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

(IPN/CNMC/036/23 Esquema Nacional Seguridad 5G)

CONSEJO. PLENO

Presidenta
Dª. Cani Fernández Vicién

Consejeros
D. Bernardo Lorenzo Almendros
D. Xabier Ormaetxea Garai
Dª. Pilar Sánchez Núñez
D. Carlos Aguilar Paredes
D. Josep Maria Salas Prat
Dª. María Jesús Martín Martínez

Secretario
D. Miguel Bordiu García-Ovies

En Madrid, a 13 de febrero de 2024

De acuerdo con la función establecida en el artículo 5.2 de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, el Pleno emite el siguiente informe:

TABLA DE CONTENIDO

I. OBJETO DEL INFORME

1. El 21 de diciembre de 2023, tuvo entrada en el Registro de la Comisión Nacional de los Mercados y la Competencia (CNMC) un escrito de la Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual del Ministerio para la Transformación Digital y de la Función Pública (MTDFP) por el que solicitaba la emisión de informe sobre el proyecto de Real Decreto por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G (ENS5G).

2. Se acompaña al proyecto de Real Decreto la correspondiente Memoria del Análisis de Impacto Normativo (MAIN).

3. El presente informe tiene por objeto analizar el Proyecto de Real Decreto y manifestar el parecer de la CNMC sobre el mismo.

II. HABILITACIÓN COMPETENCIAL

4. El artículo 5.2.a) de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia (LCNMC), establece que la CNMC participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en los sectores sometidos a su supervisión.

5. El artículo 100.2.x) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones (LGTel), establece que, entre otras funciones, la CNMC será consultada por el Gobierno y el MTDFP en materia de comunicaciones electrónicas, particularmente en aquellas materias que puedan afectar al desarrollo libre y competitivo del mercado. En el ejercicio de esta función, la CNMC participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en materia de comunicaciones electrónicas.

6. En aplicación de los anteriores preceptos, la CNMC es el organismo competente para elaborar el presente informe.

III. ANTECEDENTES

7. La Recomendación de la Comisión (UE) 2019/534, de 26 de marzo de 2019, de Ciberseguridad de las redes 5G, identificó una serie de acciones coordinadas a tomar por los Estados Miembros para evaluar los riesgos de seguridad de las redes 5G y reforzar las medidas para reducirlos. Como resultado, en enero de 2020, el Grupo de Cooperación para la Seguridad de las Redes y Sistemas de

Información (SRI)[1] publicó la caja de herramientas de la UE para la seguridad de las redes 5G, que incluye un conjunto de medidas destinadas a mitigar los riesgos de seguridad observados en los análisis de vulnerabilidades de las redes 5G por parte de los países europeos[2].

8. El Real decreto-ley 7/2022, de 29 de marzo de 2022, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (RDL5G), trasladó a la normativa nacional las medidas recomendadas en la caja de herramientas de la UE[3]. Es de aplicación a los operadores y suministradores 5G y a los usuarios corporativos que tengan derecho 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. Entre las obligaciones que pueden imponerse a los operadores destaca la posibilidad de restringir o prohibir el uso de equipos y recursos de suministradores que hayan sido calificados de alto riesgo.

9. El RDL5G ha sido modificado[4] en lo que se refiere a las obligaciones de los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G (artículo 12), concretamente:

- Se mantiene para la red de acceso la obligación de los operadores de diseñar una estrategia de diversificación con al menos dos suministradores diferentes para cada elemento crítico de la red, pero se flexibiliza para el núcleo de la red, los sistemas de control y gestión y los servicios de apoyo, donde el suministrador podrá ser único (apartado 3.a).

- Se incluye una nueva obligación de solicitud de autorización previa al MTDFP para la instalación, modificación o adaptación de las estaciones radioeléctricas de la red de acceso 5G considerada crítica, es decir, donde 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 servicios

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

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

[3] El RDL5G fue informado por CNMC el 24 de noviembre de 2021 (IPN/CNMC/029/21).

[4] Mediante la disposición final quinta del Real del Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

esenciales para la comunidad o sectores estratégicos, sean determinados por el Consejo de Seguridad Nacional (apartado 3.d).

- Se exceptúa a determinados elementos, funciones y sistemas del núcleo de red o de los sistemas de control y gestión y los servicios de apoyo de la obligación de estar ubicados en territorio nacional (apartado 3.e).

- Se habilita al MTDFP para modificar la estrategia de diversificación en la cadena de suministro de un operador 5G (apartado 6).

10. El proyecto de Real Decreto ha sido objeto de un trámite de audiencia e información pública, cuyo plazo para presentar aportaciones finalizó el 15 de enero de 2024. Asimismo, con carácter previo a su elaboración, tuvo lugar un trámite de consulta pública, entre el 30 de mayo y 22 de junio de 2022.

IV. DESCRIPCIÓN DEL PROYECTO DE REAL DECRETO

11. El proyecto de Real Decreto tiene por objeto el desarrollo reglamentario a través del ENS5G de los requisitos establecidos en el RDL5G. Consta de una parte expositiva, un artículo único por el que se aprueba el ENS5G, dos disposiciones adicionales y cuatro disposiciones finales.

12. En la exposición de motivos se recogen los motivos que impulsan la aprobación del ENS5G y los artículos del RDL5G que se desarrollan. En concreto, los artículos 5.3, 20 y 21, que especifican que el ENS5G:

- Debe llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G, considerando las aportaciones de cada agente de la cadena de valor de 5G, así como la normativa, las recomendaciones y los estándares técnicos de la Unión Internacional de Telecomunicaciones (UIT) y de otras organizaciones internacionales.

- Efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G e identificará, concretará y desarrollará medidas a nivel nacional para mitigar y gestionar los riesgos analizados.

- Será aprobado por el Gobierno, mediante real decreto, a propuesta del MTDFP, previo informe del Consejo de Seguridad Nacional, y será revisado al menos cada cuatro años o cuando las circunstancias lo aconsejen.

13. El artículo único aprueba el ENS5G. Las disposiciones adicionales y finales regulan entre otros su revisión cuando las circunstancias lo aconsejen y, en todo caso, cada cuatro años, la aplicación supletoria de la normativa sobre seguridad

e integridad de las redes de comunicaciones electrónicas[5], la habilitación para el desarrollo del ENS5G y modificación de sus anexos y su entrada en vigor al día siguiente de su publicación en el Boletín Oficial del Estado (BOE).

14. El ENS5G consta de 33 artículos divididos en 8 capítulos y de 3 anexos.

15. Capítulo I: Disposiciones generales (artículos 1 a 8)

Comprende los objetivos del ENS5G, las definiciones y los sujetos a los que aplica. Señala el conjunto mínimo de elementos, infraestructuras y recursos que integran una red 5G (descritos detalladamente en el anexo I) y establece cuáles son los elementos críticos de una red 5G que deben situarse como norma general en territorio nacional. Establece que los sujetos obligados deberán llevar a cabo un tratamiento integral de la seguridad, para lo cual deberán realizar un análisis de los riesgos que les afecten y una gestión adecuada de dichos riesgos mediante la aplicación de técnicas y medidas adecuadas para lograr su mitigación o eliminación. Asimismo, se indica que el ENS5G ha tenido y deberá tener en cuenta estas aportaciones, así como las recomendaciones y estándares técnicos de la UE, UIT y otras organizaciones internacionales. Por último, se señala que el análisis y la gestión de los riesgos deben vigilarse y reevaluarse periódicamente, por ser parte esencial del proceso de seguridad.

16. Capítulo II: Análisis y gestión de riesgos a nivel nacional (artículos 9 y 10)

Incluye el análisis de riesgos a nivel nacional en su Anexo II, realizado en base a la información aportada por los sujetos obligados, el examen de las vulnerabilidades de la cadena de suministro de las redes y servicios 5G, la evaluación del grado de dependencia de los suministradores y el riesgo de interrupción del suministro. Asimismo, se incluye la evaluación de la eficacia de las medidas de seguridad aplicadas, de acuerdo con el artículo 22 del RDL5G.

Respecto a la gestión de riesgos a nivel nacional, se señala que los criterios, requisitos, condiciones y plazos para que los sujetos obligados puedan diseñar e implantar medidas de mitigación de riesgos son los señalados en el Anexo III, donde se incluyen las medidas de seguridad necesarias para mitigar y gestionar los riesgos a nivel nacional del Anexo II.

[5] De acuerdo con lo dispuesto en la LGTel, 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 sus respectivas normativas de desarrollo.

17. Capítulo III: Medidas específicas para garantizar la seguridad de las redes y servicios 5G (artículos 11 a 13)

Incluye el desarrollo del artículo 14 del RDL5G relativo la declaración de suministradores de alto riesgo y los criterios aplicables para determinar el plazo de sustitución en la red de los elementos proporcionados por dichos suministradores.

Incorpora la previsión de que se pueden determinar las ubicaciones, áreas y centros en las que no se podrán instalar equipos radio de suministradores calificados de alto riesgo. Asimismo, añade la modificación del artículo 12.3.d) del RDL5G respecto a que los operadores 5G deberán solicitar autorización previa para la instalación, modificación o adaptación de las estaciones radio que proporcionen cobertura a estas ubicaciones, áreas y centros.

Por último, se incluye la obligación de los operadores 5G de diseñar una estrategia de diversificación en la cadena de suministro, debiendo contar a nivel de la red de acceso con dos suministradores diferentes. Se detalla el procedimiento a seguir en caso de operaciones de concentración empresarial que redujeran dicho número y se señalan los supuestos y el procedimiento por el que el MTDFP puede modificar la estrategia de diversificación en la cadena de suministro de un operador 5G.

18. Capítulo IV: Análisis de riesgos por los sujetos obligados (artículos 14 a 17)

Este capítulo incluye las obligaciones de análisis de riesgos que aplican específicamente a cada sujeto, según lo estipulado en el RDL5G. El ENS5G incorpora explícitamente que los operadores 5G deberán presentar al MTDFP un nuevo análisis de riesgos antes del 1 de octubre de 2024**,** y a continuación, cada dos años[6]. Los suministradores 5G deberán aportar dicho análisis cuando así se requiera y, en el caso de haber sido calificados como de alto riesgo o riesgo medio, en el plazo de seis meses y posteriormente cada dos años. Los usuarios corporativos 5G solo deberán presentar este análisis cuando sean requeridos para ello.

19. Capítulo V: Gestión de riesgos por los sujetos obligados (artículos 18 a 24)

Este capítulo incluye las obligaciones de gestión de riesgos que aplican específicamente a cada sujeto, según lo estipulado en el RDL5G. El ENS5G

[6] Los operadores 5G debían remitir por primera vez sus análisis de riesgos y un informe de las medidas técnicas y organizativas para mitigarlos en un plazo de seis meses desde la entrada en vigor del RDL5G, es decir, el 30 de septiembre de 2022, de acuerdo con la disposición adicional primera de dicha norma.

incorpora además la obligación para los operadores y suministradores 5G de aplicar el esquema de certificación GSMA Network Equipment Security Assurance Scheme (NESAS) y la norma técnica ISO/IEC 27001: Gestión de Seguridad de la Información.

También deberán presentar al MTDFP con una periodicidad anual una auditoría sobre la aplicación de ambas obligaciones. Se establecen las mismas fechas que en el capítulo anterior para que los sujetos obligados remitan la descripción de las medidas aplicadas para gestionar y mitigar los riesgos. El ENS5G extiende la restricción que el RDL5G aplicaba a las AAPP, que impide el uso de suministradores de riesgo medio a los elementos críticos de red de los usuarios corporativos 5G.

20. Capítulo VI: Otras medidas en materia de seguridad (artículos 25 a 29)

Señala el deber de todos los sujetos obligados, así como AAPP, fabricantes, importadores, distribuidores y comercializadores de equipos terminales y dispositivos, de colaborar y remitir información.

Se establece que mediante orden ministerial se podrá supeditar el uso de un equipo, sistema, programa o servicio a la obtención previa de una certificación, en virtud del Reglamento de ciberseguridad o de los esquemas de certificación y normas de certificación de equipos y productos 5G que sean aprobados.

Los equipos terminales y dispositivos que se conecten a las redes 5G deberán cumplir los requisitos de seguridad para productos digitales y los requisitos esenciales que sean de aplicación, conforme a la normativa europea.

También se señala la cooperación internacional a desarrollar por el MTDFP, en especial en el ámbito de la UE.

21. Capítulo VII: Aplicación del ENS5G (artículos 30 y 31)

Este capítulo se refiere a la competencia del MTDFP para aplicar el ENS5G y el desglose de facultades que puede ejercer para ello.

22. Capítulo VIII: Inspección y régimen sancionador (artículos 32 y 33)

Se atribuye al MTDFP todas las potestades de la función inspectora y se remite a lo dispuesto en el RDL5G respecto al régimen sancionador.

23. Por último, se incluyen tres anexos. El Anexo I describe los elementos, infraestructuras y recursos de una red 5G; el Anexo II contiene el análisis de riesgos a nivel nacional; y el Anexo III recoge la gestión de riesgos a nivel nacional.

V. VALORACION DEL PROYECTO DE REAL DECRETO

24. Se analiza a continuación el proyecto de Real Decreto que aprueba el ENS5G, cuyo contenido debe desarrollar lo estipulado en el artículo 20 del RDL5G. En especial destaca que el ENS5G incorpora:

- En su anexo II, el análisis de riesgos a nivel nacional, elaborado en base a las recomendaciones y estándares técnicos en la materia y la información proporcionada por los sujetos del ámbito de aplicación del RDL5G.
- En su Anexo III, la concreción de las medidas de seguridad necesarias para solventar, disminuir o paliar los riesgos identificados a nivel nacional.

25. Este esquema incorpora un mayor detalle con respecto al RDL5G de los activos que integran las redes 5G y su criticidad. Cumple con el objetivo de especificar la metodología seguida para identificar las amenazas que afectan a las redes y servicios 5G, evaluar la criticidad de los activos y el nivel de riesgo de las amenazas en función de su probabilidad de ocurrencia e impacto en la red y, en base a este análisis, proponer una categorización de medidas de seguridad para solventar o mitigar los riesgos. Sin embargo, se aprecia una falta de concreción en la determinación del resultado del análisis de los niveles de riesgo y otros aspectos exigidos según el artículo 22.2 (letras b, c y d) y 22.3 del RDL5, así como en el desarrollo de los criterios, condiciones y plazos de aplicación de las medidas de seguridad establecidas a nivel nacional, que debe cumplir cada sujeto obligado, que son objeto de comentarios en este informe.

Primero. Observaciones preliminares

26. El RDL5G reflejó en su redacción final muchas de las observaciones incluidas en el Informe CNMC IPN/CNMC/029/21. Sin embargo, conviene reiterar en el presente informe los comentarios relacionados con la afectación a la competencia de algunas de las medidas del RDL5G[7], cuyo desarrollo es incorporado en el ENS5G. Concretamente, el ENS5G (i) fija los criterios a valorar para determinar la calificación de suministrador 5G de alto riesgo y el procedimiento para fijar el plazo de sustitución de los equipos de dicho suministrador en la red 5G del operador, (ii) condiciona la instalación de equipos radio en ubicaciones críticas a la obtención de una autorización previa, y (iii) incorpora la posibilidad de modificar las estrategias de diversificación de las cadenas de suministro de los operadores 5G.

[7] Consideraciones vertidas en las secciones IV.1, IV.8 y IV.10 del IPN/CNMC/029/21.

27. Estas medidas pueden alterar las condiciones de competencia en el mercado de suministradores y tener consecuencias en la capacidad competitiva de los operadores afectados por las medidas. Por ello, se recomienda incluir la afectación a la competencia como uno de los criterios a sopesar en la valoración de estas medidas de mitigación de riesgos de seguridad.

Segundo. Comentarios generales

28. Se han detectado artículos[8] que modifican determinadas medidas del RDL5G de forma sustantiva, y cuyo carácter restrictivo podría requerir una norma con rango de ley para su establecimiento. Por ello, se señalan en las observaciones particulares del presente informe los artículos en cuestión sobre los que ENS5G podría carecer del suficiente soporte legal para su desarrollo mediante una norma de carácter reglamentario (véanse los párrafos 36 y 42).

Tercero. Comentarios particulares

A. Elementos de la red 5G

29. El artículo 5 del ENS5G recoge la lista de elementos, infraestructuras y recursos mínimos que componen una red 5G, de conformidad con el artículo 6 del RDL5G, y añade su descripción respectiva en el Anexo I, centrándose únicamente en la arquitectura de red 5G-SA. Aunque esta arquitectura ya está siendo desplegada por varios operadores nacionales (por el momento Orange y Telefónica), todavía hay operadores con arquitectura 5G-NSA, donde el núcleo de la red es 4G. Dado que ambas configuraciones se mantendrán en el tiempo[9] y ambas prestan servicios 5G, convendría aclarar cómo se debe tener en cuenta la configuración 5G-NSA en el ENS5G.

30. También debería completarse el Anexo I con la descripción de los elementos y funciones mencionados sobre los que no se aporta información. Concretamente, los elementos NSSF, UDSF, UCMF y NWDAF.

B. Criticidad de activos

31. Una de las novedades del RDL5G, que no formaba parte del texto informado por esta Comisión, fue la delimitación de una categoría de activos de la red 5G que son considerados elementos críticos. Concretamente, (i) las funciones del núcleo de red, (ii) los sistemas de control, gestión y servicios de apoyo y (iii) la red de

[8] Artículo 5.4 (segundo párrafo) y 21.2.

[9] Según el informe BoR (23) 180 “BEREC Report Secure 5G Networks”, de 5 de octubre de 2023, una amplia mayoría de operadores europeos estima que el núcleo de red 5G coexistirá con el núcleo 4G durante más de 5 años.

acceso en determinadas zonas geográficas y ubicaciones. Esta delimitación tiene importancia porque los operadores no podrán utilizar en dichos elementos críticos los equipos y recursos de los suministradores calificados de alto riesgo.

32. Por su parte, el análisis de riesgos a nivel nacional del Anexo II determina el nivel de criticidad de los activos con respecto al grado de afectación particular de cada elemento ante amenazas. En este análisis se observa que uno de los elementos de la red con mayor nivel de criticidad es la infraestructura de virtualización (compuesta por hardware y software de virtualización) y está valorada con un nivel de criticidad alto en los tres parámetros de seguridad CIA (Confidencialidad, Integridad y Disponibilidad).

33. A pesar del alto nivel de criticidad de la infraestructura de virtualización observado en el Anexo II, este activo no forma parte de la lista de elementos críticos del artículo 5.3 del ENS5G (y del artículo 6.3 del RDL5G). Se desconoce el resultado del nivel de riesgo obtenido para este activo en función de la probabilidad de ocurrencia de una amenaza y su impacto en la red, dado que no se aporta en el Anexo II. Ahora bien, dada la significativa importancia de la infraestructura de virtualización en las redes 5G, al ser la tecnología subyacente que permite la virtualización de las funciones del núcleo de la red 5G[10], cabría considerar su incorporación como elemento crítico.

C. Ubicación de los elementos críticos

34. El artículo 5.4 del ENS5G incluye la vigente redacción del artículo 12.3.e del RDL5G por el que se estipula que determinados elementos, funciones y sistemas del núcleo de red o de los sistemas de control, gestión y de apoyo pueden estar ubicados fuera del territorio nacional. Aunque esta reciente modificación del artículo 12.3.e no pudo ser informada en su momento por esta Comisión, se considera positiva, ya que la imposición de medidas de ubicación nacional de los equipos supone una restricción para los operadores, que podrían llegar a reducir las eficiencias operativas y la escalabilidad de sus soluciones. Todo ello sin perjuicio de que la legislación y contexto político del país tercero donde se ubiquen dichos equipos deban permitir el ejercicio de las obligaciones del RDL5G.

35. Sin embargo, el ENS5G ha añadido un nuevo párrafo -no incluido en la modificación del RDL5G- por el que se podrá requerir la reubicación de tales

[10] Según el informe BoR (23) 180 “BEREC Report Secure 5G Networks”, de 5 de octubre de 2023, la mayoría de operadores utilizan funciones virtualizadas en sus redes, identificando como riesgos significativos el aislamiento de estas funciones virtualizadas y las amenazas al gestor de virtualización y el orquestador.

elementos en territorio nacional en el plazo que indique por resolución el MTDFP, previa audiencia del titular de la red, que no podrá ser inferior a tres meses.

36. La reubicación de equipos ya instalados es una medida de gran calado por su carácter restrictivo, que afecta al libre ejercicio empresarial del operador. Además, al tratarse de una nueva obligación (reubicación) al margen del texto del RDL5G podría considerarse un reglamento "ultra vires"[11]. Por tanto, se recomendaría su inclusión previa en el RDL5G de rango normativo superior, para que su cumplimiento pueda desarrollarse en el ENS5G.

37. Además, esta medida puede generar una gran inseguridad entre los operadores si los criterios y plazos para su aplicación no quedan suficientemente detallados y justificados de antemano. Se recomienda reducir en lo posible esta incertidumbre, delimitando los criterios y ámbito de aplicación, para evitar que suponga una traba regulatoria que llegue a impedir, de facto, la ubicación fuera del territorio nacional de todo nuevo elemento crítico de la red de núcleo 5G y sus sistemas de control, gestión y apoyo. Se propone acotar los activos específicos de la red sobre los que sería potencialmente de aplicación esta medida de seguridad, de conformidad con el análisis sobre criticidad y nivel de riesgo para cada activo del Anexo II.

38. Asimismo, se recomienda que el plazo para hacer efectiva la reubicación de los equipos sea suficientemente amplio para que pueda realizarse con las máximas garantías.

D. Sustitución de suministradores 5G de alto riesgo y riesgo medio

39. Como se señaló en el Informe CNMC IPN/CNMC/029/21, la imposición de restricciones al uso en las redes 5G de determinados suministradores considerados de alto riesgo, puede modificar las condiciones de competencia en el mercado de suministradores, reducir los incentivos a la innovación y aumentar el coste de prestación de servicios. La sustitución de equipos de estos suministradores en la red 5G es una medida altamente restrictiva, que puede distorsionar la capacidad competitiva de los operadores 5G que se vean afectados por dicha sustitución en activos especialmente críticos de su red.

40. El artículo 11.4 del ENS5G introduce una novedad con respecto al RDL5G, al desarrollar el procedimiento para determinar el plazo de sustitución de los equipos, productos y servicios proporcionados por un suministrador calificado de

[11] Según lo indicado en la Sentencia del Tribunal Supremo 760/2019 de 3 de junio de 2019 (recurso 84/2018), en relación con los principios generales del control de la potestad reglamentaria fijados en la posterior Sentencia 622/2021 de 5 de mayo de 2021 (recurso 608/2019).

alto riesgo. Así, el Consejo de Ministros podrá establecer un plazo diferente para los distintos elementos críticos de la red 5G, en función de la criticidad de cada elemento o parte de él, de su afectación al funcionamiento y operatividad de la red y de la disponibilidad de equipos en ese momento en el mercado. Además, este plazo podrá ser diferente para los distintos operadores 5G afectados, en función de la repercusión de dicha sustitución en sus redes, en los contratos de suministro de equipos suscritos y de la capacidad de suministro existente en el mercado de equipos de telecomunicación.

41. Se considera acertada la aplicación de los criterios señalados, para reducir el impacto de la medida al mínimo posible. En este sentido, se propone considerar en la aplicación de los plazos de sustitución de equipos la valoración de su impacto sobre la capacidad competitiva de los operadores afectados por la medida, para evitar beneficiar las posiciones relativas de unos operadores frente a otros en el despliegue de redes y servicios 5G.

42. En el artículo 21 aplicable a los usuarios corporativos 5G, se ha incorporado la prohibición de utilizar suministradores que hayan sido calificados de riesgo medio en los elementos críticos de red. Esta medida de carácter restrictivo estaba prevista en el RDL5G para las AAPP, por razones de seguridad nacional, pero no aplicaba a los usuarios corporativos 5G. Por tanto, el desarrollo reglamentario en el ENS5G de esta medida podría requerir su inclusión con rango de ley en el RDL5G, ya que el establecimiento de prohibiciones absolutas no formaría parte de las disposiciones que pueden desarrollarse en el ENS5G[12]. Asimismo, el nivel de riesgo asociado a la red y servicios 5G desplegados en autoprestación puede variar en función del tipo de usuario corporativo 5G, por lo que se recomienda mitigar el impacto de esta medida a aquellos usuarios corporativos que sean considerados críticos o presten servicios esenciales.

E. Autorización previa para la instalación de estaciones radio en ubicaciones críticas

43. Esta medida, que no pudo ser informada por la CNMC, condiciona el despliegue de cobertura 5G en las ubicaciones que determine el Consejo de Seguridad Nacional, imponiendo una restricción que puede dilatar el despliegue de servicios 5G en dichas áreas, al requerir de una autorización administrativa previa por parte de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID). Es una medida de gran calado, que limita la libertad de despliegue de los operadores y puede condicionar el uso de

[12] El artículo 23 del RDL5G declara que en el ENS5G "*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*".

determinados suministradores de red 5G, sin que el Consejo de Ministros los haya calificado de alto riesgo.

44. Se considera que los criterios para que la SETID autorice la instalación, modificación o adaptación de dichas estaciones radio no están suficientemente precisados y, por tanto, pueden implicar un alto grado de discrecionalidad en su aplicación, lo que puede generar incertidumbre en los operadores y suministradores, e incluso dificultar operaciones habituales de aumento de capacidad de las estaciones 5G, tanto para los nuevos despliegues como para las estaciones ya existentes, dado que la autorización se aplica igualmente a la "modificación o adaptación" de estaciones.

45. Cabría de todos modos precisar el procedimiento aplicable en las estaciones existentes, que no sean objeto de modificación o adaptación, pero que esté justificado examinar a la vista de esta nueva obligación, al dar cobertura igualmente a ubicaciones críticas.

F. Modificación de la estrategia de diversificación de suministradores

46. El ENS5G incorpora en su texto la nueva potestad del Ministerio para modificar la estrategia de diversificación de la cadena de suministro de un operador 5G, si considera que no queda garantizada la continuidad en la prestación de los servicios 5G, la integridad física o lógica de la red 5G, se pone en peligro la funcionalidad y operatividad de la red 5G o se debe garantizar la seguridad en la provisión de servicios para Seguridad Nacional, Defensa Nacional u otras Administraciones Públicas.

47. Como se puso de manifiesto en el IPN/CNMC/029/21, la diversificación de suministradores en las redes 5G de los operadores es una de las medidas principales de la caja de herramientas de la UE. Además de mejorar la resiliencia de las redes, añadir suministradores reduce la dependencia excesiva de determinados proveedores que puede perjudicar la competencia (*vendor lock-in*). Sin embargo, las estrategias multi-proveedor también son difíciles de implantar, ya que los operadores encuentran dificultades asociadas a la gestión de red y la interoperabilidad entre suministradores[13]. De hecho, según información reciente recabada por BEREC[14], más de la mitad de los operadores encuestados tienen un único proveedor para las funciones críticas del núcleo de red 5G. Un aspecto señalado por los operadores se refiere a que la

[13] Información recabada en el informe BEREC BoR (20) 228 "Report of BEREC recent activities concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)

[14] Informe BoR (23) 180 "BEREC Report Secure 5G Networks", de 5 de octubre de 2023.

interoperabilidad de equipos requiere un mayor esfuerzo de integración en las redes 5G.

48. Teniendo en cuenta esta información, el RDL5G tiene en cuenta la realidad del mercado al haberse modificado la obligación de los operadores de disponer de dos suministradores en el núcleo de la red y los sistemas de control y gestión y posibilitar que puedan tener un único suministrador.

49. La potestad de modificar la cadena de suministro por el Ministerio es una medida de gran impacto, que podría forzar a los operadores a incorporar suministradores y llegar a afectar la escalabilidad y eficiencia operativa de las soluciones de red 5G-SA implantadas, si no se diseña una estrategia de diversidad de suministradores apropiada. Por ello, se recomienda incluir criterios y plazos de ejecución adecuados, focalizando el objetivo de diversificación en aquellos elementos de la red que sean prioritarios y minimizando los inconvenientes asociados a la interoperabilidad e integración de equipos. Para llegar a este objetivo parecen prometedoras las actividades de certificación de equipos y productos que se están llevando a cabo a nivel europeo, e incluso podría valorarse su impulso por medio de ayudas públicas (véase el apartado I).

50. Asimismo, a la hora de aplicar esta medida, conviene tener en cuenta que debe existir un balance de suministradores 5G suficiente a nivel nacional para asegurar la resiliencia en caso de incidente de seguridad que pueda afectar a un determinado suministrador, de acuerdo con lo estipulado en el artículo 23.3 del RDL5G, pudiendo el ENS5G llegar a proponer objetivos de diversificación de suministradores 5G para el conjunto del Estado.

G. Análisis de riesgos a nivel nacional

51. Con respecto al análisis de riesgos a nivel nacional aportado en el Anexo II del ENS5G, se considera apropiado el planteamiento por fases empleado para su realización, ya que sigue la metodología utilizada en el estándar ISO/IEC 27005: 2018 y es el seguido de manera general en el Esquema Nacional de Seguridad del sector público. No obstante, se señalan las siguientes consideraciones:

- Incorporación de determinados activos de red al análisis de riesgos: Los activos de computación en el borde o MultiAccess Edge-Computing (MEC) se incluyen como activos de las redes 5G, pero no consta su análisis particularizado de riesgos, lo cual debería solventarse al igual que para las funcionalidades de segmentación de la red (network slicing). Aunque el despliegue de estos elementos está por el momento limitado a entornos de prueba o pilotos, estos activos serán primordiales para el despliegue de servicios avanzados de baja latencia en aplicaciones multi-sectoriales. Por tanto, sería conveniente

incluir su valoración de riesgos si se ha aportado información por parte de los sujetos obligados.

- Análisis relativo a la dependencia de suministradores: el análisis de riesgos a nivel nacional no incluye la dependencia de suministradores como un factor considerado en dicho análisis, ni las vulnerabilidades ligadas a la cadena de suministro, a pesar de la importancia otorgada a las estrategias de diversificación de la cadena de suministro del RDL5G y del propio ENS5G (apartados b y c del artículo 22.2 del RDL5G).
- Falta de información sobre la jerarquía de riesgos: se incluye la metodología para identificar el nivel de riesgo de una amenaza según su probabilidad de ocurrencia y su impacto en la red, dependiendo de la criticidad del activo afectado y alcance del ataque. Sin embargo, no se establece una jerarquía de los riesgos que pueden afectar a cada activo de red, en función de dicho análisis (artículo 22.3 del RDL5G). Además, se debe incorporar al análisis si el nivel de riesgo se considera mitigado o eliminado en función de las medidas aplicadas por los operadores, a partir de la información recabada (artículo 22.2.d del RDL5G).
- Se sugiere diferenciar el análisis del nivel de criticidad de la infraestructura física de la red de acceso con respecto a otras infraestructuras físicas que alberguen activos con mayor nivel de criticidad.

H. Condiciones de aplicación de las medidas de mitigación de riesgos

52. El ENS5G incorpora un catálogo de medidas para solventar los riesgos identificados en el análisis de riesgos a nivel nacional, incluido en el Anexo III. El artículo 18 especifica que los sujetos obligados deberán adoptar las medidas adecuadas en base a lo establecido en el RDL5G, el propio ENS5G y los actos que se dicten para su ejecución. Sin embargo, no especifica qué medidas concretas del Anexo III son aplicables para cada sujeto.

53. Se recomendaría especificar si son requisitos mínimos exigibles a todos los sujetos obligados o si su aplicación está condicionada en función del tipo de entidad obligada (operador, suministrador, usuario corporativo o incluso Administración Pública).

54. Se considera conveniente aportar detalles sobre los criterios, condiciones y plazos de aplicación de las medidas mencionadas, como se estipula en el propio artículo 10.1 del ENS5G. Asimismo, se propone la inclusión de una tabla o esquema que relacione la aplicabilidad de cada medida a cada activo de red en función de la jerarquía de riesgos analizada en la metodología del Anexo II, para facilitar su identificación.

I. Impulso a la interoperabilidad y apoyo a la I+D+I

55. Por el momento el ENS5G no incorpora el desarrollo de medidas de apoyo a la I+D+I y de impulso a la interoperabilidad (previstas en el artículo 26 y 27 del RDL5G). Dado que la interoperabilidad de equipos, programas y servicios tiene especial relevancia en el ámbito de las redes 5G (véanse los párrafos 47 y 49), cabría valorar el desarrollo de tecnologías y entornos que favorezcan dicha interoperabilidad como parte de estas medidas.

Cuarto. Comentarios formales

56. En el artículo 13.4 del ENS5G se hace referencia al "límite mínimo de dos suministradores diferentes establecido en el apartado anterior". Esta referencia debería corregirse, dado que no se incluye en el apartado inmediatamente anterior, sino en el apartado 2 de dicho artículo.

57. El artículo 33 especifica que el régimen sancionador será el establecido en los artículos 30 y 31 del RDL5G. Estos artículos del RDL5G se remiten, excepto en lo previsto en dicha norma, a la regulación en materia de régimen sancionador establecida en la Ley 9/2014[15], régimen actualmente derogado. Para mayor claridad se sugiere incluir en el artículo 33 del ENS5G la mención expresa al Título VIII de la actual LGTel, al igual que se menciona esta Ley en el artículo 32 relativo a las facultades de inspección.

58. Se observa también que el preámbulo del proyecto de Real Decreto incluye una referencia errónea a la disposición final séptima del Real Decreto-ley 6/2023, de 19 de diciembre, en lugar de referirse a la disposición final quinta.

VI. CONCLUSIONES

59. Como se ha visto en el presente Informe, el proyecto de Real Decreto por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G desarrolla con mayor detalle la metodología de análisis de riesgos que afectan a las redes y servicios 5G y propone una serie de medidas de seguridad para solventar o mitigar dichos riesgos.

60. Conforme a lo expuesto se considera conveniente abordar la modificación de algunas de sus disposiciones, especialmente en relación con los siguientes aspectos:

[15] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Se proponen ciertas aclaraciones respecto a los elementos críticos de la red 5G y su descripción.
- Se recomienda delimitar los criterios, plazos y ámbito de aplicación de las medidas de reubicación de elementos críticos en territorio nacional.
- Se recomienda valorar el potencial impacto en la capacidad competitiva de los sujetos afectados por las medidas de sustitución de elementos críticos de suministradores de alto riesgo o de denegación de la autorización para la instalación de estaciones radio en ubicaciones críticas.
- Se deberían precisar adecuadamente los criterios aplicados en la denegación de autorizaciones de instalación de estaciones radio en ubicaciones críticas.
- Se recomienda incluir criterios y plazos de ejecución adecuados en caso de modificación de las estrategias de diversificación de los operadores.
- Se debería incorporar al análisis de riesgos nacional información sobre determinados activos, la dependencia de suministradores y el resultado del establecimiento de una jerarquía de riesgos.
- Cabría aclarar los criterios, condiciones y plazos de aplicación de las medidas de seguridad establecidas a nivel nacional, que debe cumplir cada sujeto obligado.
- Se sugiere la revisión del soporte legal necesario para el desarrollo de algunas medidas no incluidas en el RDL5G (posibilidad de instar la reubicación de equipos en territorio nacional y restricciones a los usuarios corporativos).