EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Número de notificación : 2023/0761/ES (Spain)

REAL DECRETO POR EL QUE SE APRUEBA EL ESQUEMA NACIONAL DE SEGURIDAD DE REDES Y SERVICIOS 5G

Fecha de recepción : 29/12/2023
Final del periodo de statu quo : 02/04/2024 (closed)

Message

Mensaje 001

Comunicación de la Comisión - TRIS/(2023) 3739

Directiva (UE) 2015/1535

Notificación: 2023/0761/ES

Notificación de un proyecto de texto de un Estado miembro

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta' dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20233739.ES

1. MSG 001 IND 2023 0761 ES ES 29-12-2023 ES NOTIF

2. Spain

3A. Subdirección de Asuntos Industriales, Energéticos, de Transportes, Comunicaciones y de Medioambiente
D.G. de Mercado Interior y otras Políticas Comunitarias
Ministerio de Asuntos Exteriores, UE y Cooperación

3B. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual.
Subdirección General de Ordenación de las Telecomunicaciones.
Ministerio de Transformación Digital

4. 2023/0761/ES - V00T - Telecomunicaciones

5. REAL DECRETO POR EL QUE SE APRUEBA EL ESQUEMA NACIONAL DE SEGURIDAD DE REDES Y SERVICIOS 5G

6. Redes y servicios de comunicaciones electrónicas 5G

Equipos de telecomunicaciones.

7.

8. 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.

9. 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.

10. Referencias de los textos de base:

11. No

12.

13. No

14. No

15. Sí

16.
Aspecto TBT: No

Aspecto SPS: No

****
Comisión Europea
Punto de contacto Directiva (UE) 2015/1535
email: grow-dir2015-1535-central@ec.europa.eu