministerio de Transformación Digital para la aplicación del ENS5G, debiendo coordinarse con los demás órganos competentes en materia de ciberseguridad e infraestructuras críticas para garantizar una aplicación coherente del ENS5G.

El artículo 31 desglosa las facultades para la aplicación del ENS5G que corresponden al Ministerio de Transformación Digital, entre las que se encuentran, por ejemplo, el desarrollo, concreción y detalle del contenido del ENS5G, la realización de auditorías para verificar y controlar el cumplimiento de las obligaciones impuestas o la concesión de ayudas públicas.

El artículo 32 atribuye Ministerio de Transformación Digital todas las potestades de la función inspectora.

El artículo 33 relativo al régimen sancionador remite a lo dispuesto en los artículos 30 y 31 del Real Decreto-ley 7/2022, de 29 de marzo.

El Anexo I describe los elementos, infraestructuras y recursos que integran una red 5G.

El Anexo II contiene el análisis de riesgos a nivel nacional.

El Anexo III recoge la gestión de riesgos a nivel nacional.

2. Análisis jurídico.

- **Relación con otras normas nacionales**.

- La norma desarrolla el 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, y en particular, su capítulo IV, relativo al ESN5G.

- La Ley 9/2014, de 9 de mayo (especialmente su artículo 44), recoge obligaciones de seguridad genéricas que los operadores de redes 5G siguen teniendo que cumplir.

- El Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, establece requisitos que deberán seguir cumpliendo los operadores que hayan sido designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

- La Orden IET/1090/2014, de 16 de junio, por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas regula, en su capítulo VI, la obligatoria notificación a las Autoridades de los casos de interrupción del servicio telefónico y de acceso a Internet y su capítulo VII, se refiere a la potestad inspectora de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

- El Plan Nacional de Ciberseguridad aprobado el día 29 de marzo de 2022 por el Consejo de Ministros concreta, a través de actuaciones y proyectos específicos, distintas medidas recogidas en la Estrategia Nacional de Ciberseguridad 2019.

- Asimismo la norma es coherente con el Componente 15 del Plan de Recuperación, Transformación y Resiliencia de España, cuyo objetivo es garantizar la conectividad en todo el territorio nacional, liderar el despliegue de las redes y servicios basado en tecnologías 5G en Europa, y posicionar a España como un hub internacional de infraestructuras y talento en materia de ciberseguridad. Este componente se articula a través de dos planes fundamentales de la Agenda digital del Gobierno de España (España Digital 2025): el Plan para la Conectividad y las Infraestructuras Digitales, y la Estrategia de Impulso a la Tecnología 5G.

- **Coherencia con el Derecho de la Unión Europea**

- El Código Europeo de las Comunicaciones Electrónicas, establecido por la Directiva 2018/1972, de 11 de diciembre de 2018. exige que se adopten medidas para salvaguardar la seguridad de las redes y servicios y para evitar o reducir al mínimo el impacto de los incidentes de seguridad.

- 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 (Reglamento general de protección de datos), y la Directiva 2002/58/CE del Parlamento europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), también se relacionan con esta norma, ya que el refuerzo de la seguridad en las redes 5G redundará en una mayor protección frente a intromisiones ilegítimas en los derechos a la intimidad y al secreto de las comunicaciones en este ámbito.

- La norma es, asimismo, coherente con la Directiva sobre la seguridad de las redes y sistemas de información (SRI), adoptada en 2016, en la que se establecieron obligaciones de seguridad para los operadores de servicios esenciales (en sectores vitales como la energía, el

transporte, la sanidad y las finanzas) y los proveedores de servicios digitales (mercados en línea, motores de búsqueda y servicios en la nube) y con su revisión de 2022 (Directiva SRI2).

- El presente proyecto aplica la Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G, en la que se proponía una acción coordinada de los Estados miembros para analizar los riesgos de seguridad de la tecnología 5G y la recopilación y aplicación de buenas prácticas que garantizasen la seguridad de estas redes. Los Estados miembros apoyaron esta Recomendación en las conclusiones acordadas por el Consejo de la Unión Europea de 3 de diciembre de 2019.

- Como consecuencia de la Recomendación a la que se refiere el apartado anterior, el día 29 de enero de 2020, se publicó la "Caja de herramientas" o "Toolbox" europeo. Ese mismo día, la Comisión europea emitió la Comunicación "Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE" en la que se señala que las conclusiones y acciones recomendadas en el "toolbox" han de ser "medidas clave" que deben implementar los Estados miembros y la Comisión europea para garantizar la seguridad de estas redes en Europa.

- La norma es, asimismo, coherente con el Reglamento UE 2019/881, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la ciberseguridad, en el que se regula el procedimiento conforme al que podrán adaptarse los esquemas europeos de certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

- La norma, por último, se relaciona con la propuesta de Reglamento de Ciberresiliencia, con la que se pretende establecer unos requisitos de ciberseguridad obligatorios para los productos consistentes en equipos informáticos (hardware) y en programas informáticos (software) con elementos digitales conectados.

- **Normas que se modifican o derogan**

No se modifica ni deroga ninguna norma.

- **Entrada en vigor**

Según su disposición final cuarta el real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Conforme a lo establecido en el artículo 23 de la ley 50/1997, de 27 de noviembre, del Gobierno, ello se justifica en la necesidad de fijar cuanto antes las reglas aplicables a los

despliegues 5G que ya están realizando los operadores, evitando posibles incidentes de seguridad.

Además, ha de tenerse en cuenta que el apartado segundo de la Disposición final tercera del Real Decreto-ley 7/2022, de 29 de marzo, establecía un plazo de seis meses a contar desde su entrada en vigor, para la aprobación del ENS5G, que ya ha sido superado.

3. Descripción de la tramitación

- **Participación pública**

De acuerdo con lo establecido en el artículo 26.2 de la Ley 50/1997, de 27 de noviembre, del Gobierno y en el artículo 133.1 de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en aras a conocer la opinión de operadores, ciudadanos y cualquier interesado sobre la elaboración de una nueva norma sobre el Esquema Nacional de Seguridad de Redes y Servicios 5G entre los días 30 de mayo y 22 de junio de 2022 se ha llevado a cabo consulta pública previa, a través de la sede electrónica del Ministerio de Asuntos Económicos y Transformación Digital.

En la citada consulta se han recibido 15 aportaciones, que han sido tenidas en cuenta a la hora de elaborar la propuesta de norma.

En concreto se han recibido 14 aportaciones de entidades y 1 de un particular:

- AMETIC (20/06/22)
- ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN, UNE (20/06/22)
- CÁMARA DE COMERCIO DE ESPAÑA (20/06/22)
- CEOE (20/06/22)
- DIGITALES (20/06/22)
- ERICSSON (20/06/22)
- HUAWEI TECHNOLOGIES ESPAÑA, S.L. (20/06/22)
- MASMOVIL IBERCOM, S.A.U. (20/06/22)
- NOKIA ESPAÑA (20/06/22)
- ORANGE ESPAGNE, S.A.U. (20/06/22) (CONFIDENCIAL)
- SAMSUNG ELECTRONICS IBERIA, S.A.U. (19/06/22)
- TELEFÓNICA ESPAÑA (20/06/22) (CONFIDENCIAL)
- VODAFONE ESPAÑA, S.A.U. Y VODAFONE ONO, S.A.U. (20/06/22)
- ZTE ESPAÑA, S.L.U. (20/06/22)

- MIGUEL BAÑÓN (16/06/22)

Asimismo, deberá llevarse a cabo el trámite de audiencia pública, conforme a lo señalado en los artículos 26.6 de la Ley 50/1997, de 27 de noviembre y 133.2 de la Ley 39/2015, de 1 de octubre.

- **Informes que deben ser recabados**

-

- Informe de la CNMC

- Procedimiento de información en materia de normas y reglamentaciones técnicas y de reglamentos relativos a los servicios de la sociedad de la información previsto en la Directiva (UE) 2015/1535

- Informe de la Secretaría General Técnica del Ministerio de Trasformación Digital

- Informe del Consejo de Seguridad Nacional

- Dictamen del Consejo de Estado.

C. ADECUACIÓN AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS

La norma se adecua al orden constitucional de distribución de competencias, dictándose en virtud de las competencias exclusivas en materia de telecomunicaciones y seguridad pública atribuidas al Estado por los artículos 149.1.21ª y 149.1.29ª de la Constitución Española (CE).

En relación con las competencias exclusivas del Estado en materia de telecomunicaciones y de régimen general de comunicaciones del **artículo 149.1.21ª** CE, la primera de ellas se conecta con los aspectos técnicos de la emisión relativos al uso de las ondas radioeléctricas o electromagnéticas (dominio público radioeléctrico), lo que justifica proceder a una «ordenación conjunta de todas las variantes de telecomunicación y radiocomunicación» [STC 78/2017, de 22 de junio, FJ 4 a), citando la STC 168/1993, de 27 de mayo, FJ 4]. Por su parte la competencia exclusiva estatal respecto del «régimen general de comunicaciones» «comprende, desde luego, la totalidad de las competencias normativas sobre la misma (SSTC 84/1982, FJ 4, y 38/1983, FJ 3); pero implica también un plus», ya que «puede comportar la atribución de las competencias de ejecución necesarias para configurar un sistema materialmente unitario» (STC 195/1996, de 28 de noviembre, FJ 6)". Por tanto dentro de la competencia del artículo 149.1.21 de la CE se encuadra la regulación de los servicios de comunicaciones electrónicas prestados mediante cualquier tecnología y, por tanto, también la

garantía de la disponibilidad y "seguridad" de las redes o servicios, término definido en el Código Europeo de las Comunicaciones Electrónicas, como "la capacidad de las redes y servicios de comunicaciones electrónicas de resistir, con un determinado nivel de confianza, cualquier acción que comprometa la disponibilidad, autenticidad, integridad y confidencialidad de dichas redes y servicios, de los datos almacenados, procesados o transmitidos y la seguridad de los servicios conexos que dichas redes y servicios de comunicaciones electrónicas ofrecen o hacen accesibles".

Como recuerda la STC 8/2016, de 21 de enero, FJ 3: «Desde una última perspectiva, más global, se integra también en la materia de telecomunicaciones y de régimen general de comunicaciones (y corresponde por tanto al Estado la competencia exclusiva conforme al 149.1.21 CE) la conformación, regulación o configuración del propio sector de telecomunicaciones (comunicaciones electrónicas) atendiendo a la convergencia tecnológica (y de servicios) y al marco regulador de las comunicaciones electrónicas de la Unión Europea para asegurar una regulación homogénea en todo el territorio español. Esta homogeneidad resulta necesaria, no solo para el desarrollo e innovación del sector, sino también para la garantía de los derechos de los ciudadanos en el marco de la sociedad de la información (o sociedad del conocimiento), si se tiene en cuenta que el desarrollo de las comunicaciones y de las nuevas tecnologías de la información constituye un factor esencial para lograr la cohesión social, económica y territorial necesarias para evitar, o al menos disminuir, la llamada fractura digital»

En relación con el título competencial sobre seguridad pública del **artículo 149.1.23ª** nos remitimos a lo establecido al respecto en los FJ de la Sentencia 142/2018 de 20 de diciembre, que se acaban de transcribir, así como a lo mencionado en apartados anteriores en relación con el previsible empleo generalizado de estas redes en funciones esenciales para la economía y la sociedad, teniendo en cuenta que la dependencia de proveedores externos, obliga a que en un momento como el actual de graves tensiones geopolíticas, la ciberseguridad de las redes 5G se convierta en un objetivo prioritario de seguridad nacional, dentro de la que se encuadra la seguridad púbica.

Así lo señala la sentencia del Tribunal Constitucional 84/2016, de 3 de noviembre de 2016, al señalar que "puede afirmarse que existe una coincidencia sustancial entre el sentido y finalidad de los títulos competenciales de las materias 4 y 29 del art. 149.1. CE y el concepto de seguridad nacional, definido en el art. 3 de la Ley 36/2015, como: «la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos».

Por último, debe señalarse que Las Comunidades Autónomas y Entidades locales han tenido ocasión de pronunciarse sobre el proyecto de norma en el trámite de consulta pública efectuado entre los días 30 de mayo y 20 de junio de 2022 sin que ninguna de ellas haya

presentado aportaciones. Asimismo, podrán participar en el correspondiente trámite de audiencia pública.

D. IMPACTO ECONÓMICO Y PRESUPUESTARIO.

1. Impacto económico general.

El sector de las comunicaciones electrónicas se caracteriza por un elevado grado de dinamismo e innovación, que por lo general ha estado ligado a la inversión en el despliegue de nuevas redes.

En la actualidad existe la oportunidad de continuar con esta dinámica innovadora, mediante la inversión redes 5G, pero ello solo será posible si se introducen las medidas adecuadas que garanticen la integridad, continuidad y seguridad de estas redes, evitando los riesgos que su implantación generalizada podría llegar a provocar.

Pero es que además, las telecomunicaciones, por su carácter transversal, no solo garantizan la prestación de servicios cada día más necesarios como el teletrabajo, la telemedicina o la enseñanza online, sino que al tiempo favorecen el crecimiento de otros sectores como la industria de los contenidos, el Big Data, el Internet de las Cosas o la automoción conectada, permitiendo, asimismo, la gestión inteligente del transporte y de los recursos energéticos y la reducción de la brecha digital entre los distintos territorios.

En este sentido, las nuevas redes 5G, se sitúan como una pieza clave para acelerar la transformación digital de la sociedad y la economía.

En nuestro entorno más inmediato, los análisis de la Comisión Europea prevén que los beneficios estimados al introducir 5G en cuatro sectores productivos (automoción, salud, transporte y utilities) aumentarían progresivamente hasta alcanzar en 2025 los 62.500 millones de euros de impacto directo anual dentro de la Unión Europea, que se elevarían a 113.000 millones de euros sumando los impactos indirectos. El mismo estudio estima que en nuestro país se obtendrían unos beneficios indirectos en los cuatro sectores analizados de 14.600 millones de euros y una importante creación de empleos.

En conclusión, debe señalarse que, en el actual momento de incertidumbre internacional, las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir, por su carácter transversal, al crecimiento, la productividad y al empleo y, por tanto, al desarrollo económico y al bienestar social

Asimismo, se prevé que las medidas de seguridad propuestas en el proyecto tengan un impacto neutro en los precios, ya que los operadores y prestadores de servicios ya están

realizando fuertes inversiones para ofrecer conectividad a través de 5G, siendo la seguridad un aspecto marginal de esos costes.

En todo caso, el esfuerzo económico dedicado a medidas de seguridad debe considerarse como una inversión, puesto que reduce los gastos en reposición del servicio y en posibles indemnizaciones, aumentando asimismo los ingresos por la entrada de nuevos clientes que confían en la nueva tecnología.

Por su impacto transversal, la introducción de la tecnología 5G está llamada a crear un importante efecto positivo en el empleo de numerosos sectores.

Pero además, el cumplimiento de las concretas medidas de seguridad previstas en esta norma tendrá también un efecto positivo para la creación de empleo en sectores como la I+D+I, la certificación o la auditoria, señalándose como objetivo concreto de la norma el de fortalecer la industria y fomentar la I+D+i nacionales en ciberseguridad.

El efecto de la norma sobre los consumidores se prevé también positivo, ya que a la mayor posibilidad de elección entre tecnologías que deriva de la propia introducción del 5G, se suman los beneficios intangibles asociados a una mayor seguridad y confianza en el uso de la nueva tecnología.

2. Efectos en la competencia y en la unidad de mercado.

La norma tiene efectos positivos en cuanto las disposiciones relacionadas con la diversificación de proveedores en la cadena de suministro y las medidas destinadas a fortalecer la industria y fomentar la I+D+I nacionales en ciberseguridad pueden contribuir a la aparición y crecimiento de nuevos actores.

Por otro lado, las limitaciones a la libre competencia derivadas de la restricción de la participación de suministradores de alto riesgo o riesgo medio salvaguardan la seguridad nacional, al garantizar la continuidad de servicios y aplicaciones esenciales que descansan sobre estas redes (salud, protección civil, educación, etc) y son, únicamente, aquellas imprescindibles, a la vista de un riguroso análisis de riesgo y de las decisiones tomadas por otros Estados miembros o por la propia UE.

Por tanto, dado que se prevé que la norma tenga tanto efectos positivos como negativos para la competencia, se espera que ambos se contrarresten, creando una nueva situación competitiva en la que nuevos suministradores contribuyan a la autonomía tecnológica de la Unión europea, evitando los riesgos derivados de ciberataques.

3. Impacto presupuestario.

- **Desde el punto de vista de los ingresos:**

El proyecto no implicará la generación o percepción de ingresos para la Hacienda estatal ni para la Hacienda de otras Administraciones Públicas.

- **Desde el punto de vista del gasto:**

El proyecto no implicará la realización de gastos con cargo a los Presupuestos Generales del Estado ni supondrá la asunción de costes o gastos para la Hacienda estatal ni para la Hacienda de otras Administraciones Públicas.

Las tareas de coordinación, inspección y sanción encomendadas al Ministerio de Transformación Digital serán realizadas con los medios y recursos ya atribuidos a este Ministerio.

E. DETECCIÓN Y MEDICIÓN DE CARGAS ADMINISTRATIVAS.

No se imponen cargas nuevas, ya que las cargas administrativas para operadores, suministradores y usuarios corporativos, ya estaban previstas en el 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, que ahora se desarrolla, por lo que debemos remitimos a la medición de cargas, contenida en la MAIN de dicha norma.

F. IMPACTO POR RAZÓN DE GÉNERO

El proyecto tiene un impacto de género nulo, en la medida en que su contenido no incluye ningún tipo de medida que pueda atentar contra la igualdad de oportunidades entre hombres y mujeres.

G. IMPACTO EN LA LUCHA CONTRA LA DESPOBLACIÓN Y EL CAMBIO CLIMÁTICO

La seguridad de la tecnología 5G se configura como una pieza clave para la vertebración territorial del país, ya que el acceso seguro a las nuevas redes y a los nuevos contenidos y servicios digitales que podrán prestarse a través de las mismas, son un elemento imprescindible para la incorporación de la ciudadanía y de las empresas a la Sociedad de la Información y del Conocimiento, fomentando con ello la cohesión social y el desarrollo económico y contribuyendo al desarrollo de la nueva Administración Electrónica.

En este sentido las medidas que introduce la norma se convierten en importantes pilares para conseguir la eliminación de la brecha digital y la vertebración de los distintos territorios, de modo que el acceso a nuevos servicios y aplicaciones como los de telemedicina, aprendizaje

online o teletrabajo quede garantizado en cualquier parte del territorio español, favoreciendo el asentamiento y la fijación de población en el medio rural.

A ello se une la importancia de las telecomunicaciones como factor clave para la lucha contra el cambio climático. En este contexto, se enmarca el objetivo establecido por la Unión Europea de reducir en un 40% las emisiones de gases de efecto invernadero para el año 2030, con relación a los niveles de 1990.

El sector de las Tecnologías de la Información y Comunicación es un sector que genera un bajo nivel de emisiones relativo, y a la vez su papel puede ser fundamental en la lucha frente al cambio climático al facilitar un uso más eficiente de los recursos energéticos por otros sectores.

En este sentido deben resaltarse los ahorros energéticos de las propias redes, gracias a la mayor eficiencia energética de las tecnologías 5G, así como el papel transformador que el sector TIC en su conjunto, ha jugado en la innovación y rediseño de los modelos de negocio de todos los sectores en la denominada era digital, lo que le convierte en el catalizador que necesitan otros sectores para contribuir a la nueva economía de bajas emisiones de gases de efecto invernadero, ya que facilita usos innovadores de productos y servicios "inteligentes", ayudando a generar beneficios medioambientales y permitiendo ahorros de costes de energía a los usuarios.

Además, las telecomunicaciones son muy útiles en la tarea de supervisión ambiental y climática, incluido el pronóstico del tiempo, y fundamentales para las comunicaciones de alerta temprana y mitigación en caso de catástrofes.

Las conclusiones del estudio "Telecomunicaciones y CO2: El Papel de la Tecnología Móvil frente al Cambio Climático", indican que aplicando 13 iniciativas de la tecnología móvil se pueden reducir en 113 millones de toneladas las emisiones de CO2 (lo que equivale a las emisiones generadas por unos 50 millones de vehículos) y generar unos ahorros de energía de 43.000 millones de euros en Europa.

Para ello, se necesitarían 1.040 millones de nuevas conexiones móviles, de las cuales el 87% corresponderían a conexiones "máquina a máquina" (M2M).

Su aplicación en España implicaría una reducción de 10,6 millones de toneladas de emisiones de CO2 (lo que equivale a las emisiones generadas por 4,7 millones de vehículos, que es el 15% del parque actual), y unos ahorros de energía de 4.042 millones de euros. En el caso español, se precisarían unos 98 millones de nuevas conexiones, de las cuales unos 85 millones serían conexiones M2M.

El ahorro energético se producirá principalmente tanto por ese mayor protagonismo de servicios inteligentes M2M (redes eléctricas inteligentes, logística inteligente, ciudades inteligentes y sistemas de producción inteligente) como por la sustitución de actividades físicas por otras virtuales.

Ese proceso de virtualización supondría la sustitución de procesos, desplazamientos, reuniones y viajes por alternativas virtuales de bajas emisiones. Se trataría, por ejemplo, de reducir los viajes apostando por salas de reuniones virtuales a las que conectarse a través de las telecomunicaciones, fomentar el uso de productos de telecomunicaciones para que los empleados puedan trabajar a distancia desde su casa o utilizar las comunicaciones móviles para mejorar los procesos de comercio electrónico y facilitar los sistemas de pedido y entrega de compras. Estas iniciativas no solo permitirían adaptarnos a posibles medidas de contención sanitaria por posibles epidemias, sino que al tiempo lograrían reducir las emisiones de CO2 en Europa en más de 22 millones de toneladas, así como un ahorro potencial en consumo energético de 14.100 millones de euros (en España: ahorros de 2 millones de toneladas de emisiones de CO2, y 1.330 millones de euros).

H. OTROS IMPACTOS

El proyecto de norma no tiene impacto en relación con la igualdad de oportunidades, la no discriminación y la accesibilidad universal de las personas con discapacidad.

No se aprecian tampoco impactos significativos del proyecto de norma en relación con la infancia la adolescencia y la familia**.**