MINISTERIO
DE TRANSFORMACION
DIGITAL

REF.:
REF.C.M.:

Capítulo Epígrafe (A rellenar en el “Boletín Oficial del Estado”)	

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

Las comunicaciones móviles de quinta generación o 5G constituye un nuevo paradigma de las comunicaciones electrónicas con un gran potencial transformador en beneficio de la sociedad y la economía, pues se abre la posibilidad a la incorporación de nuevas funcionalidades que van a tener un gran impacto como la computación en la red, permitirán crear redes virtuales, ofrecer baja latencia y prestar servicios de gran valor añadido para la sociedad y economía en ámbitos como el de la medicina, el transporte y la energía. Por eso, la Unión Europea y España, directamente y a través del Mecanismo de Recuperación y Resiliencia, impulsan 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 las de generaciones precedentes. Pero presentan también riesgos específicos derivados, por ejemplo, de su arquitectura de red más compleja, abierta y desagregada, y de su capacidad para transportar ingentes volúmenes de información y permitir la interacción simultánea de múltiples personas y cosas. Su interconexión con otras redes y el carácter transnacional de muchas de las amenazas inciden en su seguridad, y el previsible empleo generalizado de estas redes para funciones esenciales para la economía y la sociedad incrementará el impacto potencial de los incidentes de seguridad que sufran.

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 la «caja de herramientas».

El Real decreto-ley 7/2022, de 29 de marzo, se ha visto modificado recientemente por la disposición final séptima del Real Decreto-ley 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, con el objetivo de reforzar los controles a efectuar por el Gobierno y el Ministerio de Transformación Digital sobre las condiciones en las que se vienen efectuando la instalación de los distintos equipos, elementos, funciones y sistemas propios de la tecnología 5G, el despliegue de las redes 5G y la prestación de servicios de comunicaciones electrónicas 5G, en aras de alcanzar el objetivo último que persigue dicha norma, cual es, como indica su artículo 1, establecer requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G).

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. Así, el artículo 21 del Real decreto-ley 7/2022, de 29 de marzo, establece que el Gobierno aprobará, 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.

A su vez, el artículo 20 del Real decreto-ley 7/2022, de 29 de marzo, establece que el Esquema Nacional de Seguridad de redes y servicios 5G llevará a cabo un tratamiento integral y global de la seguridad de las redes y servicios 5G, considerando las aportaciones al alcance de cada agente

de la cadena de valor de 5G para garantizar un funcionamiento continuado y seguro de la red y los servicios 5G. A tal efecto, en el Esquema Nacional de Seguridad de redes y servicios 5G se efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G así como identificará, concretará y desarrollará medidas a nivel nacional para mitigar y gestionar los riesgos analizados.

Por último, para completar el marco de referencia, cabe mencionar que el artículo 5.3 del Real Decreto-ley 7/2022, de 29 de marzo, establece que el Esquema Nacional de Seguridad de redes y servicios 5G 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.

Para dar cumplimiento a este mandato, la presente norma aprueba el Esquema Nacional de Seguridad de las redes y servicios 5G.

Se cumple el principio de necesidad, pues este real decreto se dicta para garantizar un bien de interés general, como es la seguridad y confianza en las comunicaciones electrónicas. Es conforme con el principio de proporcionalidad ya que las medidas son adecuadas a los riesgos identificados en cada caso. Se ajusta al principio de seguridad jurídica porque se reconoce el marco normativo vigente en materia de seguridad y solo se añaden requisitos y controles adecuados a la singularidad de las redes y servicios 5G y sus riesgos. Se respeta el principio de transparencia, ya que los interesados han podido participar en el procedimiento de elaboración de la norma. Por último, 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.

Este real decreto ha sido sometido al 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 del Parlamento Europeo y del Consejo, de 9

de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

Este real decreto se dicta al amparo de lo dispuesto 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,

En su virtud, en cumplimiento de lo establecido en el artículo 21 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, a propuesta del Ministro de Transformación Digital, previo informe del Consejo de Seguridad Nacional y dictamen del Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día xx de xxxxxx de 2024,

DISPONGO:

Artículo único. Aprobación del Esquema Nacional de Seguridad de las redes y servicios 5G.

Se aprueba el Esquema Nacional de Seguridad de las redes y servicios 5G, que se inserta a continuación

Disposición adicional primera. Revisión del Esquema Nacional de Seguridad de las redes y servicios 5G.

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.

Disposición adicional segunda. Aplicación del Real decreto-ley 7/2022, de 29 de marzo, y el Esquema Nacional de Seguridad de las redes y servicios 5G a las sucesivas generaciones de comunicaciones electrónicas.

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 el Esquema Nacional de Seguridad de las redes y servicios 5G que se aprueba serán de aplicación a generaciones de comunicaciones electrónicas posteriores a la quinta generación mientras no exista norma específica para las mismas.

Disposición final primera. Título competencial.

Este 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.

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

1. En todo lo que no esté regulado en este real decreto y el esquema que aprueba, será de aplicación supletoria lo dispuesto en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y su normativa de desarrollo.

2. En lo no regulado en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y su normativa de desarrollo, será aplicación supletoria el Real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, así como su respectiva normativa de desarrollo.

Disposición final tercera. Habilitación para el desarrollo reglamentario y modificación de anexos.

1. Se habilita a la persona titular del Ministerio de Transformación Digital para desarrollar lo previsto en este real decreto y el esquema que aprueba.

2. Se habilita a la persona titular del Ministerio de Transformación Digital para modificar mediante orden el contenido de los anexos del Esquema Nacional de Seguridad de las redes y servicios 5G 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.

Disposición final cuarta. Entrada en vigor.

Este real decreto y el esquema que aprueba entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ELÉVESE AL CONSEJO DE MINISTROS

Madrid, XX de xxxxxx de 2024

EL MINISTRO DE TRANSFORMACIÓN DIGITAL

José Luis Escrivá Belmonte

ESQUEMA NACIONAL DE SEGURIDAD DE LAS REDES Y SERVICIOS 5G

Capítulo I
Disposiciones generales

Artículo 1. Esquema Nacional de Seguridad de las redes y servicios 5G.

El Esquema Nacional de Seguridad de las redes y servicios 5G (en adelante, ENS5G) se aprueba 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.

Artículo 2. Objetivos.

El ENS5G tiene los siguientes objetivos:

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

Artículo 3. Definiciones.

A los efectos del ENS5G, se utilizarán las definiciones establecidas 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, así como las definiciones establecidas en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y en el Código Europeo de las Comunicaciones Electrónicas.

Artículo 4. Ámbito de aplicación.

El ENS5G se aplica a los siguientes sujetos obligados:

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

Artículo 5. Red 5G.

1. Una red de comunicaciones electrónicas 5G está integrada, al menos, por los siguientes elementos, infraestructuras y recursos:

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

e) Las funciones de computación en el borde, virtualización de red y gestión de sus componentes.

f) Los relativos a intercambios de tráfico o interconexión con redes externas e Internet.

g) Otros componentes y funciones a los que se refiere el anexo I.

2. La descripción detallada de los elementos, infraestructuras y recursos que integran una red 5G figura en el anexo I.

3. Son elementos críticos de una red 5G:

a) Los relativos a las funciones del núcleo de la red.

b) Los sistemas de control y gestión y los servicios de apoyo.

c) La red de acceso en aquellas zonas geográficas y ubicaciones que se determine.

4. Los elementos críticos de una red 5G deberán ubicarse dentro del territorio nacional. No obstante, determinados elementos, funciones y sistemas tanto del núcleo de la red como de los sistemas de control y gestión y los servicios de apoyo podrán ubicarse fuera del territorio nacional, siempre y cuando el Ministerio de Transformación Digital pueda ejercer las facultades que le atribuye el Real Decreto-ley 7/2022, de 29 de marzo, en particular, las facultades de inspección y régimen sancionador previstas en su capítulo V, de manera que pueda efectuar una verificación integral sobre el funcionamiento, operatividad y condiciones de uso de dichos elementos críticos de una red 5G y, en su caso, poder adoptar medidas, cautelares o definitivas, sobre dichos elementos, funciones y sistemas o el equipamiento utilizado en el ejercicio de las potestades que al Ministerio de Transformación Digital le atribuye el Real Decreto-ley 7/2022, de 29 de marzo y la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

En el caso de que el Ministerio de Transformación Digital llegue a la conclusión de que los elementos, funciones y sistemas tanto del núcleo de la red como de los sistemas de control y gestión y los servicios de apoyo que estén ubicados fuera del territorio nacional afectan, ya sea por razones de aplicación de medidas técnicas o por medidas estratégicas, a la seguridad o integridad de la red 5G o condiciona sensiblemente el ejercicio de sus facultades de supervisión y potestades de inspección, podrá requerir al titular de la red 5G que dichos elementos, funciones y sistemas se

ubiquen en territorio nacional. A tal efecto, la reubicación de los elementos, funciones y sistemas deberá producirse en el plazo que indique el Ministerio de Transformación Digital en su resolución, previa audiencia del titular de la red 5G, si bien este plazo no podrá ser inferior a tres meses.

Artículo 6. Tratamiento integral de la seguridad.

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con la red o servicio 5G. El ENS5G tiene la vocación de llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G.

2. A tal efecto, el ENS5G ha tenido en cuenta y deberá tener en cuenta en futuras actualizaciones o modificaciones la normativa, las recomendaciones y los estándares técnicos de la Unión Europea, de la Unión Internacional de Telecomunicaciones (UIT) y de otras organizaciones internacionales,

Asimismo, el ENS5G ha tenido en cuenta y deberá tener en cuenta en futuras actualizaciones o modificaciones las aportaciones, análisis de riesgos, planes de mitigación de riesgos y estrategias de diversificación de la cadena de suministro que se han ido proporcionando y que deberán proporcionar por los sujetos obligados en cumplimiento de las obligaciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, en este esquema y en el resto de normativa.

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

Artículo 7. Gestión de la seguridad basada en los riesgos.

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado en la red o servicio 5G, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza y características de la red, de los servicios a prestar y de los riesgos a los que estén expuestos.

Artículo 8. Vigilancia continua y reevaluación periódica.

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de las redes y servicios 5G permitirán medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Capítulo II
Análisis y gestión de riesgos a nivel nacional

Artículo 9. Análisis de riesgos a nivel nacional.

1. El análisis de riesgos a nivel nacional que debe realizar el ENS5G es el que figura en el anexo II de este esquema.

2. En la realización de este análisis, se ha tenido en cuenta:

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

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

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

d) La evaluación de la eficacia de las medidas de seguridad aplicadas hasta la aprobación de cada análisis de riesgos nacional para mitigar los riesgos puestos de manifiesto por tal análisis.

Artículo 10. Gestión de riesgos a nivel nacional.

1. 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 de este esquema.

2. En la determinación de estos criterios y requisitos de gestión de riesgos se han tenido en cuenta el análisis de riesgos nacional que incorpora esta estrategia y la evaluación de la eficacia de las medidas aplicadas con anterioridad por los sujetos obligados para mitigar y gestionar los riesgos en las redes y servicios 5G.

Capítulo III

Medidas específicas para garantizar la seguridad de las redes y servicios 5G

Artículo 11. Declaración de suministradores 5G de alto riesgo y de riesgo medio.

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

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

2. En relación con el análisis de las medidas técnicas y las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios se valorarán aspectos relativos al cumplimiento de normas o especificaciones técnicas, su verificación mediante esquemas de certificación, o la superación de pruebas o auditorías de seguridad realizadas por entidades independientes.

3. En relación con el análisis de las medidas estratégicas y exposición a injerencias externas, se valorarán los siguientes aspectos:

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

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

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

d) Las características de la legislación y la política de ciberdefensa y el respeto al derecho internacional y a las resoluciones y acuerdos de la Organización de las Naciones Unidas de ese tercer Estado.

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

f) El grado de adecuación de la normativa del tercer Estado sobre protección de datos personales a la de España, al Reglamento General de Protección de Datos aprobado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, adoptada por la Unión Europea y a cualquier otra normativa aplicable en materia de seguridad de las redes y sistemas de información y de telecomunicaciones.

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

En la determinación del plazo de sustitución, el acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como suministradores de alto riesgo podrá establecer un plazo diferente para los distintos elementos críticos de la red pública 5G en función de la criticidad de dicho 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 de equipos de telecomunicación, si bien, en ningún caso, este plazo podrá ser inferior a un año para cualquier elemento crítico de la red pública 5G.

El acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como suministradores de alto riesgo podrá determinar un plazo diferente para la sustitución de los equipos, productos y servicios para los distintos operadores 5G afectados en función de la repercusión que dicha sustitución tiene en la red de cada operador, de la afectación de la sustitución a los distintos elementos o partes de la red 5G, de los contratos de suministro de equipamiento suscritos y de la capacidad de suministro existente en el mercado de equipos de telecomunicación.

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

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

Artículo 12. Determinación de ubicaciones en las que no se podrá instalar equipos de suministradores calificados de alto riesgo.

1. 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.

2. En la determinación de estas ubicaciones, áreas y centros se incluirán las centrales nucleares, centros vinculados a la Defensa Nacional y las ubicaciones, áreas y centros que, por su vinculación a la seguridad nacional o al mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, sean determinados por Consejo de Seguridad Nacional.

3. En las estaciones radioeléctricas con las que se proporcione cobertura a estas ubicaciones, áreas y centros, los operadores 5G no podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo.

4. Asimismo, para la instalación, modificación o adaptación de estaciones radioeléctricas que proporcionen cobertura a estas ubicaciones, áreas y centros previamente declarados, habida cuenta de su vinculación con la seguridad nacional o al mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, los operadores 5G deberán solicitar autorización a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en cuyo otorgamiento se tendrán en cuenta los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares a instalar, las condiciones técnicas en el uso del dominio público radioeléctrico y las características intrínsecas y fines a proteger en esas ubicaciones, áreas y centros previamente declarados.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en el otorgamiento de estas autorizaciones, podrá valorar los planes que los operadores 5G puedan presentar para la renovación tecnológica o la sustitución de equipos de transmisión radio y en la red de acceso que afecten a las ubicaciones, áreas y centros previamente declarados para las que se solicita autorización.

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

5. La determinación y difusión de estas ubicaciones serán tratadas como materias clasificadas conforme a la regulación establecida en la Ley 9/1968, de 5 de abril, sobre secretos oficiales.

Artículo 13. Diversificación en la cadena de suministro.

1. Los operadores 5G deberán diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales en una red pública 5G.

2. En la red de acceso, los operadores 5G deberán contar con equipos de transmisión radio que sean proporcionados, como mínimo, por dos suministradores diferentes a efecto de favorecer la continuidad de los servicios 5G, la más fácil sustituibilidad de los equipos y evitar la dependencia exclusiva de un suministrador único.

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

3. En el núcleo de la red y en los sistemas de control y gestión y los servicios de apoyo, el suministrador podrá ser único.

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

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

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

Capítulo IV

Análisis de riesgos por los sujetos obligados

Artículo 14. Análisis de riesgos por los operadores 5G.

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

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

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

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

4. A fin de llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G, el operador 5G deberá recabar de sus suministradores las prácticas y medidas de seguridad que se han adoptado en los productos y servicios que les han suministrado, teniendo en cuenta los factores de riesgo indicados en este capítulo y el perfil de riesgo del suministrador. Esta información deberá ser proporcionada por los suministradores y su tratamiento será confidencial, de manera que sólo podrá ser utilizada por los operadores 5G para efectuar un análisis y gestión de riesgos y por el Ministerio de Transformación Digital y los demás organismos públicos competentes para la aplicación de lo dispuesto en el Real decreto-ley 7/2022, de 29 de marzo y en este esquema a los exclusivos fines de los mismos.

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

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

6. Un nuevo análisis de riesgos por el operador 5G debe ser llevado a cabo y ser remitido al Ministerio de Transformación Digital antes del 1 de octubre de 2024, y, a continuación, cada dos años.

Artículo 15. Análisis de riesgos por los suministradores 5G.

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

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

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

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

Artículo 16. Análisis de riesgos por los usuarios corporativos 5G.

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

recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes privadas 5G o en la prestación de servicios 5G en autoprestación.

2. Los usuarios corporativos 5G mencionados en el apartado anterior deberán aportar este análisis de riesgos al Ministerio Transformación Digital, cuando sean requeridos para ello.

Artículo 17. Confidencialidad de la información sobre análisis de riesgos.

1. El Ministerio de Transformación Digital podrá recabar de los sujetos obligados la información necesaria para el análisis de riesgos.

2. Los sujetos obligados deben proporcionar la información en el plazo de quince días hábiles a contar desde el día siguiente al de la notificación del requerimiento de información.

3. El incumplimiento de los requerimientos de información formulados conforme a lo indicado en el apartado anterior cuando haya pasado un mes desde la finalización del plazo dado para su cumplimiento es calificado como infracción grave.

4. La información que los sujetos obligados proporcionen sobre el análisis de riesgos 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 este Esquema y en los actos que se dicten en ejecución de ambas disposiciones.

Capítulo V
Gestión de los riesgos por los sujetos obligados

Artículo 18. Deber de gestionar los riesgos de seguridad.

Los sujetos obligados deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G, con base en lo establecido en el Real decreto-ley 7/2022, de 29 de marzo, en este Esquema y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 19. Gestión de seguridad por los operadores 5G.

1. Los operadores 5G deberán garantizar la instalación, despliegue y explotación seguros de redes públicas 5G y la prestación segura de servicios 5G disponibles al público mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de redes y servicios 5G, así como el cumplimiento de la normativa en esta materia.

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

a) Adoptar medidas técnicas y operativas para garantizar la integridad física y lógica de las redes 5G o cualesquiera de sus elementos, infraestructuras y recursos, así como la continuidad en la prestación de servicios 5G.
b) Adoptar planes y medidas de contingencia específicas para asegurar la continuidad de otros servicios esenciales para la sociedad que dependan de las redes y servicios 5G.
c) Seleccionar e identificar a las personas que puedan acceder a los activos físicos y lógicos de la red, y realizar el mantenimiento de registros de acceso.
d) Mantener las credenciales de usuario para el acceso a la red en posesión del operador.
e) Utilizar únicamente productos, recursos, servicios o sistemas certificados para la operación de las redes 5G, o en alguna de sus partes o elementos.
   En particular, es de aplicación el esquema de certificación GSMA Network Equipment Security Assurance Scheme (NESAS).
f) Cumplir las normas o especificaciones técnicas aplicables a redes y sistemas de información.
   En particular, es de aplicación la norma técnica ISO/IEC 27001: Gestión de Seguridad de la Información.

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

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

   En particular, los operadores 5G deben presentar al Ministerio de Transformación Digital con una periodicidad anual una auditoria sobre la aplicación del esquema de certificación GSMA Network Equipment Security Assurance Scheme (NESAS) y de la norma técnica ISO/IEC 27001: Gestión de Seguridad de la Información.

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

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

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

a) Deberán diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales en una red pública 5G que dé cumplimiento a lo dispuesto en el artículo 13.

b) No podrán utilizar en los elementos críticos de red equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo conforme a lo dispuesto en el artículo 11.

c) No podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo, en aquellas estaciones radioeléctricas con las que se proporcione cobertura en las ubicaciones, áreas y centros que se hayan identificado conforme a lo establecido en el artículo 12.

d) Deberán ubicar los elementos críticos de una red pública 5G dentro del territorio nacional, sin perjuicio de lo establecido en el artículo 5.4.

4. Los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Transformación Digital una nueva estrategia de diversificación en la cadena de suministro antes del 1 de octubre de 2024.

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

Igualmente, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Transformación Digital antes del 1 de octubre de cada año información sobre el estado de ejecución de la estrategia de diversificación en la cadena de suministro.

5. Los operadores 5G deberán remitir al Ministerio de Transformación Digital una nueva descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos antes del 1 de octubre de 2024 y, a continuación, cada dos años.

Artículo 20. Gestión de seguridad por los suministradores 5G.

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

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

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

En particular, es de aplicación la norma técnica ISO/IEC 27001: Gestión de Seguridad de la Información.

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

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

   En particular, es de aplicación el esquema de certificación GSMA Network Equipment Security Assurance Scheme (NESAS).

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

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

   En particular, los suministradores 5G deben presentar al Ministerio de Transformación Digital con una periodicidad anual una auditoria sobre la aplicación del esquema de certificación GSMA Network Equipment Security Assurance Scheme (NESAS) y de la norma técnica ISO/IEC 27001: Gestión de Seguridad de la Información

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

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

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

4. No obstante lo dispuesto en el apartado anterior, los suministradores 5G que hayan sido calificados de alto riesgo o de riesgo medio deberán remitir al Ministerio de Transformación Digital un informe de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos en el plazo de seis meses a contar desde que hayan sido calificados de alto riesgo o de riesgo medio.

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

Artículo 21. Gestión de seguridad por los usuarios corporativos 5G.

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

2. Los usuarios corporativos 5G mencionados 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.

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

Artículo 22. Gestión de seguridad por las Administraciones públicas.

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

2. En particular, las administraciones públicas que quieran llevar a cabo la instalación, despliegue y explotación de redes 5G, ya sean públicas o privadas, o la prestación de servicios 5G, disponibles

al público o en autoprestación, no podrán, por razones de seguridad nacional, utilizar equipos, productos y servicios proporcionados por suministradores de alto riesgo o riesgo medio.

Artículo 23. Condiciones de cumplimiento de las obligaciones.

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 este esquema y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 24. Confidencialidad de la información sobre gestión de riesgos.

1. El Ministerio de Transformación Digital podrá recabar de los sujetos obligados la información necesaria para la gestión de riesgos.

2. Los sujetos obligados deben proporcionar la información en el plazo de quince días hábiles a contar desde el día siguiente al de la notificación del requerimiento de información.

3. El incumplimiento de los requerimientos de información formulados conforme a lo indicado en el apartado anterior cuando haya pasado un mes desde la finalización del plazo dado para su cumplimiento es calificado como infracción grave.

4. La información que los sujetos obligados proporcionen sobre la gestión de riesgos 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 este esquema y en los actos que se dicten en ejecución de ambas disposiciones.

Capítulo VI

Otras medidas de cumplimiento en materia de la seguridad de las redes y servicios 5G

Artículo 25. Deber de colaboración en la modificación y ejecución del ENS5G.

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 le sea requerida para la modificación y ejecución del ENS5G.

Artículo 26. Certificación de equipos y productos.

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.

Artículo 27. Cumplimiento de la normativa sobre inversiones extranjeras y sobre competencia.

Las obligaciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, en este esquema y en los actos que se dicten en ejecución de ambas disposiciones se entienden sin perjuicio de la aplicación de los instrumentos de control sobre inversiones extranjeras directas en los sujetos obligados que sean de nacionalidad española, así como de la aplicación de la normativa en materia de defensa de la competencia.

Artículo 28. Equipos terminales.

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.

Artículo 29. Cooperación internacional.

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

2. En particular, el Ministerio de Transformación Digital podrán compartir información relacionada con los análisis que realicen las instituciones de la Unión Europea y con otros Estados miembros de la Unión Europea preservando, como corresponda en Derecho, la seguridad, los intereses comerciales y la confidencialidad de la información recabada en la elaboración del análisis, así como servirse de la información que le envíen otros Estados o las instituciones de la Unión Europea para su realización. Igualmente, podrá llevar a cabo estos análisis de forma conjunta con otros Estados miembros de la Unión Europea.

Capítulo VII
Aplicación del ENS5G

Artículo 30. Competencia para la aplicación del ENS5G.

1. El Ministerio de Transformación Digital será el departamento competente para aplicar el ENS5G y ejercer las demás funciones que le atribuye el Real decreto-ley 7/2022, de 29 de marzo.

2. El Ministerio de Transformación Digital se coordinará con los demás órganos competentes en materia de ciberseguridad e infraestructuras críticas para garantizar una aplicación coherente del ENS5G.

Artículo 31. Facultades para la aplicación del ENS5G.

El Ministerio de Transformación Digital, en el ejercicio de las funciones que le asigna el Real decreto-ley 7/2022, de 29 de marzo, y el ENS5G podrá ejercer, entre otras, las siguientes facultades:

a) Desarrollar, concretar y detallar el contenido del ENS5G.
b) Autorizar la instalación, modificación o adaptación de estaciones radioeléctricas que proporcionen cobertura a determinadas ubicaciones, áreas y centros en los términos establecidos en el artículo 12.4.
c) Formular requerimientos de información a los sujetos obligados, que deberán ser respondidos en el plazo de 15 días hábiles a contar desde el día siguiente al de su notificación, a efecto de poder ejercer las funciones que le asigna el Real decreto-ley 7/2022, de 29 de marzo, el ENS5G y su normativa de desarrollo y, en concreto, para verificar y controlar el cumplimiento de las respectivas obligaciones que se imponen a los sujetos obligados.
d) Realizar auditorías u ordenar su realización para verificar y controlar el cumplimiento de las respectivas obligaciones que el Real decreto-ley 7/2022, de 29 de marzo, el ENS5G y su normativa de desarrollo impone a los sujetos obligados.
e) Realizar inspecciones por los funcionarios destinados en la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y ejercer la potestad sancionadora en los términos indicados en el capítulo siguiente.
f) Conceder ayudas públicas.
g) Ejercer las demás funciones que le correspondan según la legislación aplicable.

Capítulo VIII
Inspección y régimen sancionador

Artículo 32. Facultades de inspección.

El Ministerio de Transformación Digital ejercerá en la aplicación y supervisión de lo establecido en el Real decreto-ley 7/2022, de 29 de marzo, el ENS5G y su normativa de desarrollo todas las potestades de la función inspectora previstas en dichas normas y en el Título VIII de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

Artículo 33. Régimen sancionador.

Será de aplicación el régimen sancionador establecido en los artículos 30 y 31 del Real decreto-ley 7/2022, de 29 de marzo.

ANEXO I

Elementos, infraestructuras y recursos que integran una red 5G

1. Descripción de la arquitectura de la red 5G-SA.

Para el análisis requerido en el presente Esquema Nacional de Seguridad de redes y servicios 5G, se utiliza una arquitectura de red de referencia, siguiendo la recomendación del 3GPP y la especificación ETSI TS 123 501.

En la figura siguiente, se muestra un esquema simplificado de una arquitectura 5G-SA para escenarios de no-roaming (que será utilizada de forma genérica como base). Elementos no presentados en la figura son el UDR, UDSF, UCMF, CHF, 5G-EIR, NWDAF y SEPP.

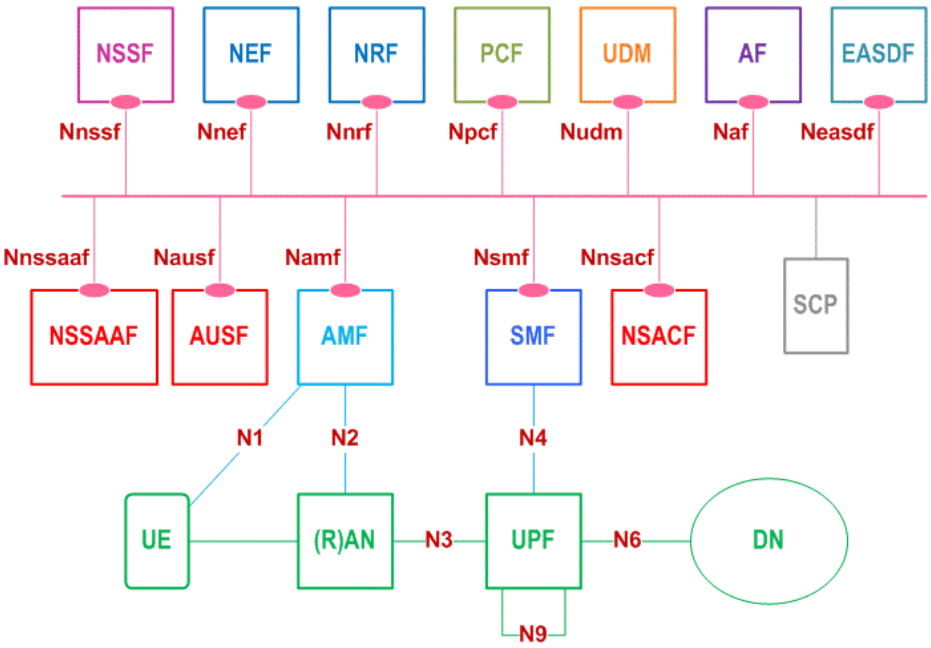


Fig. 1: Arquitectura 5G según especificación ETSI TS 123 501

Estos elementos de red son funciones software que se despliegan sobre una infraestructura de virtualización (compuesta, a su vez, de hardware y software de virtualización), la cual puede ser dedicada y específica para una función de red, o común para varias funciones, incluso funciones de red de varios suministradores 5G. En este escenario, la infraestructura para hospedar las

funciones de red virtualizadas puede estar diversificada tanto geográficamente como por suministradores 5G diferentes, tal y como se describirá más adelante en este documento.

Adicionalmente a los elementos de red, se despliegan un conjunto de Sistemas para la operación y gestión de la red GER (también denominados OSS, Operations Support System).

2. Identificación y descripción de los entornos de red 5G-SA.

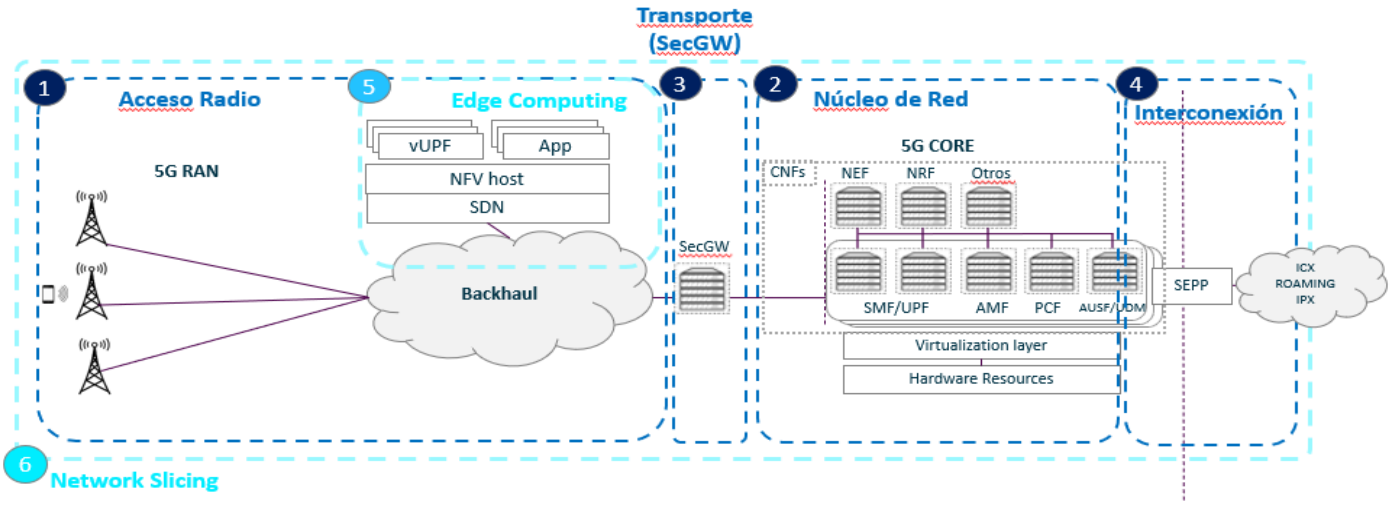
Con el objetivo de desglosar la complejidad de la arquitectura de una red 5G-SA, se divide la misma en entornos de red.

Un entorno de red es una agrupación de activos que tienen un cometido y unas características particulares dentro de la red que los diferencian del resto de entornos.

Se puede distinguir dos tipologías de entorno:

a) Entornos Primarios: Se consideran entornos primarios aquellos propios de la tecnología o naturaleza de 5G que no existirían sin su despliegue.
b) Entornos Secundarios: Se consideran entornos secundarios aquellos comunes en un operador de telecomunicaciones.

En la siguiente figura (figura 2) se puede apreciar una clasificación de la red 5G-SA por entornos:



3. Entornos de red primarios.

Dentro de los entornos de red primarios, se encuentra el Acceso Radio, el Núcleo de Red, el Transporte-Backhaul (SecGW), la Interconexión de Roaming y los Sistemas de Control, Gestión y Operación de la Red.

a) Acceso Radio: El entorno de acceso radio (RAN) se encarga de dotar de cobertura a los terminales para que estos se puedan conectar a la red. Destacan las siguientes funciones en el entorno:

    i) Operación y mantenimiento del emplazamiento radio. El software permite configurar cada emplazamiento con una serie de células por tecnología para poder prestar servicio a los usuarios y, durante el funcionamiento de la estación base, supervisa su estado para detectar posibles problemas o averías, ante cuya aparición reportaría una alarma al sistema de gestión para que el operador sea consciente y resuelva el problema.
    ii) Señalización. Para que los usuarios puedan registrarse en la red y establecer servicios portadores para sus comunicaciones, es necesaria señalización entre los terminales, la estación base, y el núcleo de red, y parte de estas funciones las realiza el software de la estación base.
    iii) Gestión de recursos radio. Los recursos radio de una célula dada son compartidos entre distintos usuarios y el software de la estación base es el responsable de repartirlos entre dichos usuarios (calidad del enlace radio decada usuario, demanda de velocidad, etc.). El software también puede distribuir a los usuarios entre las células de su estación base (o incluso con células de emplazamientos vecinos), para que el reparto de usuarios sea más homogéneo entre células vecinas.
    iv) Movilidad. el software de la estación base gestiona el traspaso de las comunicaciones de los usuarios entre distintas células, de su emplazamiento o de emplazamientos vecinos, a medida que los usuarios se desplazan por la red.

v) Transporte: La comunicación física con el resto de la red se realiza por medio de enlaces IP, eléctricos u ópticos, y la estación base tienen que encargarse de gestionar dichos enlaces (priorización entre los distintos tipos de tráfico que van por dichos enlaces, configuración de VLANs, supervisión del enlace, etc.).

La red 5G, en el plano de acceso radio (RAN), se implementa con un solo tipo de elemento de red denominado, de forma genérica, gNodoB (gNB). La mayoría de los suministradores 5G de Red de acceso radio disponen de distintos modelos de gNB, adaptados a distintos tipos de escenarios.

De forma genérica, existen los tipos siguientes:

i) Macro gNB: proporcionan mayor área de cobertura y capacidad de tráfico. Se instalan típicamente en azoteas de edificios o lugares con mucha visibilidad radioeléctrica, con el objetivo de dar cobertura y capacidad general.
ii) Micro gNB: de menor potencia, orientados a dar cobertura en localizaciones concretas, ya sean pequeños espacios públicos (como plazas) o espacios de interior (como lugares de eventos, oficinas pequeñas, etc.), o bien para dar capacidad complementaria a la capa general o macro. Se instalan principalmente en puntos de alta demanda de capacidad, para absorber dicha demanda.
iii) Sistemas gNB de cobertura de interiores: especializados en cubrir espacios de interiores grandes, con numerosos puntos radiantes de baja potencia, para distribuir la cobertura 5G por dicho espacio interior. Se instalan típicamente en grandes edificios de oficinas, estadios deportivos, metros, etc.

En este contexto, un emplazamiento de la Red de acceso radio 5G estará compuesto por una banda base y varias cabezas remotas y/o antenas activas. El número de cabezas remotas y antenas activas dependerá del número de bandas presentes en el emplazamiento, y del número de sectores.

El software del gNB es común a la banda base, a las cabezas remotas y a las antenas activas, y también es común entre los distintos sistemas de comunicaciones móviles presentes en el emplazamiento (2G, 3G, 4G y/o 5G). Mediante la interfaz NG la estación base se comunica con el Núcleo de red y mediante la interfaz aire con los terminales móviles.

b) Núcleo de Red: El núcleo de la red 5G-SA se compone de una serie de funciones de red estandarizadas por el 3GPP que se comunican entre ellas por conexiones tipo SBI (Service Based Interfaces), permitiendo un mallado total en función de las necesidades de cada una de ellas.

Los principios clave de esta arquitectura 5G-SA son:

i) Separar las funciones del plano de usuario (UP) de las funciones del plano de control (CP), lo que permite escalabilidad independiente, evolución e implementaciones flexibles, por ejemplo, ubicación centralizada o ubicación distribuida (remota).

ii) Modularizar el diseño de la función, por ejemplo, para permitir un corte de red flexible y eficiente.

iii) Permitir que cada Función de Red (y sus Servicios asociados) interactúen con otras Funciones de red, directa o indirectamente a través de un Proxy.

iv) Integrar diferentes tipos de acceso, por ejemplo, acceso 3GPP y acceso no 3GPP.

v) Soporta un marco de autenticación unificado.

vi) Desacoplar en las funciones de red las funciones de lógica de tipo “stateless” y relacionadas con capacidad de cómputo, de las funciones de estado de tipo “statefull” relacionadas con capacidades de almacenamiento.

vii) Permitir la exposición de datos de red de forma segura para el desarrollo de nuevos servicios en base a ellos.

viii) Soporte de acceso simultáneo a servicios locales (con requisitos de baja latencia) y servicios centralizados.

ix) Permitir y aceptar la itinerancia de tráfico con otras redes, según diferentes modelos de arquitectura.

El conjunto de funciones de núcleo de red definidas por el 3GPP es el siguiente:

i. AMF – Access and Mobility Management Function: función del plano de control de la red 5G. Sus principales funciones son la gestión del registro, la gestión de la movilidad, la gestión de la conexión, y la gestión de diversos aspectos relacionados con la seguridad y autorización de los accesos.

ii. SMF – Session Management Function: función del plano de control que se encarga de la gestión de las sesiones (establecimiento, modificación y liberación), gestión y asignación de IP a los terminales de usuario. En resumen, es la responsable de interactuar con el plano de usuario, creando, actualizando o borrando sesiones PDU, a la vez que administra el contexto de la sesión con el UPF.

iii. UPF – User Plane Function: función del plano de usuario. Es la responsable del reenvío, enrutamiento e inspección de paquetes, así como de la gestión de la calidad de servicio. Representa el punto de interconexión a la red de datos.

iv. PFC – Policy Control Function: es la encargada de proporcionar reglas de políticas a las funciones de red del plano de control, incluyendo network slicing, roaming, gestión de movilidad, o políticas de calidad de servicio 5G. Para la ejecución de las políticas, accede a la información de suscripción del UDR.

v. NRF – Network Repository Function: es la encargada del descubrimiento de los servicios, y mantiene el perfil e instancias de red disponibles. Sus funciones principales son la gestión del servicio, el descubrimiento de servicios, y access token, permitiendo poner en comunicación a dos elementos de la red 5G.

vi. SEPP – Security Edge Protection Proxy: es la función de red que permite una interconexión segura entre redes 5G, garantizando la confidencialidad y/o integridad de extremo a extremo entre la red de origen y la de destino, para todos los mensajes de roaming de interconexión 5G.

vii. UDM – Unified Data Management: función del plano de control cuyas principales misiones son la generación de credenciales de autenticación, la gestión de identidades de usuario, la gestión de suscripción, la autorización de acceso basado en datos de suscripción, y almacenamiento y gestión de las funciones de red que dan servicio al usuario. El UDM utiliza los datos de suscripción almacenados en el UDR.

viii. UDR – Unified Data Repository: es el repositorio unificado de datos de usuario. Estos datos se estructuran en diferentes categorías o tipos, y son accesibles a las diversas

funciones de red mediante una serie de servicios expuestos para la gestión y consulta de los mismos (UDM, PCR, NRF…, entre otros).

ix. AUSF – Authentication Server Function: es la función del plano de control de la red 5G que se encarga de la autenticación del usuario.

x. CHF – Charging Function: la funcionalidad de tarificación reside en el tarificador convergente (CCS, Converged Charging System), que ofrece las funcionalidades de tarificación online y offline. Entre sus funciones, está el OCF (Online Charging Function), para realizar el control online de las sesiones de datos, el CDF (Charging Data Function), para construir un CDR con la información de red recibida, el ABMF (Account Balance Management Function), para la gestión del saldo y controles de consumo, el RF (Rating Function), función para establecer un precio al uso recibido (tanto online como offline), y el CGF (Charging Gateway Function), para generar CDRs tarificados.

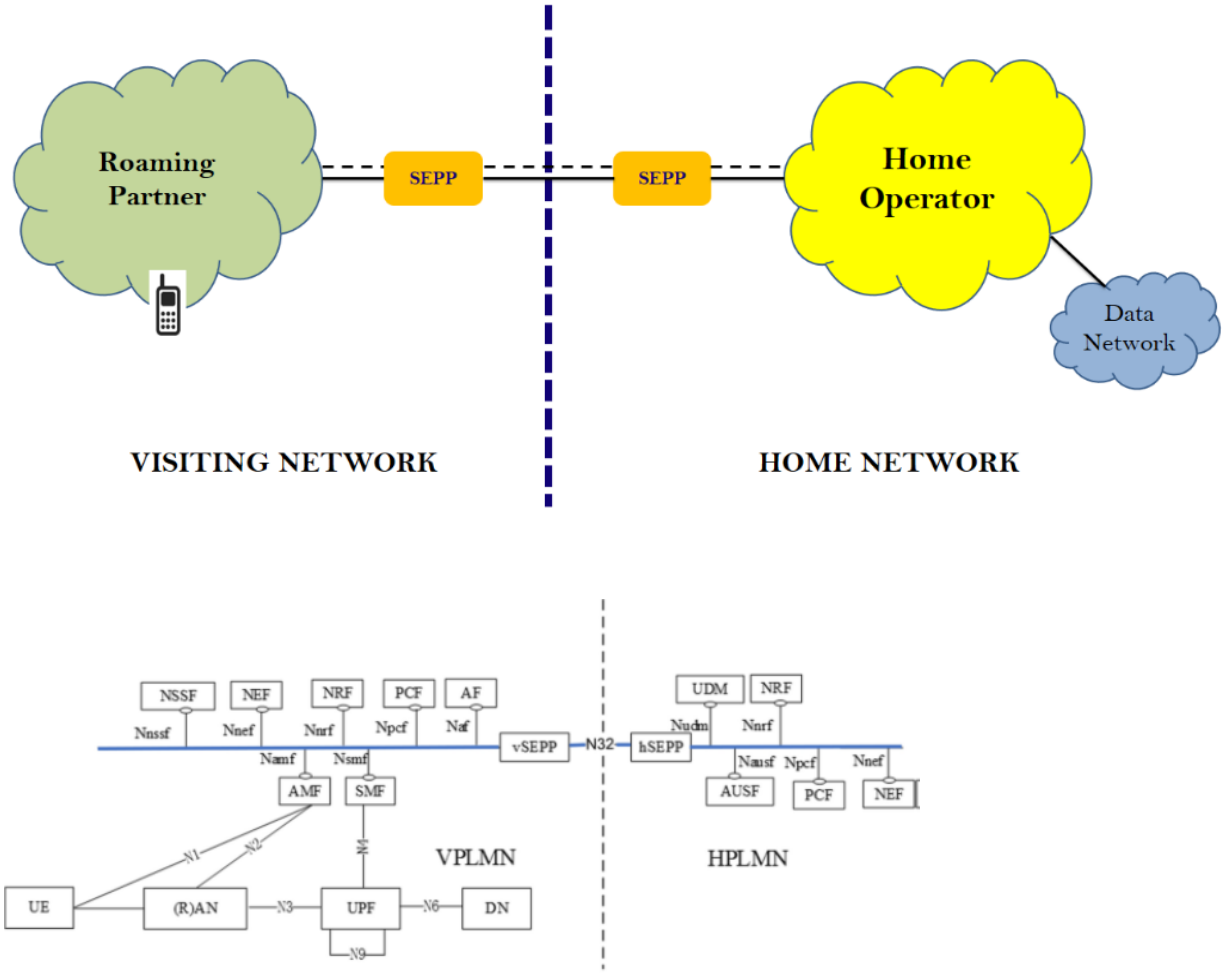
xi. NEF – Network Exposure Function: proporciona un medio para exponer, de forma segura, los servicios y capacidades ofrecidos por las funciones de red de 5G.

xii. 5G-EIR – 5G-Equipment Identity Register: es una funcionalidad opcional que ofrece la capacidad de chequear el estatus de la identidad del terminal (IMEI) y comprobar que no se encuentre en una lista negra.

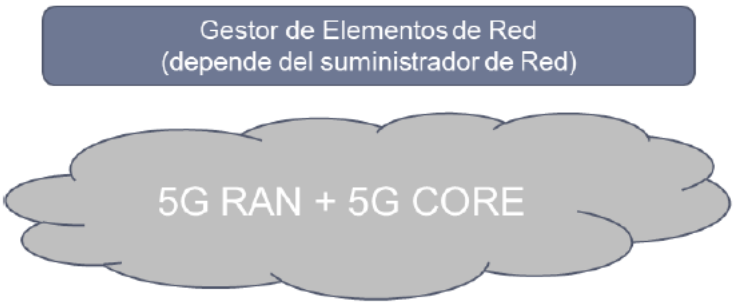
c) Transporte-Backhaul (SecGW): El Security Gateway (SecGW) proporciona el cifrado del tráfico del plano de control y del plano de usuario entre los entornos de Acceso Radio y de Núcleo de Red, evitando además exposiciones innecesarias de elementos críticos.

d) Interconexión Roaming: El entorno de Interconexión Roaming es necesario para la comunicación con el resto de los operadores de cara a permitir que un usuario de 5G pueda moverse de manera internacional ininterrumpiendo su servicio de voz o banda ancha.

En la siguiente figura (figura 3) se contiene la representación de un Entorno de Interconexión de Roaming:



e) Sistemas de Control, Gestión y Operación y Servicios de Apoyo: El proceso de aseguramiento del núcleo de red 5G se apoya en un conjunto de sistemas de apoyo a la operación (OSS) que se muestran en la siguiente figura (figura 4).



Estos sistemas OSS no forman parte de la prestación del servicio y, por tanto, fallos en su funcionamiento no afectan de forma directa a la disponibilidad de la red ni a la calidad del servicio prestado sobre ella. Sin embargo, la indisponibilidad de estos sistemas afectaría a la capacidad de supervisión, análisis, configuración y planificación de la red descrita en el punto anterior. Desde el punto de vista de la seguridad estos sistemas gestores están segmentados según el suministrador y por tanto una incidencia de seguridad en uno de ellos no afectaría a las funciones de red que no esté bajo el amparo de este OSS.

4. Entornos de red secundarios.

Dentro de los entornos de red secundarios, se encuentran las Plataformas de Virtualización, la Infraestructura física, el Edge-Computing y el Network Slicing.

a) Plataformas de Virtualización y Orquestación: Muchos de los elementos de una red 5G son funciones “software” que se despliegan sobre una infraestructura de virtualización (que, a su vez, se compone de hardware y software de virtualización), la cual puede ser dedicada y específica para una función de red, o común para varias funciones (incluso funciones de red de varios suministradores). En este contexto, la infraestructura para hospedar las funciones de red virtualizadas está diversificada tanto geográficamente como por suministradores diferentes.

b) Infraestructura física: Los elementos y funciones de red pertenecientes a los distintos entornos requieren de una infraestructura física donde emplazarlos, cuya naturaleza, disponibilidad y seguridad dependerá obviamente de la criticidad del activo en concreto. Esta infraestructura física otorga a los elementos y funciones de red las necesidades básicas para un correcto funcionamiento.

c) MultiAccess Edge-Computing (MEC): El edge computing multiacceso es un tipo de arquitectura o entorno de red que pretende llevar las funciones de procesamiento de tráfico de usuario y cloud computing TI al extremo de la red con el objetivo garantizar el funcionamiento de nuevos casos de uso que requieren una latencia mínima.

En concepto, se define en términos más amplios como una evolución del cloud computing que utiliza las tecnologías móviles y de nube para separar los hosts de aplicaciones del centro de datos donde se encuentran y trasladarlos hacia el extremo de la red. Esto no sólo permite que los usuarios finales estén más cerca de las aplicaciones, sino también que los servicios informáticos estén más cerca de los datos que estas generan.

En este Edge-Computing conviven tanto aplicaciones de terceros, como funciones de red para procesar en el Edge el tráfico de usuario.

d) Network Slicing: Se trata de una forma de arquitectura que ofrece la posibilidad de crear, sobre una infraestructura física de virtualización común compartida, varias redes virtuales personalizadas y aisladas de manera lógica entre sí, otorgando a cada una de ellas una criticidad determinada en función de las necesidades específicas de aplicaciones, servicios, dispositivos, clientes u operadores.

Se prevé que, con esta tecnología, los operadores de redes y servicios 5G puedan implementar una segmentación de red para crear múltiples redes virtuales con diferentes tamaños de conectividad, adaptándose a las necesidades de conexión de los diferentes usuarios, asignado de forma específica los recursos necesarios para garantizar el servicio correcto.

En líneas generales, dentro del concepto network slicing, cada red virtual (o porción de la red) engloba un conjunto independiente de funciones lógicas de red que soportan los requerimientos del caso de uso particular. Cada uno de ellos se optimizará para brindar los recursos y razonamientos matemáticos de red para el servicio y el tráfico que será usado en la segmentación.

En el caso de la tecnología 5G-SA, capacidad, conectividad, variedad, velocidad, cobertura y seguridad se asignarán para satisfacer las demandas específicas de cada caso de uso.

ANEXO II

ANÁLISIS DE RIESGOS A NIVEL NACIONAL

1. Metodología empleada.

Un análisis de riesgos tiene como objetivo identificar y categorizar las principales amenazas sobre las redes y servicios 5G, con la finalidad de determinar medidas correctivas que puedan disminuir sus consecuencias o incluso evitarlas.

Conociendo esta finalidad, el paso siguiente lógico es establecer los medios para lograr dicho objetivo. Un análisis de riesgos ha de realizarse con una metodología estandarizada, holística y un orden consecuente y lógico, pormenorizando cada uno de los aspectos de manera cualitativa y cuantitativa. En caso contrario, el nivel de riesgo calculado podría desvirtuarse y con él, los criterios y prioridades en las medidas de protección y/o acciones clave a llevar a cabo.

Se muestra a continuación las fases seguidas para el análisis efectuado, así como las fuentes de información utilizadas para la metodología utilizada.

1) Identificación y descripción de la arquitectura 5G, los entornos de red existentes en la misma y los activos que la componen, todo ello sujeto a la evolución tecnológica (ver anexo I)
2) Identificación de criticidad para los activos: para poder identificar el impacto de una amenaza en la red, es necesario primeramente determinar la criticidad de cada uno de los activos, basándonos en los tres ejes principales de la seguridad (**CIA**: *Confidencialidad*, *Integridad* y *Disponibilidad*).
3) Identificación de los riesgos de la tecnología 5G y su impacto en los activos identificados: determinar las potenciales amenazas presentes en este entorno específico, clasificándolas por activo e identificando su nivel de riesgo.
4) Identificación de las medidas de seguridad técnicas, organizativas y estratégicas, para paliar o reducir el nivel de riesgo de las amenazas identificadas para cada

entorno de red. Su efectividad será directamente proporcional al grado de disminución del nivel de riesgo para una determinada amenaza y activo.

5) Gestión de los riesgos y riesgos remanentes, en aquellas amenazas cuyo nivel sea considerable y no pueda ser disminuido por ninguna medida adicional desde el diseño (ver anexo III).

2. Factores que afectan a la criticidad de un activo.

De manera estandarizada y ampliamente reconocida, se consideran tres factores o conceptos claves a la hora de evaluar la criticidad de los activos de un determinado escenario, cuando de evaluar la seguridad de una solución es lo que aplica.

Los tres factores o conceptos principales son confidencialidad, integridad y disponibilidad (tríada CIA por sus siglas en inglés).

a) Confidencialidad: La confidencialidad en un activo o una red valora la capacidad de evitar que la información que está contenida en el activo, o en tránsito en la red, sea expuesta a usuarios no autorizados, los cuales no deben tener acceso a ésta. Las medidas de seguridad para garantizar la confidencialidad son diversas, desde la segmentación y el control de acceso, hasta el cifrado robusto de la información. El principal factor a la hora de valorar importancia de la confidencialidad en un activo es la sensibilidad de la información que almacena o transita por el mismo. Es importante tener en cuenta cuando se atiende a este factor, el impacto que puede tener para el resto de la red el hecho de que se comprometa ese activo.

   Ejemplos de riesgos que puedan comprometer la confidencialidad son los siguientes: Espiar/interceptar el tráfico/datos de usuario en la red (Man in the Middle/, Eavesdropping), u obtener las credenciales de los operadores, ya sea debido a una errónea configuración de la red, a la ausencia de políticas de segmentación y control de acceso a los activos, o, por ejemplo, a la ausencia de cifrado en interfaces muy expuestos.

b) Integridad: La integridad es la capacidad de garantizar que los datos de un activo/usuario/red durante su ciclo de vida, ya sea en tránsito o almacenados, mantienen su autenticidad y son modificados sólo por los agentes autorizados a ello, evitando que fuentes no deseadas puedan cambiar o manipular dichos datos. Algunas medidas para garantizar la integridad pueden ser la segmentación y el control de acceso, la comprobación del hash en los paquetes, la verificación de integridad de las versiones a instalar o almacenadas, etc.

   Ejemplos de riesgos que comprometan la integridad son: Manipulación del tráfico/datos (en tránsito o almacenado) en muy interfaces expuestas de la red 5G.

c) Disponibilidad: La disponibilidad se basa en el principio de garantizar que los usuarios legítimos tengan acceso ininterrumpido a los servicios y datos dentro del entorno para su correcto funcionamiento. Este concepto pretende juzgar la importancia del activo y su solución en la continuidad de negocio de un determinado servicio, recurso o infraestructura. El nivel de afectación a la disponibilidad que tiene un riesgo se suele anclar al número y al tipo de usuarios afectados que supondría la caída del servicio por dicho ataque.

   Para garantizar la disponibilidad se pueden tomar diversas medidas entre las que están la creación de soluciones de backup, la redundancia/resiliencia de los activos, la capacidad de mitigación frente a ataques DDoS, o los procedimientos eficaces de restauración del servicio tras la caída.

   Dentro del entorno, algunos riesgos que puedan comprometer la disponibilidad son los siguientes: Ataques como, por ejemplo, denegación de servicio a la función de red, a la infraestructura de virtualización, o la infraestructura física, o catástrofes naturales, terrorismo, etc.

3. Determinación de la criticidad de los activos.

Se procede, en este apartado, a identificar la criticidad de los activos de una red 5G-SA identificados, teniendo en cuenta los factores y conceptos clave (triada CIA) descritos en el apartado anterior.

a) Red de acceso.

- **gNB**: Criticidad media

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Red de acceso	gNB	2 - Media	2 - Media	1 - Baja	**2 – Media**

Los nodos de acceso radio se encuentran ubicados, en su gran mayoría, en emplazamientos en lugares públicos no seguros. Esto hace que su exposición a ataques in situ aumente. La afectación de una celda puede suponer la interrupción de servicio en un área reducida, afectando a una cantidad de usuarios pequeña, además de poder ser soportado su tráfico por alguna otra estación base cercana, por lo que se considera que la criticidad es **baja** en cuanto a **disponibilidad**.

Estos nodos no almacenan datos de usuario. A pesar de ello, si se produce un ataque *Man in the Middle* (*MitM*), podría verse comprometido el tráfico no cifrado (afectando sólo a los pocos usuarios conectados a ese nodo), además de poder manipular los paquetes en curso si no existe verificación de integridad. Debido a la dificultad de realizar este ataque en el escenario descrito, a la **confidencialidad** y la **integridad** se le otorga una criticidad **media**.

b) Núcleo de red.

- **AUSF, UDM y UDR:** Criticidad alta

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Núcleo de red	UDM	3 - Alta	3 - Alta	3 - Alta	3 – Alta
		UDR	3 - Alta	3 - Alta	3 - Alta	3 – Alta
		AUSF	3 - Alta	3 - Alta	3 - Alta	3 – Alta

Un atentado contra la confidencialidad/integridad en estos activos puede suponer la exposición de información crítica del usuario en la red (claves de autenticación, integridad y cifrado, datos de provisión de los usuarios y sus identidades, etc.).

La obtención de esta información tendría un impacto muy alto debido a que es información asociada directamente a la tarjeta SIM de los clientes, y su exfiltración puede conllevar no sólo a una exposición de las comunicaciones de los usuarios, sino también a la pérdida de imagen del operador de redes y servicios 5G, y puede implicar la sustitución de las tarjetas SIM comprometidas. Por dichos motivos, la criticidad del activo en lo que a **confidencialidad** e **integridad** se refiere es **alta**.

Además, al ser un elemento centralizado que recibe las peticiones de autenticación de todos los usuarios de la red, en caso de no desplegarse con una solución correcta que garantice su resiliencia y continuidad de negocio, una disrupción en el mismo puede provocar la caída completa de la red. Por tanto, en cuanto a **disponibilidad**, también tiene una criticidad **alta**.

- **AMF**, **NRF** y **NEF**: Criticidad media

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Núcleo de red	AMF	3 - Alta	2 - Media	2 - Media	2 – Media
		NRF	3 - Alta	3 - Alta	1 - Baja	2 – Media
		NEF	2 - Media	2 - Media	1 - Baja	2 – Media

  - **NRF**: Criticidad media

    Este elemento dispone de un mapa de toda la red, nodos y servicios. Un acceso no autorizado puede dar el detalle del despliegue de la red, los enrutamientos, DNNs, *slices*, servicios, etc. Además, la

alteración de su configuración puede provocar errores de comunicaciones internas en la red. Dadas estas razones, la **confidencialidad** e **integridad** del NRF se consideran de criticidad **alta**.

Sin embargo, el hecho de poder configurar el servicio para que, en caso de caída del elemento, exista continuidad del servicio de forma temporal entre las funciones de red, hace que su **criticidad** en cuanto a disponibilidad sea **baja**.

- **AMF**: Criticidad media

  Al ser el encargado de gestionar la movilidad de los usuarios, un ataque o acceso no autorizado puede permitir obtener o exfiltrar información delicada (identidades del usuario, localización a nivel de *Tracking Area*, e incluso el identificador del nodo donde se encuentra el cliente cuando el terminal está en modo conectado).

  Por este motivo, riesgos de exfiltración más que de alteración de información, se considera **alta** la criticidad en cuanto a **confidencialidad**, y **media** en cuanto a **integridad**.

  Por otra parte, dado que únicamente atiende a una parte de los usuarios de la red, se considera que la criticidad en cuanto a **disponibilidad** es **media**.

- **NEF**: Criticidad media/baja

  Este elemento es el responsable de garantizar la autenticación, confidencialidad e integridad de las comunicaciones de entidades externas al Núcleo de red, contra alguna de las funciones internas del Núcleo de red (interfaz *SBI*). Un acceso no autorizado, puede permitir la modificación de alguna política de seguridad entre las funciones externas al Núcleo de red y las internas. Sin embargo, esta función de red no se utiliza para la prestación de servicio generalista

a los usuarios 5G. Por ese motivo, la **confidencialidad** e **integridad** tienen una valoración **media**.

Si atendemos a la **disponibilidad**, la caída de este equipo, en caso de no tener redundancia, sólo afectaría a aquellos servicios que necesiten comunicación externa con los elementos del Núcleo de red, lo que no tendría una afectación considerable y por eso se considera **baja**.

- **SMF/UPF** y **PCF**: Criticidad baja

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Núcleo de red	SMF/UPF	1 - Baja	1 - Baja	1 - Baja	1 - Baja
		PCF	1 - Baja	1 - Baja	1 - Baja	1 - Baja

En esta categoría se agrupan los siguientes elementos, en los que, en general, una afectación a los mismos no tiene un impacto notable en la prestación del servicio 5G, por lo que su valoración de criticidad es baja.

- **SMF/UPF**: Criticidad baja

  El SMF se encarga del establecimiento de las sesiones, y el UPF se encarga de la gestión del plano de usuario: desencapsula el tráfico del usuario que llega del acceso radio y lo encamina a otras redes de datos. Un acceso no autorizado puede desactivar la sesión de un usuario, pero se establecería en otro SMF/UPF. Además, el uso del SecGW entre la Red de acceso y el Núcleo de red imposibilita un *MiTM*, lo que hace que su criticidad atendiendo a la **confidencialidad** e **integridad** sea **baja**.

  Por otra parte, atendiendo a la **disponibilidad**, su criticidad se considera **baja** igualmente, debido a que un usuario no puede estar más que en un AMF, pero sus sesiones sí pueden estar en diversos SMF/UPF.

- **PCF**: Criticidad baja

  Este elemento no es especialmente crítico para los servicios de datos. Aunque dispone de las políticas relacionadas con los servicios y la tarificación, los AMF/SMF siempre son configurados para poder dar servicio sin este elemento. Un efecto normal de caída de PCF en servicio de datos es no poder tarificar online a los clientes. La eventual afectación sobre el servicio de voz puede mitigarse mediante servicio de voz por 2G/3G. Por dichos motivos, su criticidad atendiendo a los **diferentes criterios** sería **baja**.

c) Transporte – Backhaul.

- **SecGW**: Criticidad media

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Transporte - Backhaul	SecGW	3 - Alta	2 - Media	2 - Media	**2 - Media**

La red de transporte conecta los elementos del Núcleo con los de la Red de acceso. Un posible corte de esta en uno de sus tramos hace que solamente la zona de nodos de acceso radio en la que se produce dicho corte se vea afectada y, de forma temporal, se puede forzar a que el tráfico no pase por este elemento en dicha zona, con lo que la **disponibilidad** tiene una criticidad **media**.

Por otro lado, comprometer un sitio o interceptar el tráfico conlleva a una fuga de información importante, dado que es el elemento encargado de cifrar la información en tránsito que llega desde una gran cantidad de nodos. Por ello, atendiendo a la **confidencialidad** se le asigna una criticidad **alta**. Estando cifrada esta comunicación, alterarla es complicado, por lo que la criticidad en cuanto a **integridad** se considera **media**.

d) Interconexión Roaming.

- **SEPP**: Criticidad media

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Interconexión Roaming	SEPP	3 - Alta	2 - Media	2 - Media	2 – Media

Este elemento permite el intercambio de señalización con otras redes en escenarios de itinerancia. Pese a ser un elemento expuesto a otras redes, únicamente transporta tráfico de usuarios de roaming, y no el de los usuarios nacionales. Este hecho hace que la criticidad en cuanto a **disponibilidad** sea **media**.

Por otra parte, la confidencialidad de las comunicaciones y su integridad sí son aspectos importantes (sobre todo la primera), pues es un entorno en el que, en caso de carecer de las protecciones adecuadas, se puede obtener o exfiltrar información sensible de los usuarios, incluso de aquellos que no están en Roaming. Esto hace que la criticidad en cuanto a **confidencialidad** sea **alta**.

Es un entorno que la industria y los organismos de estandarización se ha tomado muy en serio, donde, de manera nativa, los fabricantes van a incluir capacidades de configuración de cifrado e integridad, lo que permite que, si el tráfico va cifrado, atentar contra la **integridad** sea más complicado. Por todo ello, se le otorga una criticidad **media**.

e) Sistemas de control y gestión y servicios de soporte.

- **GER**: Criticidad media

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Sistemas de gestión/operación y servicios de soporte	GER	3 - Alta	3 - Alta	1 - Baja	2 – Media

Estos elementos permiten una correcta operación de los elementos que conforman el entorno de red 5G. Pueden gestionar todo un entorno de red,

intercambiando mensajes de configuración que pueden dar órdenes fraudulentas a los equipos, o incluso transportar credenciales.

Por tanto, se considera que la **integridad** y **confidencialidad** de este elemento es **alta**.

Sin embargo, una interrupción o falta de comunicación con la red por parte de los Sistemas de gestión no ocasiona una caída de esta, considerando que la **disponibilidad** es de criticidad **baja**.

f) Infraestructura de virtualización /orquestación.

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Secundario	Infraestructura de virtualización/orquestación	Infraestructura de virtualización	3 - Alta	3 - Alta	3 - Alta	3 – Alta
		Gestión/orquestación de virtualización	3 - Alta	3 - Alta	1 - Baja	2 – Media

- **Infraestructura de virtualización**: Criticidad alta

  Todos los elementos del Núcleo de red 5G se encuentran desplegados sobre una Infraestructura virtualizada. Esto implica que cualquier ataque que consiga una disrupción de su funcionamiento, poder controlar los nodos de esta, interceptar el tráfico, modificar el funcionamiento, etc., puede tener graves consecuencias en la prestación del servicio, llegando a incluso su interrupción total. Por los motivos descritos, la criticidad en cuanto a **confidencialidad**, **integridad** y **disponibilidad** es **alta**, considerándose este un activo crítico dentro de la red.

- **Gestión/orquestación de la virtualización**: Criticidad media

  De forma análoga a los Sistemas de gestión/operación y servicios de soporte, lo más crítico en este activo son la **confidencialidad** e **integridad** de las comunicaciones y accesos, calificadas de criticidad **alta**, pues desde los *Orquestadores de la virtualización* se controlan todos los elementos de

la plataforma de virtualización, que podrían ser vulnerados o atentados (por ejemplo, eliminación de *CNF*, apagado de hardware, etc.).

Sin embargo, una interrupción o falta de comunicación con la red por parte del Orquestador no ocasiona una caída de las plataformas de virtualización, considerando así que la criticidad en cuanto a **disponibilidad** es **baja**.

g) Infraestructura física.

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	**Dominio**	**Activo**	**C**	**I**	**A**	
Secundario	Infraestructura Física	Infraestructura Física	1 - Baja	1 - Baja	3 - Alta	**2 – Media**

- **Infraestructura física**: Criticidad media

  La Infraestructura física es especialmente vulnerable a los ataques que provocan daños físicos en el equipamiento, robo, cortes de energía, etc. La disponibilidad de esta es fundamental para el funcionamiento de las redes y los servicios, ya que se va a utilizar de base para ubicar muchas funciones de red y Sistemas de gestión de toda la red, por lo que el valor de criticidad, en cuanto a **disponibilidad**, es **alto**.

  La **confidencialidad** e **integridad** de este activo se consideran **bajas**, dado que no representa un riesgo para la información o las comunicaciones en sí misma, dependiendo fundamentalmente de los protocolos y mecanismos de control lógicos implementados en las capas superiores (Infraestructura de virtualización, aplicaciones, etc.) con objeto de evitar la obtención de información si alguien se hace con un activo.

Cuadro resumen: tabla de criticidad de activos

Descripción del activo			Evaluación CIA			Criticidad
Entorno de red	Dominio	Activo	C	I	A	
Primario	Red de acceso	gNB	2 - Media	2 - Media	1 - Baja	2 - Media
	Núcleo de red	AMF	3 - Alta	2 - Media	2 - Media	2 - Media
		SMF/UPF	1 - Baja	1 - Baja	1 - Baja	1 - Baja
		PCF	1 - Baja	1 - Baja	1 - Baja	1 - Baja
		UDM	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		UDR	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		AUSF	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		NRF	3 - Alta	3 - Alta	1 - Baja	2 - Media
		NEF	2 - Media	2 - Media	1 - Baja	2 - Media
	Transporte - Backhaul	SecGW	3 - Alta	2 - Media	2 - Media	2 - Media
	Interconexión Roaming	SEPP	3 - Alta	2 - Media	2 - Media	2 - Media
	Sistemas de gestión/operación y servicios de soporte	GER	3 - Alta	3 - Alta	1 - Baja	2 - Media
Secundario	Infraestructura de virtualización/orquestación	Infraestructura de virtualización	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		Gestión/orquestación de virtualización	3 - Alta	3 - Alta	1 - Baja	2 - Media
	Infraestructura Física	Infraestructura Física	1 - Baja	1 - Baja	3 - Alta	2 - Media

4. Clasificación de activos en función de la criticidad.

En base a los análisis anteriores y a las aportaciones realizadas por los operadores de redes y servicios 5G, se ha identificado un conjunto de elementos calificándolos con importancia crítica para la operación de las redes 5G, para su configuración o gestión, o de los servicios prestados por las mismas.

Tal y como se ha recogido en el apartado anterior, todos los activos de criticidad alta del entorno primario de red pertenecen al Núcleo de red. No obstante, desde el punto de vista de la criticidad, no es posible considerar el Núcleo de red como un bloque homogéneo. Por ello, se considera aplicable un tratamiento diferenciado en relación a las medidas conducentes a garantizar la disponibilidad de los servicios que ofrecen.

Así pues, el Núcleo de red está compuesto de diversas funciones de red (o Network Functions, NF) que se despliegan en Infraestructuras virtualizadas independientes de la propia función de red. La clasificación considera cuáles de estas entidades son más críticas no sólo desde el punto de vista

de redundancia, sino también del posible impacto de accesos no autorizados o ataques desde otras redes.

Además, se tiene en cuenta los posibles accesos no autorizados a la Infraestructura virtualizada sobre la que se despliegan estas funciones de red, y se establece una importancia relativa entre las distintas entidades, recalcando que, para obtener un servicio completo, todas ellas son necesarias.

a) Criticidad alta

El riesgo que más comprometería el servicio 5G sería un acceso no autorizado al entorno AUSF/UDM/UDR. En el AUSF están las claves de autenticación que permiten el acceso a cualquier comunicación radio cifrada, y en el UDM/UDR se encuentran todos los datos de provisión de los usuarios y sus identidades, y precisamente el 3GPP ha incluido el uso del SUCI (identidad IMSI cifrada) para evitar que esa identidad viaje por el interfaz radio, ya que disponer del SUPI de un usuario es el primer paso para cualquier otro ataque. Se considera sin duda que estas son las funciones de red más críticas dado que el impacto de obtener las claves y las entidades es duradero (al estar asociado a las claves de la SIM de los clientes). La pérdida de imagen de un operador de redes y servicios 5G ante una intrusión en estas funciones de red sería enorme y podría implicar la sustitución de las SIMs comprometidas. No obstante, el diseño de red permite proveer servicio sin ningún impacto ante fallo doble de instancias de cualquiera de estos nodos.

b) Criticidad media

En esta categoría, de mayor a menor criticidad, se incluye.

i. NRF: este elemento dispone de un mapa de toda la red, nodos y servicios. Con la información del NRF se dispone de todo el detalle del despliegue de la red, enrutamientos, DNNs, slices, servicios, etc. Además, un acceso no autorizado permitiría paralizar el servicio 5G ya que todas las funciones de red consultan a esta entidad para conocer las funciones de red destino que dispone del servicio requerido. No obstante, las funciones de red tienen cacheada la información de NRF, lo que permitiría mitigar temporalmente el ataque. A

mayores, el diseño de red permite proveer el servicio sin ningún impacto ante fallo doble de instancias de este nodo.

ii. SEPP: permite el intercambio de señalización con otras redes para escenarios de itinerancia en la red propia, o en la de otras redes de terceros. Es un elemento expuesto, aunque los suministradores 5G han desarrollado un número elevado de funcionalidades para garantizar su seguridad e integridad. Adicionalmente, ha de garantizarse el aislamiento entre los dominios internos y externos.

iii. AMF: es el encargado de la gestión de la movilidad. Un ataque o acceso no autorizado al mismo, permitiría obtener información muy delicada (identidad del usuario, localización a nivel Tracking Area, e incluso gNB-id donde se encuentra el cliente cuando su terminal está en modo connected), con posibilidad de rastrear el movimiento de usuarios, y sus procedimientos de señalización relacionados con la movilidad y gestión de sesiones. Estos elementos se despliegan en modo pool y se dimensionan para soportar de forma simultánea fallo de un nodo de cada pool.

c) Criticidad baja

En esta categoría, nuevamente, de mayor a menor criticidad, se indica:

i. SMF/UPF: SMF se encarga de la gestión de las sesiones (establecimiento, modificación y liberación), la gestión y asignación de IP a los terminales de los usuarios, etc. También es responsable de interactuar con el plano de usuario creando, actualizando o borrando sesiones PDU, así como de administrar el contexto de la sesión con el UPF, mientras que el UPF gestiona el plano de usuario. Estos elementos están mucho más redundados que los AMFs anteriormente descritos, y un acceso no autorizado podría desactivar la sesión de un usuario, aunque esta se establecería en otro SMF/UPF. El plano de usuario o tráfico real de clientes, se encamina, en general a otras redes (internet/intranet) que son de seguridad más baja, por lo que un atacante de plano de usuario tiene más fácil comprometer el servicio atacando el servidor destino o incluso el terminal.

ii. PCF: no es especialmente crítico, ya que los AMF/SMF se configuran para poder dar servicio sin este elemento, afectando, eventualmente, a la tarificación online de los clientes.

d) No críticos

Los elementos CHF, NEF, NWADF y 5G-EIR no se consideran críticos para prestación del servicio 5G debido a que, en caso de caída o indisponibilidad parcial o total de cualquiera de ellos, los clientes no deberían verse afectados en el servicio.

5. Identificación de amenazas y riegos en la tecnología 5G.

En el artículo 9 del Real Decreto-ley 7/2022, de 29 de marzo, se especifica la necesidad de identificar los factores de riesgo a analizar en función de la evolución tecnológica, la incorporación de nuevos avances, funcionalidades y estándares tecnológicos, la situación del mercado de comunicaciones electrónicas y del de suministros y de la aparición de nuevas amenazas y vulnerabilidades.

Los siguientes apartados recogen las tareas realizadas.

5.1. Criterio de identificación del riesgo de un ataque

Para calcular el nivel de riesgo de seguridad que introduce una amenaza, utilizamos tres factores atendiendo a las siguientes fórmulas:

Nivel de riesgo = (Probabilidad de ocurrencia) x (Impacto en la red)

donde, a su vez,

(Impacto en la red) = (Criticidad del activo) x (Factor de escalado)

Se define, seguidamente, los conceptos empleados:

a) Probabilidad de ocurrencia: Se realiza una valoración en base a los siguientes parámetros:

i. *Grado de exposición del activo a la vulnerabilidad*: da una medida de lo expuesto que se encuentra el elemento analizado a nivel físico o lógico, y el nivel de accesibilidad/facilidad que pueda tener el atacante de cara a ejecutar la amenaza.
ii. *Complejidad o conocimientos para desarrollar el ataque*: la probabilidad de ocurrencia aumenta en el caso de que el ataque se pueda realizar sin muchos conocimientos técnicos y el entorno de ataque sea sencillo de implementar o se usen herramientas automatizadas.
iii. *Conocimiento público de la vulnerabilidad*: un ataque es más probable cuanto más conocido es a nivel de comunidad. En el caso de que la vulnerabilidad esté poco difundida o se maneje solamente en ciertos círculos (como por ejemplo suministradores 5G u operadores de redes y servicios 5G), su explotación será menos probable.
iv. *Rastro que deja el ataque*: en caso de que el ataque se realice por fuerza bruta o dejando trazabilidad en las redes, será menor la probabilidad de que existan atacantes dispuestos a aprovechar la vulnerabilidad. Se trata de casos en los cuales no pueda realizarse suplantación de identidad.
v. *Beneficio obtenido con el éxito del ataque*: valor económico, reconocimiento, relevancia, etc., de la consecución del ataque.

Los posibles valores de la ***probabilidad de ocurrencia*** son **Muy Alto**, **Alto**, **Medio**, **Bajo**.

b) Impacto en la red: de forma similar a la *probabilidad de ocurrencia*, se utiliza una valoración cualitativa para medir el impacto que podría tener el ataque en la red.

Para evaluar el servicio y dar una valoración del impacto se utilizan los siguientes parámetros:

i. *Criticidad del activo*: concepto mencionado anteriormente, que engloba la *confidencialidad*, la *integridad* y la *disponibilidad*.

ii. *Factor de escalado*: identifica la importancia y/o alcance del ataque a nivel de afectación de la red. Toma en consideración tanto el alcance (número de usuarios que pueden ser impactados), como el tipo de impacto del ataque (fuga de credenciales, disminución de disponibilidad, etc.).

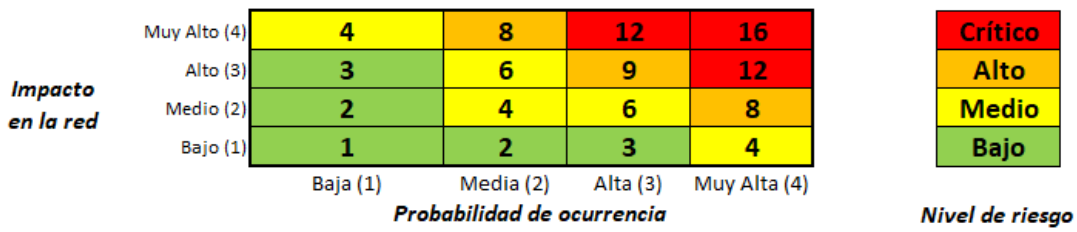
Los posibles valores del Impacto en red del ataque son: **Muy Alto**, **Alto**, **Medio**, **Bajo**, teniendo en cuenta los criterios anteriores.

c) Nivel de riesgo: Es el resultado de las dos variables anteriores siguiendo la fórmula descrita arriba.

Los posibles valores del nivel de riesgo son: **Crítico**, **Alto**, **Medio**, **Bajo**.

5.2. Matriz de riesgos

Atendiendo a las consideraciones del apartado anterior, se presenta la matriz genérica que caracteriza los niveles de riesgo que se analizan posteriormente en este documento.



6. Amenazas o riesgos en una red 5G SA.

Una vez identificados los activos y caracterizada su criticidad, el siguiente paso en el análisis de riesgos es evaluar las amenazas o posibles ataques a las que están expuestos cada uno de estos activos de red 5G SA.

Es importante destacar que una misma amenaza puede tener distinto nivel de riesgo en función del activo o entorno sobre el que se evalúe, de cara a establecer las prioridades correctas de acciones mitigadoras que permitan incrementar, en una misma línea temporal, la seguridad de la solución de la manera más eficiente posible.

A continuación, se detallan las amenazas o riesgos en una red 5G SA:

a) Actividades maliciosas debidas a accesos indebidos o maliciosos a la gestión, extracción de información sensible o modificación no autorizada de parametrización que provoque la indisponibilidad del elemento.

   Se trata de aquellas acciones llevadas a cabo por atacantes internos o externos que van dirigidas a los elementos o funciones de red e infraestructura con la intención de robar información, alterarla o destruir, mediante configuración, un objetivo específico.

   En este bloque se engloban, entre otras, las siguientes amenazas:

   i. Intrusiones en la red con el objetivo de obtener información, a través de accesos maliciosos, movimientos laterales, escalado de privilegios, por falta de políticas de seguridad robustas (ausencia de control de acceso, autenticación, autorización, segmentación, hardening, etc). Destaca, entre otros la obtención de credenciales de usuarios operadores, información sensible de clientes (datos, identificadores de usuario, claves de autenticación, cifrado e integridad), o información útil de configuración de red

(puertos, versiones, etc.) que sirva como vector de información adicional para realizar ataques de mayor impacto.

ii. Modificación malintencionada y no autorizada de parametrización o configuración de red que pueda provocar indisponibilidad parcial o total del servicio en el activo o la red, así como favorecer la exfiltración de tráfico comentada en el punto anterior.

A. Manipulación de configuración o parametrización que afecte al funcionamiento del equipo (políticas de enrutamiento de tráfico, configuración de DNS, sesiones de usuario, imágenes de funciones de red virtuales, etc.)
B. Manipulación de configuración de seguridad del equipo (políticas de seguridad, servicios ofrecidos en el aplicativo y sistema operativo, algoritmos criptográficos, reglas de acceso) y creación de puertas traseras.
C. Ejecución de forma intencionada o inconsciente de software/código malicioso (SQL,XSS injection, rootkits, malware/ransomware, etc.)

iii. Explotación de vulnerabilidades en hardware o software, que permitan un acceso simple y eficaz para poder ejecutar las amenazas comentadas en los dos puntos anteriores (vulnerabilidades conocidas/ CVEs, nuevas vulnerabilidades y de zero-day).

b) Compromiso de las comunicaciones o datos de usuario a través de la captura, interceptación, secuestro de tráfico de servicio o su modificación:

Esta categoría recoge las acciones realizadas para espiar, interrumpir o alterar las comunicaciones o datos de usuario en el plano de servicio, sin su consentimiento.

Las principales amenazas dentro de esta categoría serían:

i. Espionaje de comunicaciones de un determinado usuario en entornos con alto nivel de exposición como es el caso del acceso radio o la interconexión de Roaming.

ii. Obtención de información sensible de los usuarios (identificadores de usuario, localización, servicios, etc) en interfaces expuestos que puedan ser utilizados como vectores de información para realizar ataques de mayor impacto.

iii. Manipulación de las comunicaciones en interfaces expuestos a través de actividades Man in The Middle (MiTM) y/o de los datos de usuario, siendo posible provocar acciones ilegales tales como fraude, suplantación de identidad, etc.

c) Denegación de Servicio (DoS).

Esta categoría recoge aquellas acciones, actividades o incidencias malintencionadas o no que puedan provocar una disrupción total o parcial en el equipo, causando una afectación a los usuarios de la red. Las principales amenazas dentro de esta categoría serían:

i. Ataques volumétricos de denegación de servicio (DoS/DDoS): Inundación de tráfico a las interfaces expuestas de los activos (dispositivos de usuario, interconexiones, etc.) buscando la sobrecarga de las capacidades de los elementos, con el objetivo de provocar un malfuncionamiento/disrupción en la red.

ii. Ataques dirigidos a usuarios específicos con el objetivo de provocar su indisponibilidad en la red (por ejemplo, ataques de interferencia o desregistro de la red).

iii. Daños no intencionados por los operadores por errores de configuración: Recoge las acciones no intencionadas por parte de un operador con acceso a la gestión de un activo que puedan resultar en un fallo o la reducción de funcionalidad de este, como, por ejemplo, la configuración pobre/errónea de los activos de red y sus capacidades de seguridad (aislamiento, bastionado, segmentación, etc.) o error en su gestión o manipulación por desconocimiento o falta de formación o diligencia.

iv. Mal funcionamiento del elemento: Engloba el malfuncionamiento “nativo” (por causas ajenas a la configuración del activo) que pueda provocar una disrupción total o parcial de su servicio.

d) Amenazas físicas.

Está dirigido a destruir, inutilizar, alterar o robar activos físicos de la infraestructura física que alberga la funciones/elementos de red.

Entre las amenazas principales destacan el sabotaje o terrorismo contra los elementos críticos de equipamiento de red, las catástrofes naturales, el malfuncionamiento de la red de energía y la posible sustracción de equipamiento de red para la extracción de información sensible y su posterior explotación.

e) Escasa formación y concienciación de los empleados en materia de ciberseguridad, así como mala praxis en la gestión de la evolución de los riesgos identificados.

Por un lado, el hecho de que los empleados no estén concienciados en materia de seguridad aumenta la probabilidad de ocurrencia de incidentes tales como ataques ransomware y otro tipo de malware. La falta de formación en materia de seguridad y operación aumenta la probabilidad de errores de configuración por desconocimiento que expongan los activos a riesgos innecesarios.

Además de todo esto, si no se lleva a cabo un buen procedimiento de gestión de riesgos, controlando su evolución en la red, será imposible plantear un plan de prioridades y ejecutar las medidas de seguridad de manera eficiente.

ANEXO III

GESTIÓN DE RIESGOS A NIVEL NACIONAL

Una vez identificadas en el anexo II las distintas amenazas que afectan pormenorizadamente a las redes y servicios 5G, y con ello, la situación inicial de riesgo, la siguiente fase es prever aquellas medidas de seguridad necesarias para solventar, disminuir o paliar los riesgos identificados.

Estas medidas son:

1. Medidas de seguridad genéricas:

1.1. Configuraciones de seguridad para el equipamiento:

1.1.1. Configuraciones relacionadas con la identificación, autenticación, control, auditoría y monitorización en el acceso a los nodos. Los nodos deben ser configurados con:

a) Políticas de gestión de identidad, permitiendo garantizar tanto la autenticación (verificar que quién accede es quién dice ser), como la autorización (acceder solo con los privilegios que sean estrictamente necesarios) cuando se accede a los nodos.
b) Políticas de gestión del ciclo de vida del usuario.
c) Capacidades de trazabilidad y políticas de auditoría, permitiendo que quede registrado todos los accesos (quién y cuándo se conecta y desconecta de los nodos), así como los comandos ejecutados y las alarmas que identifican un posible fallo en el equipo.
d) Buenas prácticas de seguridad cuando se definen y gestionan las credenciales y accesos de los usuarios, siempre forzando que las credenciales sean robustas.
e) Capacidad de ser configurados de tal manera que no den información detallada en el caso que falle el acceso y se establezcan políticas de bloqueo que dificulten la obtención de credenciales.

1.1.2. Bastionado:

a) Autoprotección de los nodos, asegurándose que solo estén activos los servicios necesarios para su correcto funcionamiento.
b) Los nodos deben tener la capacidad de separar el interfaz de gestión del de servicio, ya sea a través de un interfaz físico o lógico.
c) Los nodos deben ser capaces de detectar y manejar los paquetes malformados manteniendo los servicios sin afectación.
d) Los nodos deben ser capaces de hacer frente a altos volúmenes/picos de tráfico teniendo mecanismos de autorregulación para evitar el colapso de su CPU.
e) Capacidad de proteger los datos e información almacenados.
f) Los nodos/elementos de la red deben estar configurados de manera que no se permita iniciar a través de dispositivos de memoria no autorizados.
g) Los nodos deben configurarse de manera que no se pueda realizar una explotación maliciosa de las APIs que expongan.

1.1.3. Realización de pruebas de seguridad periódicas. Son necesarias para estudiar si han aparecido nuevas vulnerabilidades para los componentes del activo.

1.2. Seguridad de arquitectural y funcional.

1.2.1. Planos de red diferentes, así como áreas o ambientes de red con distinto nivel de exposición, deben ser aislados.

1.2.2. Control de flujo: Capacidad de limitar el tráfico a ciertas direcciones IPs, Protocolos, Aplicaciones, para evitar sobrecargar el enlace haciendo que un ataque sea más complicado de llevar a cabo.

1.3. Medidas de Seguridad en la Infraestructura Física:

a) Registro, validación y control de las autorizaciones de acceso físico a los emplazamientos.

b) Controles de accesos físicos, mediante medios electrónicos y/o mecánicos, a las centrales de red y edificios relevantes.

c) Vigilancia física y seguridad electrónica del emplazamiento.

d) Sistemas de seguridad electrónicos instalados y mantenidos.

1.4. Concienciación de seguridad hacia los empleados y la cadena de mando.

1.5. Formación de empleados en tecnología, seguridad y procesos.

1.6. Implementación de procesos claros de gestión de incidentes, teniendo un registro del histórico de incidentes propios y actualizado el conocimiento con los incidentes de la industria.

2. Medidas de seguridad específicas relacionadas con una red 5G.

2.1. Control de software:

a) Garantizar la integridad de la actualización del software antes de ser instalada, evitando la inyección de códigos maliciosos, troyanos o versiones no legítimas (manipuladas por un tercero).
b) Garantizar que no existan puertas traseras.
c) Garantizar que no existan vulnerabilidades (CVE) conocidas de riesgo alto en el momento de despliegue del producto en planta.
d) Cumplimiento con certificaciones de seguridad reconocidas internacionalmente para los equipos.

2.2. Debe configurarse cifrado e integridad de las comunicaciones entre el terminal y la red a ambos niveles AS (Access Stratum)/NAS (Non Access Stratum), para proteger la privacidad del usuario en el interfaz aire. Esta medida se activa tanto en la RAN (AS), como en el Núcleo de Red (NAS).

2.3. Debe configurarse cifrado e integridad de las comunicaciones en el plano de control y en el plano de usuario entre el nodo de acceso radio (RAN) y el Núcleo de Red.

2.4. La privacidad de los usuarios debe ser garantizada en el interfaz aire.

2.5. Deben ser corroboradas las mejoras en los algoritmos de autenticación entre el terminal del usuario y la red que vienen de manera nativa con la tecnología 5G SA.

2.6. Mejoras nativas en los algoritmos de autenticación entre el dispositivo del usuario y la red, para garantizar mutuamente que la comunicación es legítima.

2.7. Los diferentes elementos que manejan el tráfico de señalización deben tener medidas para evitar la suplantación de los propios elementos de red en la red de roaming, así como la de los usuarios que no están en roaming.

2.8. La confidencialidad, integridad y autenticación deben ser garantizadas en las comunicaciones entre un operador origen y destino, usando protocolos/equipamiento/soluciones seguras (SEPP).

2.9. Es necesario establecer las políticas de seguridad correspondientes de cara a exponer en la interconexión únicamente los interfaces y mensajes necesarios para el servicio, evitando dar información innecesaria que pueda ser utilizada de forma fraudulenta.

2.10. Aislamiento de funciones de red virtualizadas: Clasificación de los diferentes elementos virtualizados en la infraestructura de acuerdo con diferentes niveles de exposición y la criticidad del elemento.

2.11. Aislamiento de tráficos: Diseño seguro de la arquitectura de virtualización para garantizar el tráfico necesario para el funcionamiento de la capa de virtualización, de esta forma la operación/funcionamiento de la red será garantizado.

2.12. Es necesario seguir las pautas de los Requisitos/Configuraciones de Seguridad del Equipamiento y Seguridad Arquitectural para todos y cada uno de los elementos que componen la arquitectura de virtualización.

2.13. Monitorización y Detección: Monitorización de la trazabilidad de accesos y comandos ejecutados en los elementos críticos de la red, de cara a poder identificar actividades ilegítimas en el momento de su realización y también de cara al análisis forense de posibles ataques.

2.14. Mitigación: Capacidades que permitan mitigar posibles ataques volumétricos que tengan como objetivo la denegación de servicio en los interfaces muy expuestos.

2.15. Entornos críticos: Las pruebas de funcionamiento de redundancia/recuperación (backup) en entornos críticos deben llevarse a cabo antes del despliegue de la solución.