I. DISPOSICIONS GENERALS

MINISTERI PER A LA TRANSFORMACIÓ DIGITAL I DE LA FUNCIÓ PÚBLICA

8715 *Reial decret 443/2024, de 30 d'abril, pel qual s'aprova l'Esquema Nacional de Seguretat de xarxes i serveis 5G.*

Les comunicacions mòbils de cinquena generació o 5G constitueixen un nou paradigma de les comunicacions electròniques amb un gran potencial transformador en benefici de la societat i l'economia, ja que s'obre la possibilitat a la incorporació de funcionalitats noves que tenen un gran impacte, com ara la computació en la xarxa i la seva virtualització i segmentació o les seves funcions, cosa que permet la creació de xarxes virtuals, flexibles i intel·ligents, les quals ofereixen baixa latència, connectivitat ininterrompuda i la prestació de serveis d'un gran valor afegit per a la societat i l'economia en àmbits com ara la medicina, el transport, la logística i l'energia. Per tot això, la Unió Europea i Espanya, directament i a través del Mecanisme de Recuperació i Resiliència, impulsen el ràpid desplegament de xarxes 5G i la realització de projectes demostratius de la seva utilitat per a diferents sectors mitjançant la prestació de serveis 5G.

Malgrat els avantatges que aporten, la utilització de confiança de les xarxes i els serveis 5G exigeix disposar d'un nivell de protecció elevat, atès que presenten riscos específics derivats, per exemple, d'una arquitectura de xarxa més complexa, basada en serveis i distribuïda, amb una banda ampla mòbil millorada, de més capacitat, per al transport i la transmissió de grans volums de dades a alta velocitat, fiabilitat i capacitat per connectar un nombre massiu de dispositius a la xarxa o la provisió de serveis específics per a determinats usos o aplicacions. La naturalesa interconnectada de la seva infraestructura, així com el seu caràcter transnacional i la dimensió transfronterera de les amenaces, comporta que qualsevol vulnerabilitat o incident de seguretat important pugui tenir implicacions en funcions essencials per a l'economia i la societat, i fins i tot arribi a afectar la Unió Europea en conjunt.

Aquests riscos nous específics de seguretat de les comunicacions mòbils 5G es van abordar normativament a través del Reial decret llei 7/2022, de 29 de març, sobre requisits per garantir la seguretat de les xarxes i els serveis de comunicacions electròniques de cinquena generació, que incorpora en tota la seva extensió la Recomanació (UE) 2019/534, de 26 de març de 2019, de la Comissió Europea, sobre la ciberseguretat de les xarxes 5G, l'anàlisi coordinada dels estats membres i la «caixa d'eines», i s'hi van incloure les recomanacions de la Comunicació, de 29 de gener de 2020, de la Comissió Europea «Desplegament segur de la 5G a la UE - Aplicació de la caixa d'eines de la UE» (COM/2020/50 final).

El Reial decret llei 7/2022, de 29 de març, s'ha modificat recentment amb la disposició final cinquena del Reial decret llei 6/2023, de 19 de desembre, pel qual s'aproven mesures urgents per a l'execució del Pla de recuperació, transformació i resiliència en matèria de servei públic de justícia, funció pública, règim local i mecenatge, amb l'objectiu de reforçar els controls que ha d'efectuar el Govern i el Ministeri per a la Transformació Digital i de la Funció Pública sobre les condicions en què es duen a terme la instal·lació dels diferents equips, elements, funcions i sistemes propis de la tecnologia 5G, el desplegament de les xarxes 5G i la prestació de serveis de comunicacions electròniques 5G, amb la intenció d'assolir l'objectiu últim que persegueix el Reial decret llei 7/2022, de 29 de març, que, com indica l'article 1, és establir requisits de seguretat per a la instal·lació, el desplegament i l'explotació de xarxes de

comunicacions electròniques i la prestació de serveis de comunicacions electròniques i sense fil basats en la tecnologia de cinquena generació (5G).

La disposició final tercera del Reial decret llei 7/2022, de 29 de març, habilita el Govern per desplegar reglamentàriament i aprovar l'Esquema Nacional de Seguretat de xarxes i serveis 5G, cosa que s'ha de fer mitjançant un reial decret, a proposta del Ministeri per a la Transformació Digital i de la Funció Pública, amb l'informe previ del Consell de Seguretat Nacional, d'acord amb l'article 21 del Reial decret llei 7/2022, de 29 de març.

Al seu torn, els articles 20 i 5.3 del Reial decret llei 7/2022, de 29 de març, estableixen que l'Esquema Nacional de Seguretat de xarxes i serveis 5G ha de portar a terme un tractament integral i global de la seguretat de les xarxes i els serveis 5G, i a aquest efecte ha de considerar les aportacions a l'abast de cada agent de la cadena de valor de 5G per garantir un funcionament continuat i segur de la xarxa i els serveis 5G, així com la normativa, les recomanacions i els estàndards tècnics de la Unió Europea, de la Unió Internacional de Telecomunicacions (UIT) i d'altres organitzacions internacionals, amb la finalitat de garantir l'objectiu últim d'una explotació i operació segures de les xarxes i els serveis 5G al nostre país. A aquest efecte, en l'Esquema Nacional de Seguretat de xarxes i serveis 5G s'ha d'efectuar una anàlisi de riscos en l'àmbit nacional sobre la seguretat de les xarxes i els serveis 5G i s'han d'identificar, concretar i desplegar mesures en l'àmbit nacional per mitigar i gestionar els riscos analitzats.

En la cerca d'aquest tractament integral de la seguretat de les xarxes i els serveis 5G, l'Esquema Nacional de Seguretat de xarxes i serveis 5G que aprova aquest Reial decret reconeix l'existència del Centre d'Operacions de Seguretat 5G de referència, que depèn del Ministeri per a la Transformació Digital i de la Funció Pública i que s'encarrega, entre altres tasques, de contribuir i donar suport a l'exercici de les facultats del Ministeri per a la Transformació Digital i de la Funció Pública, i se li assignen en aquest àmbit funcions per proporcionar suport operatiu als subjectes obligats en activitats vinculades a la prevenció, protecció, detecció i resposta davant d'amenaces, incidents i ciberatacs als sistemes, les xarxes i els serveis 5G, així com en la certificació i normalització d'aquests.

Per complir el manament que preveu l'article 21 i la disposició final tercera del Reial decret llei 7/2022, de 29 de març, aquesta norma aprova l'Esquema Nacional de Seguretat de xarxes i serveis 5G.

Es compleix el principi de necessitat, ja que aquest Reial decret es dicta per garantir un bé d'interès general, com és la seguretat i confiança en les comunicacions electròniques. És de conformitat amb el principi de proporcionalitat, ja que les mesures són adequades als riscos identificats en cada cas. S'ajusta al principi de seguretat jurídica perquè es reconeix el marc normatiu vigent en matèria de seguretat i només s'afegeixen requisits i controls adequats a la singularitat de les xarxes i els serveis 5G i els seus riscos. Es respecta el principi de transparència, ja que els interessats han pogut participar en el procediment d'elaboració de la norma. Finalment, compleix el principi d'eficiència, ja que s'han limitat les càrregues administratives al mínim imprescindible per aconseguir la finalitat perseguida de garantir la seguretat de les xarxes i els serveis 5G.

Aquest Reial decret s'ha sotmès al procediment d'informació en matèria de normes i reglamentacions tècniques i de reglaments relatius als serveis de la societat de la informació que preveu la Directiva (UE) 2015/1535 del Parlament Europeu i del Consell, de 9 de setembre de 2015, per la qual s'estableix un procediment d'informació en matèria de reglamentacions tècniques i de regles relatives als serveis de la societat de la informació.

Aquest Reial decret es dicta a l'empara del que disposen l'article 149.1.21a i l'article 149.1.29a de la Constitució, que atribueixen a l'Estat, respectivament, la competència exclusiva en matèria de règim general de telecomunicacions i en matèria de seguretat pública.

En la tramitació d'aquest Reial decret, el Consell de Seguretat Nacional ha emès un informe.

En virtut d'això, a proposta del ministre per a la Transformació Digital i de la Funció Pública, d'acord amb el Consell d'Estat, i amb la deliberació prèvia del Consell de Ministres en la reunió del dia 30 d'abril de 2024,

DISPOSO:

Article únic. *Aprovació de l'Esquema Nacional de Seguretat de les xarxes i els serveis 5G.*

S'aprova l'Esquema Nacional de Seguretat de les xarxes i els serveis 5G, que s'insereix a continuació.

Disposició addicional primera. *Revisió de l'Esquema Nacional de Seguretat de les xarxes i els serveis 5G.*

El Govern, mitjançant un reial decret, a proposta del Ministeri per a la Transformació Digital i de la Funció Pública, amb l'informe previ del Consell de Seguretat Nacional, ha de revisar l'Esquema Nacional de Seguretat de xarxes i serveis 5G quan les circumstàncies ho aconsellin i, en qualsevol cas, cada quatre anys.

Disposició addicional segona. *Aplicació del Reial decret llei 7/2022, de 29 de març, i l'Esquema Nacional de Seguretat de les xarxes i els serveis 5G a les successives generacions de comunicacions electròniques.*

El Reial decret llei 7/2022, de 29 de març, sobre requisits per garantir la seguretat de les xarxes i els serveis de comunicacions electròniques de cinquena generació, i l'Esquema Nacional de Seguretat de les xarxes i els serveis 5G que s'aprova són aplicables a generacions de comunicacions electròniques posteriors a la cinquena generació mentre no hi hagi una norma específica per a aquestes.

Disposició addicional tercera. *El Centre d'Operacions de Seguretat 5G de referència en el marc del Pla de recuperació, transformació i resiliència.*

La creació del Centre d'Operacions de Seguretat 5G de referència per l'article 41 de l'Esquema Nacional de Seguretat de les xarxes i els serveis 5G contribueix al compliment de les fites CID# 243 i 244 del component 15, inversió 6 (C15.I6) del Pla de recuperació, transformació i resiliència.

Disposició final primera. *Títol competencial.*

Aquest Reial decret i l'esquema que aprova es dicten a l'empara del que preveuen l'article 149.1.21a i l'article 149.1.29a de la Constitució, que atribueixen a l'Estat, respectivament, la competència exclusiva en matèria de règim general de telecomunicacions i en matèria de seguretat pública.

Disposició final segona. *Aplicació supletòria de la normativa sobre seguretat i integritat de les xarxes de comunicacions electròniques.*

1. En tot el que no regulin aquest Reial decret i l'esquema que aprova, és aplicable de manera supletòria el que disposen la Llei 11/2022, de 28 de juny, general de telecomunicacions, i la seva normativa de desplegament.

2. En el que no regulen la Llei 11/2022, de 28 de juny, general de telecomunicacions, i la normativa de desplegament, és aplicable de manera supletòria el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació, i la Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques, així com la normativa de desplegament respectiva.

Disposició final tercera. *Habilitació per al desplegament reglamentari i la modificació d'annexos.*

1. S'habilita la persona titular del Ministeri per a la Transformació Digital i de la Funció Pública per desplegar el que preveuen aquest Reial decret i l'esquema que aprova, inclosa l'aprovació d'instruccions tècniques de seguretat.

2. S'habilita la persona titular del Ministeri per a la Transformació Digital i de la Funció Pública per modificar mitjançant una ordre el contingut dels annexos de l'Esquema Nacional de Seguretat de les xarxes i els serveis 5G en funció de l'evolució de l'avenç tecnològic, de l'aprovació de nous estàndards tècnics i esquemes de certificació d'equips de telecomunicació i productes connectats i del desenvolupament de diferents configuracions i paràmetres tècnics de xarxes i serveis 5G i de generacions de comunicacions electròniques venidores.

Disposició final quarta. *Entrada en vigor.*

Aquest Reial decret i l'esquema que aprova entren en vigor l'endemà de la publicació en el «Butlletí Oficial de l'Estat».

Madrid, 30 d'abril de 2024.

FELIPE R.

El ministre per a la Transformació Digital
i de la Funció Pública,
JOSÉ LUIS ESCRIVÁ BELMONTE

ESQUEMA NACIONAL DE SEGURETAT DE LES XARXES I ELS SERVEIS 5G

CAPÍTOL I

Disposicions generals

Article 1. *Esquema Nacional de Seguretat de les xarxes i els serveis 5G.*

L'Esquema Nacional de Seguretat de les xarxes i els serveis 5G (d'ara endavant, ENS5G) s'aprova en desplegament del que estableix el Reial decret llei 7/2022, de 29 de març, sobre requisits per garantir la seguretat de les xarxes i els serveis de comunicacions electròniques de cinquena generació, en particular, en aplicació del capítol IV.

Article 2. *Objectius.*

L'ENS5G té els objectius següents:

a) Reforçar la protecció de la seguretat nacional.
b) Garantir un funcionament continuat i segur de les xarxes i els serveis 5G.
c) Dur a terme un tractament integral i global de la seguretat de les xarxes i els serveis 5G, i considerar les aportacions a l'abast de cada agent de la cadena de valor de 5G.
d) Reforçar la seguretat en la instal·lació i operació de les xarxes de comunicacions electròniques 5G i en la prestació dels serveis de comunicacions mòbils i sense fil que es basin en les xarxes 5G.
e) Impulsar una seguretat integral de l'ecosistema generat per la tecnologia 5G.
f) Promoure un mercat de subministradors en les xarxes i els serveis de comunicacions electròniques 5G prou diversificat amb la finalitat de garantir la seguretat basada en raons tècniques, estratègiques i operatives i evitar, per aquestes raons, la presència de subministradors amb una qualificació d'alt risc o de risc mitjà en determinats elements de xarxa o àmbits.
g) Enfortir la indústria i fomentar les activitats d'R+D+I nacionals en ciberseguretat relacionades amb la tecnologia 5G.
h) Impulsar la formació i la conscienciació en ciberseguretat 5G.

Article 3. *Definicions.*

Als efectes de l'ENS5G, s'utilitzen les definicions que estableix el Reial decret llei 7/2022, de 29 de març, sobre requisits per garantir la seguretat de les xarxes i els serveis de comunicacions electròniques de cinquena generació, així com les definicions que estableixen la Llei 11/2022, de 28 de juny, general de telecomunicacions, i la Directiva 2018/1972, d'11 de desembre de 2018, del Parlament Europeu i del Consell, per la qual s'estableix el Codi europeu de les comunicacions electròniques.

El concepte de seguretat integral que recull l'ENS5G es refereix al fet que la seguretat s'entén com un procés integral constituït per tots els elements humans, materials, tècnics, jurídics i organitzatius, dins de l'àmbit i el marc de la seguretat de les xarxes i els serveis 5G que regula el Reial decret llei 7/2022, de 29 de març.

Article 4. *Àmbit d'aplicació.*

1. L'ENS5G, en el marc de la seguretat de xarxes i serveis 5G que regula el Reial decret llei 7/2022, de 29 de març, s'aplica als subjectes obligats següents:

a) Operadors 5G, que defineix l'article 3.1, apartat a) del Reial decret llei 7/2022, de 29 de març.

b) Subministradors 5G, que defineix l'article 3.1, apartat f) del Reial decret llei 7/2022, de 29 de març.

c) Usuaris corporatius 5G que tinguin atorgats drets d'ús del domini públic radioelèctric per instal·lar, desplegar o explotar una xarxa privada 5G o prestar serveis 5G per a fins professionals o en autoprestació, que defineix l'article 3.1, apartat g) del Reial decret llei 7/2022, de 29 de març.

2. L'ENS5G també s'aplica a les entitats de les administracions públiques que instal·lin, despleguin i explotin xarxes 5G, siguin públiques o privades, o prestin serveis 5G, disponibles al públic o en autoprestació, quan les seves activitats no es duguin a terme principalment en els àmbits de la seguretat nacional, la seguretat pública, la defensa nacional o la garantia del compliment de la Llei, incloses la prevenció, investigació, detecció i enjudiciament d'infraccions penals. Addicionalment, pel seu caràcter excepcional, no s'aplica en l'àmbit de la defensa nacional a escala general i, en particular, en les activitats de preparació i participació en operacions militars de les Forces Armades.

Article 5. *Xarxa 5G.*

1. Una xarxa de comunicacions electròniques 5G està integrada, almenys, pels elements, les infraestructures i els recursos següents:

a) Els relatius a les funcions del nucli de la xarxa.
b) Les funcions de transport i transmissió.
c) La xarxa d'accés.
d) Els sistemes de control i gestió i els serveis de suport.
e) Les funcions de computació a la perifèria, virtualització de xarxa i gestió dels seus components.
f) Els relatius a intercanvis de trànsit o interconnexió amb xarxes externes i internet.
g) Altres components i funcions als quals es refereix l'annex I.

2. Formen part de la xarxa 5G la totalitat dels elements de xarxa, les infraestructures, els recursos i les funcions de les xarxes utilitzades per oferir serveis 5G, encara que també s'utilitzin en les xarxes i els serveis de comunicacions electròniques de generacions mòbils precedents, d'acord amb l'article 3.1, apartat b) del Reial decret llei 7/2022, de 29 de març.

3. La descripció detallada dels elements, les infraestructures i els recursos que integren una xarxa 5G figura en l'annex I.

4. Dins de cadascuna de les parts o els elements d'una xarxa 5G, siguin parts o elements crítics o no de la xarxa 5G en els termes que indiquen l'article 6, apartats 2 i 3, del Reial decret llei 7/2022, de 29 de març, i aquest article i el següent, hi ha diferents actius que poden presentar un grau de criticitat diferent (alta, mitjana, baixa) en l'anàlisi de riscos en els termes que indica l'annex II.

Article 6. *Elements crítics d'una xarxa 5G.*

1. Són elements crítics d'una xarxa 5G:

a) Els relatius a les funcions del nucli de la xarxa.
b) Els sistemes de control i gestió i els serveis de suport.
c) La xarxa d'accés en aquelles zones geogràfiques i ubicacions que es determini.

2. Els elements crítics d'una xarxa 5G pública s'han d'ubicar dins del territori nacional, d'acord amb l'article 12.3, apartat e), del Reial decret llei 7/2022, de 29 de març.

3. No obstant això, determinats elements, funcions i sistemes tant del nucli de la xarxa com dels sistemes de control i gestió i els serveis de suport es poden ubicar fora

del territori nacional, sempre que el Ministeri per a la Transformació Digital i de la Funció Pública pugui exercir les facultats que li atribueix el Reial decret llei 7/2022, de 29 de març, en particular, les facultats d'inspecció i règim sancionador que preveu el capítol V, de manera que pugui efectuar una verificació integral sobre el funcionament, l'operativitat i les condicions d'ús d'aquests elements crítics d'una xarxa 5G i, si s'escau, poder adoptar mesures, cautelars o definitives, sobre aquests elements, funcions i sistemes o l'equipament utilitzat en l'exercici de les potestats que al Ministeri per a la Transformació Digital i de la Funció Pública li atribueixen el Reial decret llei 7/2022, de 29 de març, i la Llei 11/2022, de 28 de juny, general de telecomunicacions.

4. En cas que el Consell de Ministres, amb l'informe previ del Ministeri per a la Transformació Digital i de la Funció Pública, arribi a la conclusió que els elements, les funcions i els sistemes tant del nucli de la xarxa com dels sistemes de control i gestió i els serveis de suport que estiguin ubicats fora del territori nacional afectin la seguretat o integritat de la xarxa 5G tenint en compte l'anàlisi de les mesures tècniques o les mesures estratègiques que exposen els articles 15.2 i 15.3, respectivament, o condiciona sensiblement l'exercici de les seves facultats de supervisió i potestats d'inspecció, pot requerir al titular de la xarxa 5G que aquests elements, funcions i sistemes s'ubiquin en territori nacional. A aquest efecte, la reubicació dels elements, les funcions i els sistemes s'ha de produir en el termini que indiqui el Consell de Ministres en el seu acord, a proposta del Ministeri per a la Transformació Digital i de la Funció Pública, amb l'audiència prèvia del titular de la xarxa 5G, per bé que aquest termini no pot ser inferior a un any.

Article 7. *Tractament integral de la seguretat.*

1. La seguretat s'entén com un procés integral constituït per tots els elements humans, materials, tècnics, jurídics i organitzatius relacionats amb les xarxes o els serveis 5G dels subjectes obligats afectats per l'àmbit d'aplicació i s'ha d'incorporar des del disseny i la implementació de les xarxes 5G. L'ENS5G té la vocació de dur a terme un tractament integral de la seguretat de les xarxes i els serveis 5G.

2. A aquest efecte, l'ENS5G ha tingut en compte i ha de tenir en compte en actualitzacions o modificacions futures la normativa, les recomanacions i els estàndards tècnics de la Unió Europea, de la Unió Internacional de Telecomunicacions (UIT) i d'altres organitzacions internacionals.

Així mateix, l'ENS5G ha tingut en compte i ha de tenir en compte en futures actualitzacions o modificacions les aportacions, l'anàlisi de riscos, els plans de mitigació de riscos i les estratègies de diversificació de la cadena de subministrament que s'han anat proporcionant i que han de proporcionar els subjectes obligats en compliment de les obligacions que estableixen el Reial decret llei 7/2022, de 29 de març, aquest esquema i la resta de normativa.

3. En aquest context de seguretat integral, els subjectes obligats han de dur a terme un tractament integral i global de la seguretat de les xarxes, els elements, les infraestructures, els recursos, les facilitats i els serveis dels quals siguin responsables, per a la qual cosa han d'efectuar, mitjançant un mètode holístic, una anàlisi de les vulnerabilitats, les amenaces i els riscos que els afectin com a agents econòmics i dels components anteriorment relacionats, així com una gestió adequada i integral d'aquests riscos mitjançant la utilització de les tècniques i mesures que siguin adequades per aconseguir-ne la mitigació o eliminació i assolir l'objectiu final d'una explotació i operació segures de les xarxes i els serveis 5G, i també considerar les aportacions de cada agent de la cadena de valor de 5G.

4. Per dur a terme un tractament integral de la seguretat de les xarxes i els serveis 5G, l'operador 5G ha de recollir dels seus subministradors 5G les pràctiques i mesures de seguretat que hagin adoptat en els productes i serveis subministrats. Aquesta informació l'han de proporcionar els subministradors 5G i el seu tractament és confidencial, de manera que només la poden utilitzar els operadors 5G per efectuar una anàlisi i gestió de riscos i el Ministeri per a la Transformació Digital i de la Funció Pública

i els altres organismes públics competents per a l'aplicació del que disposen el Reial decret llei 7/2022, de 29 de març, i aquest esquema.

5. Els subjectes obligats poden enviar al Centre d'Operacions de Seguretat 5G de referència al qual es refereix l'article 41 les dades requerides per a la detecció de l'estat de la ciberseguretat de les xarxes i els serveis 5G en temps real.

6. El Ministeri per a la Transformació Digital i de la Funció Pública, directament o a través del Centre d'Operacions de Seguretat 5G de referència al qual es refereix l'article 41, pot formular els requeriments d'informació necessaris als subjectes obligats, que s'han de respondre en el termini de 15 dies hàbils a comptar de l'endemà de la seva notificació, a l'efecte de poder exercir les funcions que li assigna el Reial decret llei 7/2022, de 29 de març.

Article 8. *Gestió de la seguretat basada en els riscos.*

1. L'anàlisi i la gestió dels riscos és una part essencial del procés de seguretat, i ha de constituir una activitat contínua i permanentment actualitzada.

2. La gestió de riscos permet el manteniment d'un entorn controlat en la xarxa o servei 5G, i minimitzar els riscos a nivells acceptables. La reducció a aquests nivells s'ha de fer mitjançant una aplicació de mesures de seguretat apropiada, de manera equilibrada i proporcionada a la naturalesa i les característiques de la xarxa, dels serveis per prestar i dels riscos als quals estiguin exposats, que s'han de reflectir en l'anàlisi de riscos.

Article 9. *Prevenció, detecció, resposta i conservació.*

1. La seguretat dels sistemes, les xarxes i els serveis 5G ha de considerar les accions relatives als aspectes de prevenció, detecció i resposta, amb l'objecte de minimitzar-ne les vulnerabilitats i aconseguir que les amenaces no es materialitzin o que, en el cas de fer-ho, no afectin greument les dades tractades, l'operativitat i integritat de les xarxes 5G o a la prestació d'un servei 5G.

2. Les mesures de prevenció, per ampliar el coneixement de les vulnerabilitats, que poden incorporar components orientats a la dissuasió o a la reducció de la superfície d'exposició, han d'eliminar o reduir la probabilitat que les amenaces s'arribin a materialitzar.

3. Les mesures de detecció s'adrecen a descobrir la presència d'un ciberincident, una ciberamenaça o vulnerabilitat.

4. Les mesures de resposta, orientades a minimitzar l'impacte dels ciberincidents i, si s'escau, a aplicar mesures de bloqueig, així com posteriorment la restauració del sistema, la xarxa o el servei 5G que pugui haver estat afectat per un incident de seguretat.

5. Sense minva dels principis bàsics restants i requisits mínims establerts, el sistema d'informació ha de garantir la conservació de les dades i la informació en suport electrònic.

Article 10. *Existència de línies de defensa.*

1. Les xarxes, els elements, les infraestructures, els recursos, les facilitats i els serveis 5G han de disposar d'una estratègia de protecció i diversificació adequada i proporcionada als riscos de cada element i capa de serveis 5G, de tal manera que, quan un d'aquests es pugui veure compromès, aquesta estratègia permeti:

a) Una reacció adequada davant dels incidents que no s'han pogut evitar, i així reduir la probabilitat que el sistema es comprometi en conjunt.

b) Minimitzar l'impacte final de l'incident.

2. L'estratègia de protecció i les línies de defensa estan constituïdes per mesures de naturalesa organitzativa, física i lògica. S'han de determinar en les instruccions tècniques de seguretat corresponents.

Article 11. *Vigilància contínua i reavaluació periòdica.*

1. La vigilància contínua permet la detecció d'activitats o comportaments anòmals i la seva oportuna resposta.
2. L'avaluació permanent de l'estat de la seguretat de les xarxes i els serveis 5G permet mesurar-ne l'evolució, detectar vulnerabilitats i identificar deficiències de configuració.
3. Les mesures de seguretat s'han de reavaluar i actualitzar periòdicament, adequar la seva eficàcia a l'evolució dels riscos i els sistemes de protecció, i arribar a un replantejament de la seguretat, si és necessari.

Article 12. *Sistemes, xarxes i serveis 5G que tractin dades personals.*

Quan un sistema, una xarxa o un servei 5G tracti dades personals, li és aplicable el que disposen el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques respecte al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades), i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, o si s'escau, la resta de normativa aplicable, així com els criteris que estableixi l'Agència Espanyola de Protecció de Dades o, en el seu àmbit competencial, les autoritats autonòmiques de protecció de dades, sens perjudici dels requisits que estableix aquest Reial decret.

CAPÍTOL II

Anàlisi i gestió de riscos en l'àmbit nacional

Article 13. *Anàlisi de riscos en l'àmbit nacional.*

1. L'anàlisi de riscos en l'àmbit nacional que s'ha efectuat en el marc de l'ENS5G és el que figura en l'annex II d'aquest Reial decret.
2. En la realització d'aquesta anàlisi, s'ha tingut en compte:

a) L'anàlisi general dels riscos de les xarxes i els serveis 5G, prenent en consideració la informació recollida dels subjectes obligats.
b) L'examen de les vulnerabilitats lligades a la cadena de subministrament de les xarxes i els serveis 5G.
c) L'avaluació del grau de dependència dels subministradors del conjunt de les xarxes i els serveis 5G a Espanya tenint en compte les anàlisis de riscos i les estratègies de diversificació de subministradors remesos pels operadors 5G, així com el risc d'interrupció del subministrament per circumstàncies econòmiques, societàries o comercials que afectin els subministradors.
d) L'avaluació de l'eficàcia de les mesures de seguretat aplicades fins a l'aprovació de cada anàlisi de riscos nacional per mitigar els riscos posats de manifest per aquesta anàlisi.
e) La determinació d'una jerarquia de riscos en funció de les anàlisis de riscos dutes a terme pels subjectes obligats.

Article 14. *Gestió de riscos en l'àmbit nacional.*

1. Els criteris, els requisits, les condicions i els terminis perquè els subjectes obligats puguin dissenyar i implementar tècniques i mesures de mitigació de riscos són els que, almenys, figuren en l'annex III d'aquest Reial decret.

2. En la determinació d'aquests criteris i requisits de gestió de riscos s'han tingut en compte l'anàlisi de riscos nacional que incorpora aquest esquema i l'avaluació de l'eficàcia de les mesures aplicades pels subjectes obligats per mitigar i gestionar els riscos en les xarxes i els serveis 5G.

CAPÍTOL III

Mesures específiques per garantir la seguretat de les xarxes i els serveis 5G

Article 15. *Declaració de subministradors 5G d'alt risc i de risc mitjà.*

1. El Govern, mitjançant un acord adoptat en el Consell de Ministres, pot qualificar que determinats subministradors 5G són d'alt risc.

A aquest efecte, el Govern ha d'analitzar tant les garanties tècniques de funcionament i operativitat dels seus equips, productes i serveis com la seva exposició a ingerències externes.

2. Amb relació a l'anàlisi de les mesures i les garanties tècniques de funcionament i operativitat dels seus equips, productes i serveis s'han de valorar aspectes relatius al compliment de normes o especificacions tècniques, la seva verificació mitjançant esquemes de certificació, o la superació de proves o auditories de seguretat efectuades per entitats independents.

3. Amb relació a l'anàlisi de les mesures estratègiques i exposició a ingerències externes, s'han de valorar els aspectes següents:

a) Els vincles dels subministradors i de la seva cadena de subministrament, amb els governs de tercers països.

b) La composició del seu capital social i l'estructura dels seus òrgans de govern.

c) El poder d'un tercer Estat per exercir pressió sobre l'actuació o ubicació de l'empresa.

d) Les característiques de la legislació i la política de ciberdefensa i el respecte al dret internacional i a les resolucions i acords de l'Organització de les Nacions Unides d'aquest tercer Estat.

e) Els acords de cooperació en matèria de seguretat, ciberseguretat, delictes cibernètics o protecció de dades signats amb el país tercer del qual es tracti, així com els tractats internacionals en aquelles matèries dels quals sigui part aquest Estat.

f) El grau d'adequació de la normativa del tercer Estat sobre protecció de dades personals a la d'Espanya, al Reglament general de protecció de dades aprovat pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques respecte al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE, adoptada per la Unió Europea i a qualsevol altra normativa aplicable en matèria de seguretat de les xarxes i els sistemes d'informació i de telecomunicacions.

4. El procediment per a la qualificació de determinats subministradors 5G com d'alt risc s'inicia d'ofici mitjançant un acord que adopta el Ministeri per a la Transformació Digital i de la Funció Pública.

En la tramitació de l'expedient s'ha de sol·licitar un informe a la Comissió Nacional dels Mercats i la Competència, al Ministeri de l'Interior, al Ministeri de Defensa, al Departament de Seguretat Nacional del Gabinet de la Presidència del Govern, al Centre Nacional d'Intel·ligència del Ministeri de Defensa i a l'Institut Nacional de Ciberseguretat d'Espanya.

En la proposta de resolució, el Ministeri per a la Transformació Digital i de la Funció Pública ha de concretar amb relació al subministrador 5G afectat les garanties tècniques de funcionament i operativitat dels equips, productes i serveis subministrats, així com la seva exposició a ingerències externes de conformitat amb el que indiquen els apartats anteriors que justifiquen la decisió proposada, així com les conseqüències que d'aquesta decisió es deriven i, en cas que es declari subministrador d'alt risc, el termini en què els operadors 5G han de dur a terme la substitució dels equips, productes i serveis proporcionats per aquest subministrador.

De la proposta de resolució s'ha de donar audiència als operadors 5G i subministradors 5G afectats per un termini de 15 dies hàbils.

Una vegada efectuats aquests tràmits, el Govern, mitjançant un acord adoptat en el Consell de Ministres, amb l'informe previ del Consell de Seguretat Nacional, ha d'adoptar una decisió en el termini de sis mesos a comptar de la incoació del procediment.

5. L'acord del Consell de Ministres pel qual es qualifiqui determinats subministradors 5G de subministradors d'alt risc determina el termini en què els operadors 5G han de dur a terme la substitució dels equips, productes i serveis proporcionats per aquest subministrador en la xarxa i els serveis de l'operador 5G, quan això sigui necessari, per a la qual cosa ha de tenir en compte les amenaces detectades i els motius que han justificat la declaració d'un subministrador 5G com a subministrador d'alt risc, la situació del mercat dels subministradors, les alternatives de subministrament d'equips i productes substitutius viables, la implantació d'aquests equips i productes en la xarxa 5G de l'operador, especialment en els elements crítics de la xarxa 5G i en funció de quins són en concret els elements crítics afectats, la dificultat intrínseca per dur a terme la substitució d'equips, els cicles d'actualització d'equips, la migració de les xarxes 5G no autònomes a autònomes, així com el seu impacte econòmic.

En la determinació del termini de substitució, l'acord del Consell de Ministres pel qual es qualifiqui determinats subministradors 5G de subministradors d'alt risc pot establir un termini diferent per als distints elements crítics de la xarxa pública 5G en funció de les amenaces detectades i els motius que han justificat la declaració d'un subministrador 5G com a subministrador d'alt risc, la criticitat d'aquest element o part d'aquest, de la seva afectació al funcionament i operativitat de la xarxa i de la disponibilitat d'equips en aquell moment en el mercat d'equips de telecomunicació, per bé que, en cap cas, aquest termini no pot ser inferior a un any per a qualsevol element crític de la xarxa pública 5G.

L'acord del Consell de Ministres pel qual es qualifiqui determinats subministradors 5G de subministradors d'alt risc pot determinar un termini diferent per a la substitució dels equips, productes i serveis per als distints operadors 5G afectats en funció de la repercussió que aquesta substitució té en la xarxa de cada operador, de l'afectació de la substitució als diferents elements o parts de la xarxa 5G, de la capacitat competitiva de l'operador, dels contractes de subministrament d'equipament subscrits i de la capacitat de subministrament existent en el mercat d'equips de telecomunicació, per bé que, en cap cas, aquest termini no pot ser inferior a un any per a qualsevol element crític de la xarxa pública 5G.

6. L'acord del Consell de Ministres pel qual es qualifiqui que determinats subministradors 5G són d'alt risc posa fi a la via administrativa i és directament recurrible davant de la jurisdicció contenciosa administrativa, sens perjudici que potestativament es pugui interposar contra aquest un recurs de reposició amb caràcter previ al recurs contenciós administratiu.

7. Els subministradors d'alt risc els equips de telecomunicació dels quals, maquinari, programari o serveis auxiliars proporcionats siguin utilitzats únicament i exclusivament en xarxes privades 5G o per a la prestació de serveis 5G en règim d'autoprestació es qualifiquen de subministradors de risc mitjà.

Article 16. *Determinació d'ubicacions en què no es poden instal·lar equips de subministradors qualificats d'alt risc.*

1. El Consell de Seguretat Nacional, amb l'informe previ del Ministeri per a la Transformació Digital i de la Funció Pública, pot determinar les ubicacions, les àrees i els centres en què no es poden instal·lar equips de subministradors qualificats d'alt risc. En l'emissió de l'informe, el Ministeri per a la Transformació Digital i de la Funció Pública ha de tenir en compte les propostes que li remetin el Ministeri de l'Interior, el Ministeri de Defensa, el Departament de Seguretat Nacional del Gabinet de la Presidència del Govern i el Centre Nacional d'Intel·ligència del Ministeri de Defensa.

2. En la determinació d'aquestes ubicacions, àrees i centres s'han d'incloure les centrals nuclears, els centres vinculats a la defensa nacional i les ubicacions, les àrees i els centres que, per la seva vinculació a la seguretat nacional o al manteniment de determinats serveis essencials per a la comunitat o sectors estratègics, els determini el Consell de Seguretat Nacional.

3. A les estacions radioelèctriques amb les quals es proporcioni cobertura a aquestes ubicacions, àrees i centres, els operadors 5G no poden utilitzar en la xarxa d'accés ràdio d'una xarxa pública 5G equips de telecomunicació, sistemes de transmissió, equips de commutació o encaminament i altres recursos, que permetin el transport de senyals, maquinari, programari o serveis auxiliars de subministradors que s'hagin qualificat d'alt risc.

4. Així mateix, per a la instal·lació, modificació o adaptació d'estacions radioelèctriques que proporcionin cobertura a aquestes ubicacions, àrees i centres prèviament declarats, tenint en compte la seva vinculació amb la seguretat nacional o al manteniment de determinats serveis essencials per a la comunitat o sectors estratègics, els operadors 5G han de sol·licitar autorització a la Secretaria d'Estat de Telecomunicacions i Infraestructures Digitals, en l'atorgament del qual s'han de tenir en compte els equips de telecomunicació, sistemes de transmissió, equips de commutació o encaminament i altres recursos, que permetin el transport de senyals, maquinari, programari o serveis auxiliars per instal·lar, les condicions tècniques en l'ús del domini públic radioelèctric i les característiques intrínseques i fins que cal protegir en aquelles ubicacions, àrees i centres prèviament declarats.

La Secretaria d'Estat de Telecomunicacions i Infraestructures Digitals, en l'atorgament d'aquestes autoritzacions, pot valorar els plans que els operadors 5G puguin presentar per a la renovació tecnològica o la substitució d'equips de transmissió ràdio i en la xarxa d'accés que afectin les ubicacions, les àrees i els centres prèviament declarats per als quals se sol·licita autorització.

El termini per a l'atorgament d'aquestes autoritzacions és de tres mesos, i s'entén desestimada la sol·licitud en cas d'absència de resolució expressa. La resolució, expressa o presumpta, posa fi a la via administrativa i és directament recurrible davant de la jurisdicció contenciosa administrativa, sens perjudici que potestativament es pugui interposar contra aquest un recurs de reposició amb caràcter previ al recurs contenciós administratiu.

S'exceptua la necessitat d'obtenir l'autorització a la qual es refereix aquest apartat en les operacions d'ampliació, adaptació, reparació i manteniment d'estacions radioelèctriques que proporcionin cobertura a aquestes ubicacions, àrees i centres, sempre que aquesta estació ja estigui prèviament instal·lada i autoritzada i no impliqui cap canvi de subministrador en cap dels elements, maquinari, programari o capes en els sistemes que configuren l'estació.

S'exceptua la sol·licitud d'autorització en l'ampliació de l'equipament radioelèctric ubicat en un node d'un mateix subministrador per raons de capacitat, que ja estigui instal·lat i autoritzat prèviament, de conformitat amb els paràgrafs anteriors, així com qualsevol operació de manteniment i reparació.

5. Les obligacions que estableixen els apartats 3 i 4 d'aquest article s'apliquen de manera exclusiva als elements de la xarxa d'accés ràdio 5G segons la definició del 3GPP que esmenta l'annex I.

6. La determinació i difusió d'aquestes ubicacions tenen la qualificació de matèria reservada de conformitat amb la regulació que estableix la Llei 9/1968, de 5 d'abril, sobre secrets oficials.

Article 17. *Diversificació en la cadena de subministrament.*

1. D'acord amb el que preveu l'article 12.3.a) del Reial decret llei 7/2022, de 29 de març, els operadors 5G que siguin titulars o explotin elements crítics d'una xarxa pública 5G han de dissenyar una estratègia de diversificació en la cadena de subministrament dels equips de telecomunicació, sistemes de transmissió, equips de commutació o encaminament i altres recursos que permetin el transport de senyals en una xarxa pública 5G.

2. En la xarxa d'accés, els operadors 5G han de disposar d'equips de transmissió ràdio que siguin proporcionats, com a mínim, per dos subministradors diferents amb la finalitat d'afavorir la continuïtat dels serveis 5G, la substituïbilitat més fàcil dels equips i evitar la dependència exclusiva d'un subministrador únic.

A aquests efectes, es considera que els subministradors no són diferents si tots pertanyen al mateix grup d'empreses, de conformitat amb els criteris que estableix l'article 42 del Codi de comerç.

3. En el nucli de la xarxa i en els sistemes de control i gestió i els serveis de suport, el subministrador pot ser únic.

4. En cas que a conseqüència d'operacions de concentració empresarial, es redueixi el nombre de subministradors inclosos en l'estratègia de diversificació en la cadena de subministrament que impliqui que no es compleix el límit mínim de dos subministradors diferents que estableix l'apartat 2, l'operador 5G ho ha de comunicar al Ministeri per a la Transformació Digital i de la Funció Pública, que ha d'impulsar que el Govern, mitjançant un acord adoptat en el Consell de Ministres, amb l'audiència prèvia dels operadors 5G i subministradors 5G afectats, decideixi si és possible mantenir un subministrador únic, tenint en compte les condicions concretes de l'operació de concentració empresarial, la situació del mercat dels subministradors, les alternatives de subministrament d'equips i productes substitutius viables, la implantació d'aquests equips i productes en la xarxa 5G de l'operador, especialment en els elements crítics de la xarxa 5G, la qualificació del subministrador com d'alt risc, la dificultat intrínseca per dur a terme la substitució d'equips, els cicles d'actualització d'equips, la migració de les xarxes 5G no autònomes a autònomes, així com el seu impacte econòmic.

5. El Ministeri per a la Transformació Digital i de la Funció Pública, si considera que no queda garantida la continuïtat en la prestació dels serveis 5G, la integritat física o lògica de la xarxa 5G, que hi ha una àmplia exposició a l'equipament instal·lat per un subministrador que en determinades circumstàncies pot posar en perill la funcionalitat i l'operativitat de la xarxa 5G o per garantir la seguretat en la provisió de serveis utilitzats pels serveis de seguretat nacional, defensa nacional o per diferents administracions públiques, i tenint en compte si hi ha qualificació de subministradors d'alt risc, les alternatives de subministrament d'equips i productes substitutius viables, la implantació d'aquests equips i productes en la xarxa 5G de l'operador, especialment en els elements crítics de la xarxa 5G, i els cicles d'actualització d'equips, pot modificar l'estratègia de diversificació en la cadena de subministrament d'un operador 5G.

Abans d'aprovar la modificació, s'ha d'efectuar un tràmit d'audiència amb l'operador 5G i subministrador o subministradors 5G afectats per un termini de 15 dies hàbils. La resolució posa fi a la via administrativa i és directament recurrible davant de la jurisdicció contenciosa administrativa, sens perjudici que potestativament es pugui interposar contra aquesta un recurs de reposició amb caràcter previ al recurs contenciós administratiu.

CAPÍTOL IV

Anàlisi de riscos pels subjectes obligats

Article 18. *Anàlisi de riscos pels operadors 5G.*

1. Els operadors 5G han d'analitzar els riscos de les xarxes i els serveis 5G, detectant vulnerabilitats i amenaces que els afectin, tant com a agent econòmic, com pels elements de xarxa, infraestructures, recursos, facilitats i serveis que utilitzin o proveeixin en la instal·lació, desplegament i explotació de xarxes 5G o en la prestació de serveis 5G.

2. Els operadors 5G que siguin titulars o gestionin elements de xarxa d'una xarxa pública 5G, en la seva anàlisi de riscos, han de dur a terme un estudi detallat i individualitzat de les amenaces i vulnerabilitats que afectin els elements, les infraestructures i els recursos que integren una xarxa 5G i que figuren en l'annex I, seguint la metodologia que descriu l'annex II, apartat 1.

3. L'anàlisi de riscos que dugui a terme un operador 5G ha de tenir en compte, almenys, els factors següents:

a) Parametrització i configuració d'elements i funcions de xarxa, inclosos els equips de telecomunicació, maquinari i programari i serveis auxiliars que intervinguin en el funcionament o l'operació de xarxes 5G o en la prestació de serveis 5G.

b) Polítiques d'integritat i actualització dels programes informàtics per garantir la seguretat i la funcionalitat de la xarxa en qualsevol moment.

c) Estratègies de permisos d'accés a actius físics i lògics, les quals garanteixen que només el personal autoritzat pugui accedir a recursos crítics.

d) Avaluació de les dependències de determinats proveïdors en elements crítics de la xarxa 5G i identificació de riscos potencials associats amb la cadena de subministrament.

e) Identificació i avaluació d'amenaces potencials d'agents externs, incloent-hi grups organitzats amb capacitat per atacar la xarxa.

f) Consideració dels equips terminals i dispositius connectats a la xarxa, i el seu impacte en la seguretat global de la xarxa.

g) Anàlisi de la interacció i l'impacte de la xarxa 5G sobre elements d'usuaris corporatius i xarxes externes connectades.

h) Comprensió de la interrelació de la xarxa 5G amb altres serveis essencials per a la societat, avaluant com possibles interrupcions del servei o compromisos de seguretat poden afectar aquests serveis essencials.

i) Priorització i jerarquització de riscos basats en l'afectació a elements crítics de la xarxa, el tipus de recurs, la infraestructura i el servei afectat, la integritat i el manteniment tècnic de la xarxa, la capacitat de detecció i recuperació, el nombre i tipus d'usuaris afectats, i el tipus d'informació compromesa.

j) Implementació d'estratègies de resiliència i recuperació davant de desastres, per assegurar la continuïtat del servei davant d'atacs cibernètics, incidències tècniques o desastres naturals, incloent-hi la redundància de sistemes crítics.

k) Realització d'anàlisi de vulnerabilitats de manera regular per identificar proactivament vulnerabilitats de seguretat i resoldre-les per mitigar possibles amenaces abans que puguin ser explotades.

4. Per dur a terme un tractament integral de la seguretat de les xarxes i els serveis 5G, el subministrador ha de proporcionar als operadors 5G als quals subministri les pràctiques i mesures de seguretat que s'han adoptat en els productes i serveis que han subministrat, tenint en compte els factors de risc indicats en aquest capítol i el perfil de risc del subministrador. Aquesta informació l'han de rebre els operadors 5G i el seu tractament ha de ser confidencial, de manera que només la poden utilitzar els operadors 5G per efectuar una anàlisi i gestió de riscos i el Ministeri per a la

Transformació Digital i de la Funció Pública i els altres organismes públics competents per a l'aplicació del que disposen el Reial decret llei 7/2022, de 29 de març, i aquest esquema amb les finalitats exclusives d'aquests.

5. L'anàlisi de riscos de l'operador 5G ha d'incloure una priorització i jerarquia dels riscos en funció dels paràmetres següents:

a) Afectació a un element crític de la xarxa pública 5G.
b) Tipus de recurs, infraestructura i servei que es pugui veure afectat.
c) Afectació a la integritat i el manteniment tècnic de la xarxa o a la continuïtat del servei.
d) Capacitat de detecció i recuperació.
e) Nombre i tipus d'usuaris afectats.
f) Tipus d'informació la integritat de la qual s'hagi pogut comprometre.

6. Una nova anàlisi de riscos per l'operador 5G s'ha de dur a terme i remetre al Ministeri per a la Transformació Digital i de la Funció Pública abans de l'1 d'octubre de 2024, i, a continuació, cada dos anys o quan el Ministeri per a la Transformació Digital i de la Funció Pública ho requereixi, sempre que s'hagin produït canvis significatius en les infraestructures 5G utilitzades o els serveis 5G prestats que indueixin a pensar que les mesures de seguretat adoptades puguin haver perdut eficàcia.

Article 19. *Anàlisi de riscos pels subministradors 5G.*

1. Els subministradors 5G han d'analitzar els riscos dels equips de telecomunicació, maquinari i programari i serveis auxiliars que intervinguin en el funcionament o operació de xarxes 5G o en la prestació de serveis 5G, i detectar-hi vulnerabilitats i amenaces que afectin tant la gestió de l'empresa com aquests equips, maquinari, programari i serveis.
2. Els subministradors 5G han d'aportar aquesta anàlisi de riscos al Ministeri per a la Transformació Digital i de la Funció Pública, quan se'ls requereixi. Així mateix, els subministradors 5G han d'aportar les anàlisis de riscos als operadors 5G als quals subministri de conformitat amb el que disposa l'article 18.4.
3. No obstant el que disposa l'apartat anterior, els subministradors 5G que hagin estat qualificats d'alt risc o de risc mitjà han de remetre al Ministeri per a la Transformació Digital i de la Funció Pública una anàlisi de riscos dels seus equips, productes o serveis involucrats en les xarxes i els serveis 5G en el termini de sis mesos a comptar des que hagin estat qualificats d'alt risc o de risc mitjà.
4. Els subministradors 5G que siguin qualificats d'alt risc o de risc mitjà han de dur a terme l'anàlisi de riscos cada dos anys i remetre-la al Ministeri per a la Transformació Digital i de la Funció Pública o quan el Ministeri per a la Transformació Digital i de la Funció Pública ho requereixi o sempre que s'hagin produït canvis significatius en les infraestructures 5G utilitzades o serveis 5G prestats que indueixin a pensar que les mesures de seguretat adoptades puguin haver perdut eficàcia.
5. Els subministradors 5G són els responsables de les anàlisis de riscos que efectuïn i del compliment de les obligacions d'informació i remesa de documentació que estableix aquest article.

Article 20. *Anàlisi de riscos pels usuaris corporatius 5G.*

1. Els usuaris corporatius 5G que tinguin atorgats drets d'ús del domini públic radioelèctric per instal·lar, desplegar o explotar una xarxa privada 5G o prestar serveis 5G per a fins professionals o en autoprestació han d'analitzar els riscos de les xarxes i els serveis 5G, i detectar-hi vulnerabilitats i amenaces que afectin els elements de xarxa, infraestructures, recursos, facilitats i serveis que utilitzin o proveeixin en la instal·lació, el desplegament i l'explotació de xarxes privades 5G o en la prestació de serveis 5G en autoprestació.

2. Els usuaris corporatius 5G que esmenta l'apartat anterior han d'aportar aquesta anàlisi de riscos al Ministeri per a la Transformació Digital i de la Funció Pública, quan se'ls requereixi.

Article 21. *Confidencialitat de la informació sobre anàlisi de riscos.*

1. El Ministeri per a la Transformació Digital i de la Funció Pública pot recollir dels subjectes obligats la informació necessària per a l'anàlisi de riscos.
2. Els subjectes obligats han de proporcionar la informació en el termini de quinze dies hàbils a comptar de l'endemà de la notificació del requeriment d'informació.
3. L'incompliment dels requeriments d'informació formulats de conformitat amb el que indica l'apartat anterior quan hagi passat un mes des de la finalització del termini donat per al seu compliment és qualificat d'infracció greu.
4. S'ha de garantir la confidencialitat de la informació que els subjectes obligats proporcionin sobre l'anàlisi de riscos i no es pot utilitzar per a una finalitat diferent del compliment dels objectius i les obligacions que estableixen el Reial decret llei 7/2022, de 29 de març, aquest esquema i els actes que es dictin en execució d'ambdues disposicions.

CAPÍTOL V

Gestió dels riscos pels subjectes obligats

Article 22. *Mesures comunes per a la gestió de seguretat.*

1. Les mesures a les quals fa referència aquest esquema es fonamenten en un enfocament basat a compendiar els riscos la prevenció, detecció i mitigació o eliminació dels quals tingui per objecte protegir els sistemes, les xarxes i els serveis 5G, i han d'incloure almenys els elements següents:

a) Les polítiques de seguretat dels sistemes, les xarxes i els serveis 5G.
b) Anàlisi de riscos.
c) La gestió d'incidents.
d) La continuïtat de les activitats, com la gestió de còpies de seguretat i la recuperació en cas de catàstrofe, i la gestió de crisis.
e) La seguretat de la cadena de subministrament i, si escau, l'estratègia de diversificació, quan escaigui.
f) La seguretat en l'adquisició, el desenvolupament i el manteniment dels sistemes i les xarxes 5G.
g) Les polítiques i els procediments relatius a la utilització de la criptografia i, si s'escau, de xifratge.
h) La seguretat dels recursos humans, les polítiques de control d'accés i la gestió d'actius.
i) L'ús de solucions d'autenticació, comunicacions de veu, vídeo i text segures i sistemes segurs de comunicacions d'emergència, quan escaigui.
j) L'ús de components certificats.
k) La protecció de serveis i dades al núvol.
l) El monitoratge de sistemes, xarxes i serveis.
m) La seguretat física.
n) La protecció de la informació.
ñ) La realització d'avaluacions periòdiques de vulnerabilitats i proves de penetració per identificar i resoldre o mitigar aquestes vulnerabilitats abans que puguin ser explotades.

2. Els subjectes obligats han d'adoptar mesures tècniques i d'organització adequades per gestionar els riscos existents en la instal·lació, el desplegament i l'explotació de xarxes 5G i en la prestació de serveis 5G, d'acord amb el que estableixen

el Reial decret llei 7/2022, de 29 de març, aquest esquema i els actes que es dictin en execució d'ambdues disposicions.

Article 23. *Gestió de seguretat pels operadors 5G.*

1. Els operadors 5G han de garantir la instal·lació, el desplegament i l'explotació segurs de xarxes públiques 5G i la prestació segura de serveis 5G disponibles al públic mitjançant l'aplicació de tècniques i procediments d'operació i supervisió que garanteixin la seguretat de xarxes i serveis 5G, així com el compliment de la normativa en aquesta matèria.

2. Els operadors 5G tenen les obligacions de seguretat següents destinades a mitigar riscos:

a) Adoptar mesures tècniques i operatives per garantir la integritat física i lògica de les xarxes 5G o qualssevol dels seus elements, infraestructures i recursos, així com la continuïtat en la prestació de serveis 5G.

b) Adoptar plans i mesures de contingència específiques per assegurar la continuïtat d'altres serveis essencials per a la societat que depenguin de les xarxes i els serveis 5G.

c) Seleccionar i identificar les persones, sigui personal propi o d'empreses contractades, que puguin accedir als actius físics i lògics de la xarxa, i fer el manteniment de registres d'accés.

d) Mantenir les credencials d'usuari per a l'accés a la xarxa en possessió de l'operador.

e) Utilitzar únicament productes, recursos, serveis o sistemes certificats per a l'operació de les xarxes 5G, o en alguna de les seves parts o elements.

En particular, han d'exigir dels subministradors la certificació de l'esquema GSMA Network Equipment Security Assurance Scheme (NESAS) i les SCAS (Security Assurance Specification), d'aquests productes, recursos, serveis o sistemes certificats.

f) També han d'exigir dels subministradors els certificats de conformitat d'aquests elements amb els esquemes europeus de certificació que es puguin desplegar en el Reglament 2019/881, del Parlament Europeu i del Consell, de 17 d'abril de 2019, relatiu a ENISA (Agència de la Unió Europea per a la Ciberseguretat) i a la certificació de la ciberseguretat de les tecnologies de la informació i la comunicació, d'acord amb la normativa de requisits horitzontals de ciberseguretat per a productes amb elements digitals o d'acord amb qualsevol altra legislació relacionada de la UE o nacional.

g) Complir les normes o especificacions tècniques aplicables a xarxes i sistemes d'informació, de conformitat amb les normes nacionals, europees i internacionals.

Especialment, s'han de complir les mesures de seguretat aplicables a sistemes d'informació de categoria alta que estableix el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat o el perfil de compliment específic que sigui aplicable o, si s'escau, les que recull la norma tècnica 27002:2022: Seguretat de la informació, ciberseguretat i protecció de la privacitat-controls de seguretat de la informació, si no estan compreses en l'àmbit d'aplicació de l'Esquema Nacional de Seguretat o en el perfil de compliment específic que sigui aplicable.

h) Complir els esquemes europeus de certificació de productes, serveis o sistemes, siguin específics de la tecnologia 5G o no, que s'utilitzin en l'operació o explotació de xarxes i serveis 5G.

i) Fer ús d'eines i metodologies d'anàlisi i gestió de riscos reconegudes nacionalment o internacionalment.

j) Sotmetre's, a costa seva, a una auditoria de seguretat ordinària, almenys cada dos anys, que verifiqui el compliment dels requeriments de l'ENS5G.

Amb caràcter extraordinari, s'ha de fer aquesta auditoria sempre que es produeixin modificacions substancials que puguin repercutir en les mesures de seguretat requerides. La realització de l'auditoria extraordinària determina la data de còmput per al

càlcul dels dos anys, establerts per a la realització de l'auditoria regular ordinària següent, que indica el paràgraf anterior.

L'informe d'auditoria ha de dictaminar sobre el grau de compliment d'aquest Reial decret i identificar les troballes de compliment i incompliment detectades. Ha d'incloure, igualment, els criteris metodològics d'auditoria utilitzats, l'abast i l'objectiu de l'auditoria, i les dades, els fets i les observacions en què es basin les conclusions formulades.

El resultat d'aquesta auditoria s'ha de presentar al Ministeri per a la Transformació Digital i de la Funció Pública amb una periodicitat biennal.

k) Establir procediments apropiats per abordar les vulnerabilitats quan es detectin.

l) Exigir als seus subministradors el compliment d'estàndards de seguretat, des del disseny dels productes i serveis fins a la seva posada en funcionament.

m) Controlar la seva pròpia cadena de subministrament i l'estratègia de diversificació que hagi dissenyat.

n) Col·laborar amb el Centre d'Operacions de Seguretat 5G de referència al qual es refereix l'article 41 per enviar les dades requerides per a la detecció de l'estat de la ciberseguretat de les xarxes i els serveis 5G en temps real.

3. En particular, els operadors 5G que siguin titulars o explotin elements crítics d'una xarxa pública 5G tenen addicionalment les obligacions següents:

a) Han de dissenyar una estratègia de diversificació en la cadena de subministrament dels equips de telecomunicació, sistemes de transmissió, equips de commutació o encaminament i altres recursos que permetin el transport de senyals en una xarxa pública 5G que acompleixi el que disposa l'article 17.

b) No es poden utilitzar en els elements crítics de xarxa equips de telecomunicació, sistemes de transmissió, equips de commutació o encaminament i altres recursos, que permetin el transport de senyals, maquinari, programari o serveis auxiliars de subministradors que hagin estat qualificats d'alt risc de conformitat amb el que disposa l'article 15.

c) No poden utilitzar en la xarxa d'accés ràdio d'una xarxa pública 5G equips de telecomunicació, sistemes de transmissió, equips de commutació o encaminament i altres recursos, que permetin el transport de senyals, maquinari, programari o serveis auxiliars de subministradors que hagin estat qualificats d'alt risc, en aquelles estacions radioelèctriques amb les quals es proporcioni cobertura en les ubicacions, àrees i centres que s'hagin identificat de conformitat amb el que estableix l'article 16.

d) Han d'ubicar els elements crítics d'una xarxa pública 5G dins del territori nacional, sens perjudici del que estableix l'article 6.

Aquestes obligacions s'apliquen de manera exclusiva als elements de la xarxa d'accés ràdio 5G segons la definició del 3GPP que esmenta l'annex I.

4. Els operadors 5G que siguin titulars o explotin elements crítics d'una xarxa pública 5G han de remetre al Ministeri per a la Transformació Digital i de la Funció Pública una nova estratègia de diversificació en la cadena de subministrament abans de l'1 d'octubre de 2024.

Així mateix, l'estratègia de diversificació en la cadena de subministrament s'ha de remetre al Ministeri per a la Transformació Digital i de la Funció Pública cada vegada que sigui objecte de modificació.

Igualment, els operadors 5G que siguin titulars o explotin elements crítics d'una xarxa pública 5G han de remetre al Ministeri per a la Transformació Digital i de la Funció Pública abans de l'1 d'octubre de cada any informació sobre l'estat d'execució de l'estratègia de diversificació en la cadena de subministrament o quan el Ministeri per a la Transformació Digital i de la Funció Pública ho requereixi, sempre que s'hagin produït canvis significatius en les infraestructures 5G utilitzades o els serveis 5G prestats que indueixin a pensar que les mesures de seguretat adoptades puguin haver perdut eficàcia.

5. Els operadors 5G han de remetre al Ministeri per a la Transformació Digital i de la Funció Pública una nova descripció de les mesures tècniques i organitzatives

dissenyades i aplicades per gestionar i mitigar els riscos abans de l'1 d'octubre de 2024 i, a continuació, cada dos anys o quan el Ministeri per a la Transformació Digital i de la Funció Pública ho requereixi, sempre que s'hagin produït canvis significatius en les infraestructures 5G utilitzades o els serveis 5G prestats que indueixin a pensar que les mesures de seguretat adoptades puguin haver perdut eficàcia.

Article 24. *Gestió de seguretat pels subministradors 5G.*

1. Els subministradors 5G han de garantir la seguretat dels equips de telecomunicació, maquinari, programari o serveis auxiliars que proporcionin i que siguin objecte d'ús per les xarxes i els serveis 5G.

2. Els subministradors 5G tenen les obligacions de seguretat següents destinades a mitigar riscos:

a) Complir estàndards de seguretat des del disseny dels equips, productes i serveis fins a la seva posada en funcionament.

En particular, és aplicable la norma tècnica ISO/IEC 27001: Gestió de seguretat de la informació.

b) Reforçar la integritat del programari, actualització i gestió de pedaços. Les parts implicades han d'acordar els mecanismes per a les actualitzacions periòdiques de programari i per donar resposta a les vulnerabilitats de seguretat d'acord amb el cicle de vida dels equips i el nivell d'exposició a vulnerabilitats i els criteris d'avaluació ajustats d'aquest.

Acreditar la certificació dels productes, recursos, serveis o sistemes per a l'operació de les xarxes 5G, o en alguna de les seves parts o elements. En particular, han de complir la certificació de l'esquema GSMA Network Equipment Security Assurance Scheme (NESAS) i les SCAS (Security Assurance Specification), per als elements de la xarxa 5G que sigui aplicable i per als restants qualsevol altre esquema d'assegurament de la seguretat equiparable.

També han de disposar, si s'escau, de les certificacions que recullen els esquemes europeus de certificació que es puguin desplegar en el Reglament 2019/881, del Parlament Europeu i del Consell, de 17 d'abril de 2019, relatiu a ENISA (Agència de la Unió Europea per a la Ciberseguretat), d'acord amb la normativa de requisits horitzontals de ciberseguretat per a productes amb elements digitals o d'acord amb qualsevol altra legislació relacionada de la UE o nacional.

Aquestes certificacions les han d'aportar als operadors perquè acompleixin el que estableix l'article 23, així com al Ministeri per a la Transformació Digital i de la Funció Pública.

c) Complir les normes o especificacions tècniques aplicables a xarxes i sistemes d'informació, de conformitat amb les normes nacionals, europees i internacionals.

Especialment, s'han de complir les mesures de seguretat aplicables a sistemes d'informació de categoria alta que estableix el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat o el perfil de compliment específic que sigui aplicable o, si s'escau, les que recull la norma tècnica ISO/IEC 27002:2022: Seguretat de la informació, ciberseguretat i protecció de la privacitat - Controls de seguretat de la informació, si no estan compreses en l'àmbit d'aplicació de l'Esquema Nacional de Seguretat o en el perfil de compliment específic que sigui aplicable.

d) Garantir l'aplicació de mesures de seguretat tècniques i organitzatives estàndard a través d'un sistema de certificació.

e) Efectuar una auditoria de seguretat dels seus equips, productes i serveis.

En particular, els subministradors 5G han de presentar al Ministeri per a la Transformació Digital i de la Funció Pública amb una periodicitat biennal una auditoria sobre l'aplicació de l'esquema de certificació GSMA Network Equipment Security Assurance Scheme (NESAS) i les SCAS (Security Assurance Specification), per als elements de la xarxa 5G que sigui aplicable i per als elements restants qualsevol altre esquema d'assegurament de la seguretat equiparable, a més de la norma tècnica ISO/

IEC 27001: Gestió de seguretat de la informació, el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, o el perfil de compliment específic que sigui aplicable, en la categoria de seguretat alta, en cas de fabricar, importar, distribuir o prestar qualssevol altres serveis, en xarxes públiques 5G.

A més, s'han de sotmetre, a costa seva, a una auditoria de seguretat ordinària, almenys cada dos anys, que verifiqui el compliment dels requeriments de l'ENS5G.

Amb caràcter extraordinari, s'ha de fer aquesta auditoria sempre que es produeixin modificacions substancials que puguin repercutir en les mesures de seguretat requerides. La realització de l'auditoria extraordinària determina la data de còmput per al càlcul dels dos anys, establerts per a la realització de l'auditoria regular ordinària següent, que indica el paràgraf anterior.

L'informe d'auditoria ha de dictaminar sobre el grau de compliment d'aquest Reial decret i identificar les troballes de compliment i incompliment detectades. Ha d'incloure, igualment, els criteris metodològics d'auditoria utilitzats, l'abast i l'objectiu de l'auditoria, i les dades, els fets i les observacions en què es basin les conclusions formulades.

El resultat d'aquesta auditoria s'ha de presentar al Ministeri per a la Transformació Digital i de la Funció Pública amb una periodicitat biennal.

f) Proporcionar informació sobre possibles ingerències de tercers en el disseny, l'operació i el funcionament dels seus equips, productes i serveis.

g) Proporcionar als operadors 5G i usuaris corporatius 5G la informació i acreditar el compliment d'estàndards de seguretat d'equips, productes i serveis que subministrin. Col·laborar per fer un monitoratge correcte o detecció de la ciberseguretat per part dels centres d'operacions de seguretat 5G que puguin crear els subjectes obligats.

3. Els subministradors 5G han d'aportar al Ministeri per a la Transformació Digital i de la Funció Pública una descripció de les mesures tècniques i organitzatives dissenyades i aplicades per detectar, gestionar i mitigar els riscos, quan se'ls requereixi.

4. No obstant el que disposa l'apartat anterior, els subministradors 5G que hagin estat qualificats d'alt risc o de risc mitjà han de remetre al Ministeri per a la Transformació Digital i de la Funció Pública un informe de les mesures tècniques i organitzatives dissenyades i aplicades per gestionar i mitigar els riscos en el termini de sis mesos a comptar des que hagin estat qualificats d'alt risc o de risc mitjà.

5. Els subministradors 5G d'alt risc i de risc mitjà han de remetre al Ministeri per a la Transformació Digital i de la Funció Pública cada dos anys una descripció de les mesures tècniques i organitzatives dissenyades i aplicades per detectar, gestionar i mitigar els riscos, o quan el Ministeri per a la Transformació Digital i de la Funció Pública ho requereixi, sempre que s'hagin produït canvis significatius en les infraestructures 5G utilitzades o serveis 5G prestats que indueixin a pensar que les mesures de seguretat adoptades puguin haver perdut eficàcia.

6. Els subministradors 5G són els responsables de la definició i execució de les mesures de mitigació de riscos que duguin a terme i del compliment de les obligacions d'informació i remesa de documentació que estableix aquest article.

Article 25. *Gestió de seguretat pels usuaris corporatius 5G.*

1. Els usuaris corporatius 5G que tinguin atorgats drets d'ús del domini públic radioelèctric per instal·lar, desplegar o explotar una xarxa privada 5G o prestar serveis 5G per a fins professionals o en autoprestació han de garantir la instal·lació, el desplegament i l'explotació segurs de xarxes privades 5G i prestació segura de serveis 5G en autoprestació mitjançant l'aplicació de tècniques i procediments d'operació i supervisió que garanteixin la seguretat de les xarxes i els serveis 5G.

2. Els usuaris corporatius 5G esmentats han d'aportar al Ministeri per a la Transformació Digital i de la Funció Pública una descripció de les mesures tècniques i organitzatives dissenyades i aplicades per gestionar i mitigar els riscos, quan se'ls requereixi.

Article 26. *Gestió de seguretat per les administracions públiques.*

1. Les administracions públiques incloses en l'àmbit d'aplicació d'aquest esquema han d'adoptar mesures tècniques i d'organització adequades per gestionar els riscos existents en la instal·lació, el desplegament i l'explotació de xarxes 5G i en la prestació de serveis 5G.

2. En particular, les administracions públiques que vulguin dur a terme la instal·lació, el desplegament i l'explotació de xarxes 5G, siguin públiques o privades, o la prestació de serveis 5G, disponibles al públic o en autoprestació, per raons de seguretat nacional, no poden utilitzar equips, productes i serveis proporcionats per subministradors d'alt risc o risc mitjà.

3. Cada òrgan o entitat de l'Administració pública inclosa en l'àmbit d'aplicació d'aquest esquema ha de disposar d'una política de seguretat referida als sistemes, les xarxes i els serveis 5G, formalment aprovada per l'òrgan competent. Aquesta política de seguretat pot determinar la inclusió de la totalitat o una part d'òrgans administratius o entitats pertanyents al sector públic institucional en l'àmbit d'aplicació d'una sola política de seguretat.

Article 27. *Gestió de seguretat pels centres d'operacions de seguretat 5G.*

1. Els subjectes obligats poden constituir centres d'operacions de seguretat 5G, que han d'adoptar mesures tècniques, operatives i d'organització adequades i proporcionades per garantir la preparació, la capacitat de resposta i la recuperació davant d'incidents, inclosa la cooperació entre els sectors públic i privat, així com per gestionar els riscos que es plantegin per a la seguretat dels sistemes, les xarxes i els serveis 5G, per a la qual cosa han d'adoptar mesures per gestionar aquests riscos de conformitat amb el que preveu aquest esquema.

2. Les mesures a les quals es refereix l'apartat anterior s'han de fonamentar en un enfocament holístic dels riscos, la probabilitat que produeixin els incidents i la seva gravetat, incloses les seves repercussions socials i econòmiques, i han d'incloure, almenys, els elements següents:

a) Les polítiques de seguretat de cada element de la xarxa i la seva anàlisi de riscos corresponent.

b) El procediment de gestió en cas d'incidents.

c) L'anàlisi de la continuïtat de les activitats, la gestió de còpies de seguretat i la recuperació en cas de catàstrofe, i la gestió de crisis.

d) La seguretat de la cadena de subministrament, inclosos els aspectes de seguretat relatius a les relacions entre cada subjecte obligat i els seus proveïdors o prestadors de serveis directes.

e) La seguretat en l'adquisició, el desenvolupament i el manteniment dels sistemes, les xarxes i els serveis 5G, inclosa la gestió i divulgació de les vulnerabilitats.

f) Les polítiques i els procediments per avaluar l'eficàcia de les mesures per a la gestió de riscos de ciberseguretat.

g) Les pràctiques bàsiques de ciberhigiene i formació en ciberseguretat.

h) Les polítiques i els procediments relatius a la utilització de criptografia i, si s'escau, de xifratge.

i) La seguretat dels recursos humans, les polítiques de control d'accés i la gestió d'actius.

j) L'ús de solucions d'autenticació multifactorial o d'autenticació contínua, comunicacions de veu, vídeo i text i sistemes segurs de comunicacions d'emergència en l'entitat, quan escaigui.

k) El monitoratge o la detecció de la ciberseguretat en les xarxes i els serveis 5G i entre els seus components o la seva relació amb altres xarxes.

3. Els subjectes obligats i els centres d'operacions de seguretat 5G creats han de col·laborar i cooperar amb el Centre d'Operacions de Seguretat 5G de referència al qual es refereix l'article 41 en el desplegament de les seves funcions, a través, entre d'altres, de les actuacions següents:

a) Establir mecanismes segurs d'intercanvi d'informació.
b) Dur a terme reunions periòdiques per tractar, entre altres assumptes, l'estat de situació de la ciberseguretat 5G i estudiar possibles millores.
c) Designar una persona que ha d'exercir com a punt de contacte amb els responsables de la seguretat de la informació nomenats pels subjectes obligats del sector de les telecomunicacions en virtut de l'article 7 del RD 43/2021, pel qual desplega el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació.

Article 28. *Prestació de serveis de resposta a incidents de seguretat.*

1. La notificació d'incidents s'ha de dur a terme segons els termes que estableix el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació i el Reial decret 43/2021, de 26 de gener, pel qual es desplega el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació, o d'acord amb la normativa que pugui reemplaçar aquesta regulació fruit de la transposició de la Directiva (UE) 2022/2555 del Parlament Europeu i del Consell, de 14 de desembre de 2022, relativa a les mesures destinades a garantir un nivell comú elevat de ciberseguretat a tota la Unió.
2. L'INCIBE-CERT, de l'Institut Nacional de Ciberseguretat d'Espanya, ha de prestar els serveis de resposta a incidents de seguretat que es produeixin en els sistemes, les xarxes i els serveis 5G dels subjectes obligats que no siguin entitats del sector públic i, en conseqüència, no estiguin inclosos en l'àmbit subjectiu d'aplicació de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
A aquest efecte, en l'exercici d'aquesta comesa, INCIBE-CERT ha d'exercir les funcions i implementar els procediments oportuns en els termes que indica el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació i el Reial decret 43/2021, de 26 de gener, pel qual es desplega el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació.
3. El CCN-CERT ha de prestar els serveis de resposta a incidents de seguretat que es produeixin en els sistemes, les xarxes i els serveis 5G dels subjectes obligats que siguin entitats del sector públic i, en conseqüència, estiguin inclosos en l'àmbit subjectiu d'aplicació de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
A aquest efecte, en l'exercici d'aquesta comesa, CCN-CERT ha d'exercir les funcions i implementar els procediments oportuns en els termes que indica el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació, i el Reial decret 43/2021, de 26 de gener, pel qual es desplega el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació.
4. L'ESPDEF-CERT, del Comandament Conjunt del Ciberespai, ha de cooperar amb el CCN-CERT i l'INCIBE-CERT en les situacions que aquests requereixin en suport dels operadors 5G i, necessàriament, en aquells operadors que tinguin incidència en la defensa nacional.
5. La cooperació i coordinació oportunes entre INCIBE-CERT, CCN-CERT i ESPDEF-CERT s'ha de dur a terme de conformitat amb el que indiquen el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació, i el Reial decret 43/2021, de 26 de gener, pel qual es desplega el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació.
6. Mitjançant una ordre del Ministeri per a la Transformació Digital i de la Funció Pública s'estableixen la tipologia d'incidents i els protocols d'actuació i comunicació perquè el Ministeri per a la Transformació Digital i de la Funció Pública, a través del

Centre d'Operacions de Seguretat 5G de referència, conegui els incidents de seguretat que es produeixin en els sistemes, les xarxes i els serveis 5G dels subjectes obligats.

Article 29. *Condicions de compliment de les obligacions.*

En el compliment de les obligacions que estableixen els articles anteriors, els subjectes obligats han de tenir en compte i aplicar el que estableixen el Reial decret llei 7/2022, de 29 de març, aquest esquema i els actes que es dictin en execució d'ambdues disposicions.

Article 30. *Confidencialitat de la informació sobre gestió de riscos.*

1. El Ministeri per a la Transformació Digital i de la Funció Pública pot obtenir dels subjectes obligats la informació necessària per a la gestió de riscos.
2. Els subjectes obligats han de proporcionar la informació en el termini de quinze dies hàbils a comptar de l'endemà de la notificació del requeriment d'informació.
3. L'incompliment dels requeriments d'informació formulats de conformitat amb el que indica l'apartat anterior, quan hagi passat un mes des de la finalització del termini donat per al seu compliment, és qualificat d'infracció greu.
4. S'ha de garantir la confidencialitat de la informació que els subjectes obligats proporcionin sobre l'anàlisi de riscos i no es pot utilitzar per a una finalitat diferent del compliment dels objectius i les obligacions que estableixen el Reial decret llei 7/2022, de 29 de març, aquest esquema i els actes que es dictin en execució d'ambdues disposicions.

CAPÍTOL VI

Altres mesures de compliment en matèria de la seguretat de les xarxes i els serveis 5G

Article 31. *Deure de col·laboració en la modificació i execució de l'ENS5G.*

Tots els subjectes obligats, així com les administracions públiques, els fabricants, importadors, distribuïdors i els que posin en el mercat i comercialitzin equips terminals i dispositius per connectar-se a una xarxa 5G i poder prestar serveis 5G, han de prestar la col·laboració i remetre la informació que se'ls requereixi per a la modificació i execució de l'ENS5G.

Article 32. *Certificació d'equips, productes i serveis 5G.*

Mitjançant una ordre de la persona titular del Ministeri per a la Transformació Digital i de la Funció Pública es pot supeditar la utilització d'un equip, sistema, programa o servei en concret pels subjectes obligats a l'obtenció prèvia d'una certificació establerta en virtut del Reglament (UE) 2019/881 del Parlament Europeu i del Consell, de 17 d'abril de 2019, relatiu a ENISA (Agència de la Unió Europea per a la Ciberseguretat), o dels esquemes de certificació i normes tècniques de certificació d'equips i productes 5G que en l'àmbit europeu o internacional es puguin aprovar, o qualsevol altra legislació de la UE o nacional que així ho requereixi en cas que no n'hi hagi.

Article 33. *Procediments de determinació de la conformitat amb l'Esquema Nacional de Seguretat 5G.*

1. Els subjectes obligats són objecte d'un procés per determinar la seva conformitat amb l'ENS5G. A aquest efecte, necessiten una auditoria per a la certificació de la seva conformitat, sens perjudici de l'auditoria de la seguretat que preveuen els articles 23 i 24 que també pot servir per als fins de la certificació.

Tant l'auditoria que preveuen els articles 23 i 24 com l'auditoria de certificació s'han de fer en els termes que determini la instrucció tècnica de seguretat corresponent, que també ha de concretar els requisits exigibles a les entitats certificadores.

2. Els subjectes obligats als quals fa referència l'apartat anterior donen publicitat, en els portals d'internet corresponents o les seus electròniques, a les certificacions de conformitat amb l'ENS5G, tenint en compte el que disposa la instrucció tècnica de seguretat esmentada.

Article 34. *Compliment de la normativa sobre inversions estrangeres i sobre competència.*

Les obligacions que estableixen el Reial decret llei 7/2022, de 29 de març, aquest esquema i els actes que es dictin en execució d'ambdues disposicions s'entenen sens perjudici de l'aplicació dels instruments de control sobre inversions estrangeres directes, així com de l'aplicació de la normativa en matèria de defensa de la competència.

Article 35. *Equips terminals.*

La fabricació, importació, distribució, posada en el mercat i comercialització d'equips terminals i dispositius per connectar-se a una xarxa 5G i poder prestar serveis 5G està condicionat al compliment dels requisits de seguretat per als productes digitals i dels requisits essencials aplicables relacionats amb la ciberseguretat, adoptats de conformitat amb la normativa europea, en particular, amb relació a la protecció de les dades personals, la privacitat, i la protecció contra el frau.

Article 36. *Cooperació internacional.*

1. El Govern i el Ministeri per a la Transformació Digital i de la Funció Pública han de cooperar estretament amb les institucions d'altres estats membres de la Unió Europea i amb les institucions de la Unió Europea en la proposta de modificació i execució de l'Esquema Nacional de Seguretat de xarxes i serveis 5G i, en general, han de col·laborar amb les diferents organitzacions internacionals especialitzades per poder dur a terme un tractament integral i global de la seguretat de les xarxes i els serveis 5G.

2. En particular, el Govern i el Ministeri per a la Transformació Digital i de la Funció Pública poden compartir informació relacionada amb les anàlisis que facin les institucions de la Unió Europea i amb altres estats membres de la Unió Europea i preservar, com correspon en dret, la seguretat, els interessos comercials i la confidencialitat de la informació recollida en l'elaboració de l'anàlisi, així com utilitzar la informació que li enviïn altres estats o les institucions de la Unió Europea per a la seva realització. Igualment, poden portar a terme aquestes anàlisis de manera conjunta amb altres estats membres de la Unió Europea.

Article 37. *R+D+I en ciberseguretat 5G.*

El Ministeri per a la Transformació Digital i de la Funció Pública, directament o a través del Centre d'Operacions de Seguretat 5G de referència, ha d'impulsar l'R+D+I en ciberseguretat 5G mitjançant l'execució de diferents programes en què s'han de seguir les línies generals següents:

a) Establiment de programes de recerca i desenvolupament R+D+I en ciberseguretat 5G, amb l'objectiu de promoure la innovació i el desenvolupament de tecnologies avançades per protegir les xarxes i els serveis 5G contra possibles amenaces i ciberatacs.

b) Convocatòria d'ajudes públiques per finançar projectes de recerca en ciberseguretat 5G, amb la finalitat d'impulsar la generació de coneixement i la col·laboració entre diferents actors del sector.

c) Foment de la col·laboració publicoprivada en R+D+I en ciberseguretat 5G, a través de la creació de programes de finançament conjunt, l'organització d'esdeveniments i la facilitació de la transferència de tecnologia entre empreses i institucions de recerca.

d) Establiment de programes de suport específics per a *startups* i empreses emergents que desenvolupin solucions innovadores en ciberseguretat 5G, proporcionant finançament, i accés a infraestructures i recursos de recerca.

e) Promoció de la formació i capacitació de personal especialitzat en ciberseguretat 5G, en col·laboració amb els ministeris competents, per a la creació de programes de formació universitària i professional, l'organització de cursos i seminaris especialitzats, i el foment de la participació en programes de beques i pràctiques en empreses del sector.

f) Establiment d'estàndards i bones pràctiques en ciberseguretat 5G, amb l'objectiu de garantir la interoperabilitat, la seguretat i la protecció de la privacitat en les xarxes i els serveis 5G.

Article 38. *Impuls a la interoperabilitat.*

El Ministeri per a la Transformació Digital i de la Funció Pública, directament o a través del Centre d'Operacions de Seguretat 5G de referència, ha d'impulsar la interoperabilitat dels equips i programes lligats a la gestió de xarxes i serveis 5G, així com la participació d'actors públics i privats en l'elaboració d'estàndards sobre el funcionament de les xarxes i els serveis 5G a través de les iniciatives següents:

a) Aprovació de normatives i directrius clares per promoure la interoperabilitat dels equips i programes relacionats amb la gestió de xarxes i serveis 5G, incloent-hi la definició d'estàndards tècnics i protocols de comunicació que facilitin la integració i la compatibilitat entre diferents sistemes i dispositius.

b) Impuls per a l'adopció d'estàndards oberts en el disseny i desenvolupament d'equips i programes per a xarxes i serveis 5G, amb l'objectiu de facilitar la interoperabilitat i evitar la dependència de tecnologies propietàries.

c) Creació d'espais de col·laboració entre actors públics i privats per discutir i elaborar estàndards sobre el funcionament de les xarxes i els serveis 5G.

d) Promoció de la interoperabilitat com un criteri d'avaluació en els processos de contractació pública relacionats amb l'adquisició d'equips i serveis per a xarxes i serveis 5G. Això podria incentivar els proveïdors a desenvolupar solucions compatibles i facilitar la integració de sistemes heterogenis en entorns públics.

CAPÍTOL VII

Aplicació de l'ENS5G

Article 39. *Competència per a l'aplicació de l'ENS5G.*

1. El Ministeri per a la Transformació Digital i de la Funció Pública és el departament competent per aplicar l'ENS5G i exercir les altres funcions que li atribueix el Reial decret llei 7/2022, de 29 de març.

2. El Ministeri per a la Transformació Digital i de la Funció Pública, per a l'exercici d'aquestes funcions, disposa del suport i l'assistència del Centre d'Operacions de Seguretat 5G de referència al qual es refereix l'article 41.

3. Així mateix, el Ministeri per a la Transformació Digital i de la Funció Pública, per a la resposta a incidents de seguretat, compta amb la cooperació d'INCIBE-CERT, CCN-CERT i ESPDEF-CERT.

4. El Ministeri per a la Transformació Digital i de la Funció Pública s'ha de coordinar amb els altres òrgans competents en matèria de ciberseguretat i infraestructures crítiques per garantir una aplicació coherent de l'ENS5G.

Article 40. *Facultats del Ministeri per a la Transformació Digital i de la Funció Pública per a l'aplicació de l'ENS5G.*

1. El Ministeri per a la Transformació Digital i de la Funció Pública, en l'exercici de les funcions que li assignen el Reial decret llei 7/2022, de 29 de març, i l'ENS5G, pot exercir, entre d'altres, les facultats següents:

a) Desenvolupar, concretar i detallar el contingut de l'ENS5G.
b) Autoritzar la instal·lació, modificació o adaptació d'estacions radioelèctriques que proporcionin cobertura a determinades ubicacions, àrees i centres en els termes que estableix l'article 16.4.
c) Formular requeriments d'informació als subjectes obligats, que s'han de respondre en el termini de 15 dies hàbils a comptar de l'endemà de la seva notificació, a l'efecte de poder exercir les funcions que li assignen el Reial decret llei 7/2022, de 29 de març, l'ENS5G i la seva normativa de desplegament i, en concret, per verificar i controlar el compliment de les obligacions respectives que s'imposen als subjectes obligats.
d) Fer auditories o ordenar la seva realització per verificar i controlar el compliment de les obligacions respectives que el Reial decret llei 7/2022, de 29 de març, l'ENS5G i la seva normativa de desplegament imposen als subjectes obligats.
e) Efectuar inspeccions pels funcionaris destinats a la Secretaria d'Estat de Telecomunicacions i Infraestructures Digitals i exercir la potestat sancionadora en els termes que indica el capítol següent.
f) Concedir ajudes públiques.
g) Desenvolupar iniciatives per fomentar la recerca i el desenvolupament en matèria de seguretat en les xarxes i els serveis 5G i per a la formació de personal especialitzat.
h) Crear laboratoris que recreïn entorns de xarxes i serveis 5G reals i independents per a l'anàlisi i gestió de riscos de seguretat i per a l'assegurament del compliment dels requisits de l'ENS5G.
i) Exercir les altres funcions que li corresponguin segons la legislació aplicable.

2. El Ministeri per a la Transformació Digital i de la Funció Pública, per a l'exercici d'aquestes funcions, disposa del suport i l'assistència del Centre d'Operacions de Seguretat 5G de referència al qual es refereix l'article 41.

Article 41. *Centre d'Operacions de Seguretat 5G de referència.*

1. Dependent del Ministeri per a la Transformació Digital i de la Funció Pública, es crea el Centre d'Operacions de Seguretat 5G de referència, òrgan de suport i supervisió de les actuacions conduents a garantir la seguretat dels sistemes, les xarxes i els serveis 5G.
2. El Centre d'Operacions de Seguretat 5G de referència té les funcions següents:

a) Contribuir i donar suport a l'exercici de les facultats que s'assignen al Ministeri per a la Transformació Digital i de la Funció Pública en l'article 40.
b) Proporcionar suport operatiu als subjectes obligats en activitats vinculades a la prevenció, protecció, detecció i resposta davant d'amenaces, incidents i ciberatacs als sistemes, les xarxes i els serveis 5G, així com en la certificació i normalització d'aquests.
c) Fomentar la prevenció dels sistemes, les xarxes i els serveis 5G mitjançant activitats destinades a ampliar el coneixement respecte a les vulnerabilitats, tant tècniques com humanes, i reduir la superfície d'exposició, com poden ser la realització d'auditories, d'inspeccions tècniques de seguretat, la gestió de vulnerabilitats, l'anàlisi de vulnerabilitats automatitzada o no, el registre i seguiment de les vulnerabilitats identificades, el seguiment de la publicació de vulnerabilitats específiques relacionades amb el 5G, i suport a la posada en pràctica de remeis a aquestes vulnerabilitats.
d) Capacitació i formació específica en matèria de ciberseguretat 5G.

e) Assessorar els subjectes obligats i els seus centres d'operacions de seguretat 5G sobre el disseny de les mesures de seguretat, de les eines que cal utilitzar, el desenvolupament de guies específiques i l'aplicació de les mesures de protecció.

f) Oferir serveis de seguiment en el funcionament i l'operativitat dels sistemes, les xarxes i els serveis 5G per detectar i respondre ràpidament a possibles amenaces i ciberatacs.

g) Contribuir a la resposta d'incidents de seguretat.

h) Desenvolupar plans i procediments de gestió de crisis de ciberseguretat i plans de contingència 5G en l'àmbit nacional.

i) Proporcionar suport en l'obtenció de les certificacions tant d'àmbit nacional com europeu.

j) Identificar i difondre millors pràctiques d'implementació de ciberseguretat 5G entre els subjectes obligats.

k) Elaborar guies i documents de millors pràctiques per a la implementació i operació dels sistemes, les xarxes i els serveis 5G, i abordar aspectes com la seguretat, la privacitat i la gestió de riscos.

l) Avaluar l'impacte dels estàndards i la normativa en matèria de ciberseguretat 5G, i proporcionar informació i assessorament als responsables de formular polítiques per garantir un entorn propici per a l'adopció i el desenvolupament de la tecnologia 5G.

m) Dur a terme activitats d'R+D+I en l'àmbit de la ciberseguretat 5G, per detectar, anticipar, prevenir i millorar la resposta davant d'incidents potencials.

n) Qualsevol altra funció que li assigni el Ministeri per a la Transformació Digital i de la Funció Pública.

3. Per a l'exercici d'aquestes funcions, el Centre d'Operacions de Seguretat 5G de referència s'integra en l'estructura de ciberseguretat nacional en el marc del Sistema de Seguretat Nacional, pot subscriure els convenis i mecanismes de col·laboració oportuns amb entitats especialitzades en matèria de ciberseguretat i protecció d'operadors 5G i, si s'escau, protecció de les entitats crítiques, entre d'altres, l'Institut Nacional de Ciberseguretat d'Espanya, el Comandament Conjunt del Ciberespai, el Centre Criptològic Nacional, l'Oficina de Coordinació de Ciberseguretat i el Centre Nacional de Protecció d'Infraestructures Crítiques del Ministeri de l'Interior.

CAPÍTOL VIII

Inspecció i règim sancionador

Article 42. *Facultats d'inspecció.*

El Ministeri per a la Transformació Digital i de la Funció Pública exerceix en l'aplicació i supervisió del que estableixen el Reial decret llei 7/2022, de 29 de març, l'ENS5G i la seva normativa de desplegament totes les potestats de la funció inspectora que preveuen aquestes normes i el títol VIII de la Llei 11/2022, de 28 de juny, general de telecomunicacions.

Article 43. *Règim sancionador.*

És aplicable el règim sancionador que estableixen els articles 30 i 31 del Reial decret llei 7/2022, de 29 de març.

ANNEX I

Elements, infraestructures i recursos que integren una xarxa 5G

1. Desc%ripció de l'arquitectura de la xarxa 5G-SA

Per a l'anàlisi requerida en aquest Esquema Nacional de Seguretat de xarxes i serveis 5G, s'utilitza una arquitectura de xarxa de referència, seguint la recomanació del 3GPP i l'especificació ETSI TS 123 501.

En la figura següent, es mostra un esquema simplificat d'una arquitectura 5G-SA per a escenaris de no-itinerància (que s'utilitza de forma genèrica com a base). Elements no presentats en la figura són el UDR, UDSF, UCMF, CHF, 5G-EIR, NWDAF i SEPP.

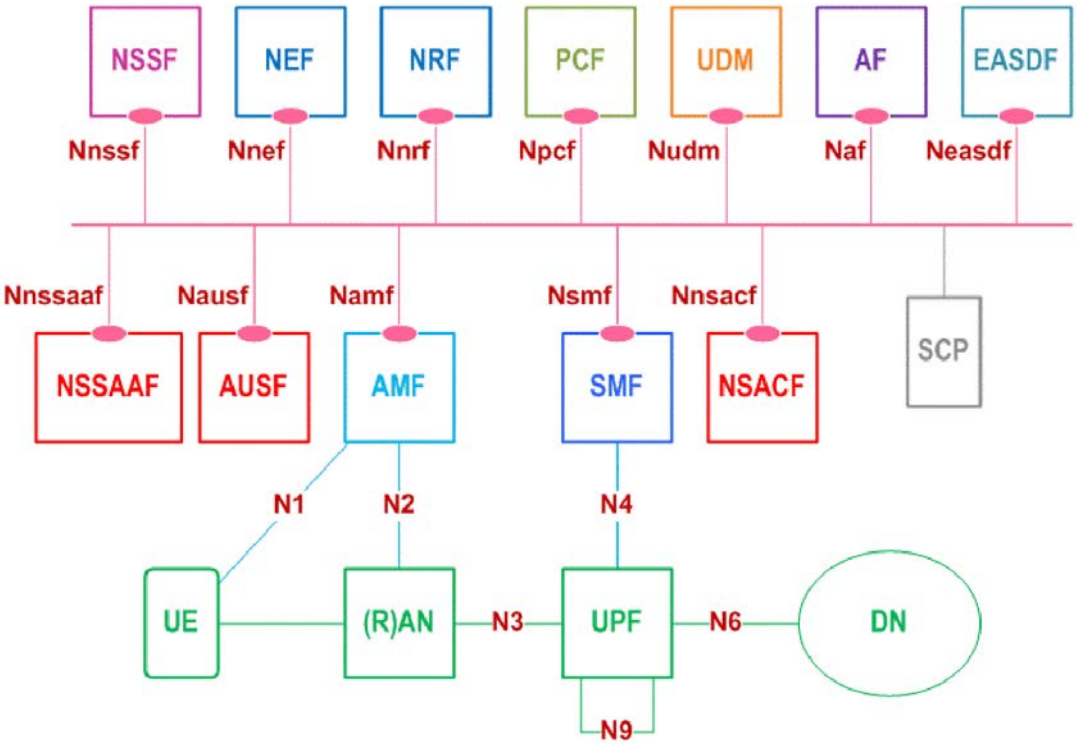


Fig. 1: Arquitectura 5G segons especificació ETSI TS 123 501

Aquests elements de xarxa són funcions programari que es despleguen sobre una infraestructura de virtualització (composta, al seu torn, de maquinari i programari de virtualització), la qual pot ser exclusiva i específica per a una funció de xarxa, o comuna per a diverses funcions, fins i tot funcions de xarxa de diversos subministradors 5G. En aquest escenari, la infraestructura per allotjar les funcions de xarxa virtualitzades pot estar diversificada tant geogràficament com per subministradors 5G diferents, tal com es descriu més endavant en aquest document.

Addicionalment als elements de xarxa, es despleguen un conjunt de sistemes per a l'operació i gestió de la xarxa GER (també anomenats OSS, Operations Support System).

2. Identificació i descripció dels entorns de xarxa 5G-SA

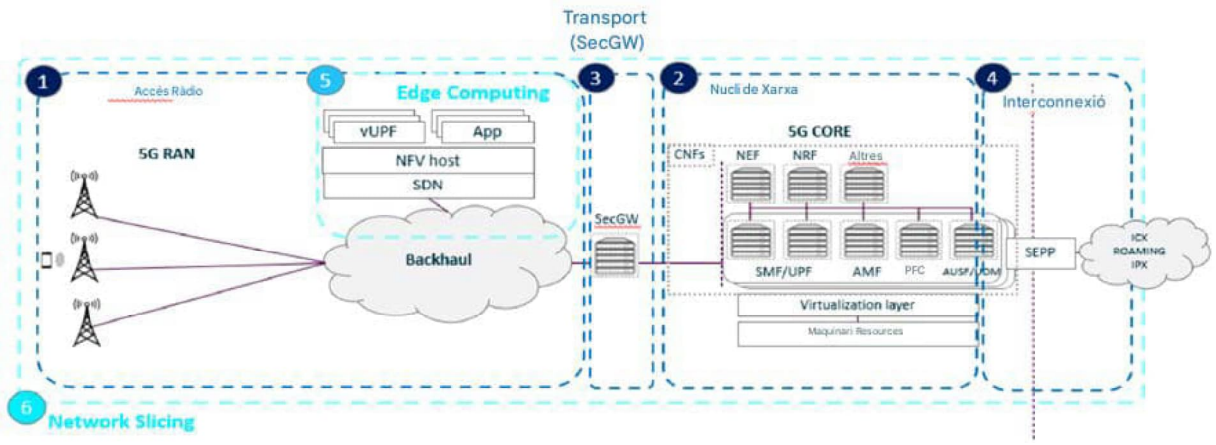
Amb l'objectiu de desglossar la complexitat de l'arquitectura d'una xarxa 5G-SA, aquesta es divideix en entorns de xarxa.

Un entorn de xarxa és una agrupació d'actius que tenen una comesa i unes característiques particulars dins de la xarxa que els diferencien de la resta d'entorns.

Es poden distingir dues tipologies d'entorn:

a) Entorns primaris: es consideren entorns primaris els propis de la tecnologia o naturalesa de 5G que no poden existir sense el seu desplegament.
b) Entorns secundaris: es consideren entorns secundaris els comuns en un operador de telecomunicacions.

En la figura següent (figura 2) es pot apreciar una classificació de la xarxa 5G-SA per entorns:



3. Entorns de xarxa primaris

Dins dels entorns de xarxa primaris, hi ha l'accés ràdio, el nucli de xarxa, el transport-Backhaul (SecGW), la interconnexió d'itinerància i els sistemes de control, gestió i operació de la xarxa.

a) Accés ràdio: l'entorn d'accés ràdio (RAN) s'encarrega de dotar de cobertura els terminals perquè aquests es puguin connectar a la xarxa. Destaquen les funcions següents en l'entorn:

1. Operació i manteniment de l'emplaçament ràdio. El programari permet configurar cada emplaçament amb una sèrie de cèl·lules per tecnologia per poder prestar servei als usuaris i, durant el funcionament de l'estació base, en supervisa l'estat per detectar possibles problemes o avaries, davant l'aparició dels quals reporta una alarma al sistema de gestió perquè l'operador en sigui conscient i resolgui el problema.
2. Senyalització. Perquè els usuaris es puguin registrar en la xarxa i establir serveis portadors per a les seves comunicacions, és necessària la senyalització entre els terminals, l'estació base, i el nucli de xarxa, i part d'aquestes funcions les fa el programari de l'estació base.
3. Gestió de recursos ràdio. Els recursos ràdio d'una cèl·lula donada són compartits entre diferents usuaris, i el programari de l'estació base és el responsable de repartir-los entre aquests usuaris (qualitat de l'enllaç ràdio de cada usuari, demanda de velocitat, etc.). El programari també pot distribuir els usuaris entre les cèl·lules de la seva estació base (o fins i tot amb cèl·lules d'emplaçaments veïns), perquè el repartiment d'usuaris sigui més homogeni entre cèl·lules veïnes.
4. Mobilitat. El programari de l'estació base gestiona el traspàs de les comunicacions dels usuaris entre diferents cèl·lules, del seu emplaçament o d'emplaçaments veïns, a mesura que els usuaris es desplacen per la xarxa.
5. Transport. La comunicació física amb la resta de la xarxa es fa mitjançant enllaços IP, elèctrics o òptics, i l'estació base s'ha d'encarregar de gestionar aquests enllaços (priorització entre els diferents tipus de trànsit que van per aquests enllaços, configuració de VLAN, supervisió de l'enllaç, etc.).

La xarxa 5G, en el pla d'accés ràdio (RAN), s'implementa amb un sol tipus d'element de xarxa anomenat, de forma genèrica, gNodeB (gNB). La majoria dels subministradors 5G de xarxa d'accés ràdio disposen de diferents models de gNB, adaptats a diferents tipus d'escenaris.

De forma genèrica, hi ha els tipus següents:

1. Macro gNB: proporcionen una àrea de cobertura i capacitat de trànsit més gran. S'instal·len típicament en terrats d'edificis o llocs amb molta visibilitat radioelèctrica, amb l'objectiu de donar cobertura i capacitat general.
2. Micro gNB: de menys potència, orientats a donar cobertura en localitzacions concretes, ja siguin petits espais públics (com ara places) o espais d'interior (com ara llocs d'esdeveniments, oficines petites, etc.), o bé per donar capacitat complementària a la capa general o macro. S'instal·len principalment en punts d'alta demanda de capacitat, per absorbir aquesta demanda.
3. Sistemes gNB de cobertura d'interiors: especialitzats a cobrir espais d'interiors grans, amb nombrosos punts radiants de baixa potència, per distribuir la cobertura 5G per aquest espai interior. S'instal·len típicament en grans edificis d'oficines, estadis esportius, metros, etc.

En aquest context, un emplaçament de la xarxa d'accés ràdio 5G està compost d'una banda base i de diversos caps remots o antenes actives. El nombre de caps remots i antenes actives depèn del nombre de bandes presents en l'emplaçament i del nombre de sectors.

El programari del gNB és comú a la banda base, als caps remots i a les antenes actives, i també és comú entre els diferents sistemes de comunicacions mòbils presents en l'emplaçament (2G, 3G, 4G o 5G). Mitjançant la interfície NG, l'estació base es comunica amb el nucli de xarxa i mitjançant la interfície aèria amb els terminals mòbils.

b) Nucli de xarxa: el nucli de la xarxa 5G-SA consta d'una sèrie de funcions de xarxa estandarditzades pel 3GPP que es comuniquen entre si per connexions tipus SBI (Service Based Interfaces) i permeten una malla total en funció de les necessitats de cadascuna d'aquestes.

Els principis clau d'aquesta arquitectura 5G-SA són:

1. Separar les funcions del pla d'usuari (UP) de les funcions del pla de control (CP), fet que permet escalabilitat independent, evolució i implementacions flexibles, per exemple, ubicació centralitzada o ubicació distribuïda (remota).
2. Modularitzar el disseny de la funció, per exemple, per permetre un tall de xarxa flexible i eficient.
3. Permetre que cada funció de xarxa (i els seus serveis associats) interactuïn amb altres funcions de xarxa, directament o indirectament a través d'un *Proxy*.
4. Integrar diferents tipus d'accés, per exemple, accés 3GPP i accés no 3GPP.
5. Suporta un marc d'autenticació unificat.
6. Desacoblar en les funcions de xarxa les funcions de lògica de tipus «stateless» i relacionades amb capacitat de còmput, de les funcions d'estat de tipus «statefull» relacionades amb capacitats d'emmagatzematge.
7. Permetre l'exposició de dades de xarxa de manera segura per al desenvolupament de nous serveis d'acord amb aquestes.
8. Suport d'accés simultani a serveis locals (amb requisits de baixa latència) i serveis centralitzats.
9. Permetre i acceptar la itinerància de trànsit amb altres xarxes, segons diferents models d'arquitectura.

El conjunt de funcions de nucli de xarxa definides pel 3GPP és el següent:

1. AMF - Access and Mobility Management Function: funció del pla de control de la xarxa 5G. Les seves funcions principals són la gestió del registre, la gestió de la

mobilitat, la gestió de la connexió i la gestió de diversos aspectes relacionats amb la seguretat i l'autorització dels accessos.

2. SMF - Session Management Function: funció del pla de control que s'encarrega de la gestió de les sessions (establiment, modificació i alliberament), gestió i assignació d'IP als terminals d'usuari. En resum, és la responsable d'interactuar amb el pla d'usuari, i crea, actualitza o esborra sessions PDU, a la vegada que administra el context de la sessió amb la UPF.

3. UPF - User Plane Function: funció del pla d'usuari. És la responsable del reenviament, l'encaminament i la inspecció de paquets, així com de la gestió de la qualitat de servei. Representa el punt d'interconnexió a la xarxa de dades.

4. PFC - Policy Control Function: és l'encarregada de proporcionar regles de polítiques a les funcions de xarxa del pla de control, incloent-hi *network slicing,* itinerància, gestió de mobilitat o polítiques de qualitat de servei 5G. Per a l'execució de les polítiques, accedeix a la informació de subscripció del UDR.

5. NRF - Network Repository Function: és l'encarregada del descobriment dels serveis, i manté el perfil i les instàncies de xarxa disponibles. Les seves funcions principals són la gestió del servei, el descobriment de serveis, i *access token,* i permet posar en comunicació dos elements de la xarxa 5G.

6. SEPP - Security Edge Protection Proxy: és la funció de xarxa que permet una interconnexió segura entre xarxes 5G, i garanteix la confidencialitat o integritat d'extrem a extrem entre la xarxa d'origen i la de destinació, per a tots els missatges d'itinerància d'interconnexió 5G.

7. UDM - Unified Data Management: funció del pla de control les principals missions de la qual són la generació de credencials d'autenticació, la gestió d'identitats d'usuari, la gestió de subscripció, l'autorització d'accés basat en dades de subscripció, i l'emmagatzematge i la gestió de les funcions de xarxa que donen servei a l'usuari. L'UDM utilitza les dades de subscripció emmagatzemades en el UDR.

8. UDR - Unified Data Repository: és el repositori unificat de dades d'usuari. Aquestes dades s'estructuren en diferents categories o tipus, i són accessibles a les diverses funcions de xarxa mitjançant una sèrie de serveis exposats per a la gestió i consulta d'aquests (UDM, PCR, NRF, etc., entre altres).

9. AUSF - Authentication Server Function: és la funció del pla de control de la xarxa 5G que s'encarrega de l'autenticació de l'usuari.

10. CHF - Charging Function: la funcionalitat de tarifació resideix en el tarificador convergent (CCS, Converged Charging System), que ofereix les funcionalitats de tarifació en línia i fora de línia. Entre les seves funcions, hi ha l'OCF (Online Charging Function), per efectuar el control en línia de les sessions de dades, el CDF (Charging Data Function), per construir un CDR amb la informació de xarxa rebuda, l'ABMF (Account Balance Management Function), per a la gestió del saldo i els controls de consum, l'RF (Rating Function), funció per establir un preu a l'ús rebut (tant en línia com fora de línia), i el CGF (Charging Gateway Function), per generar CDR tarifats.

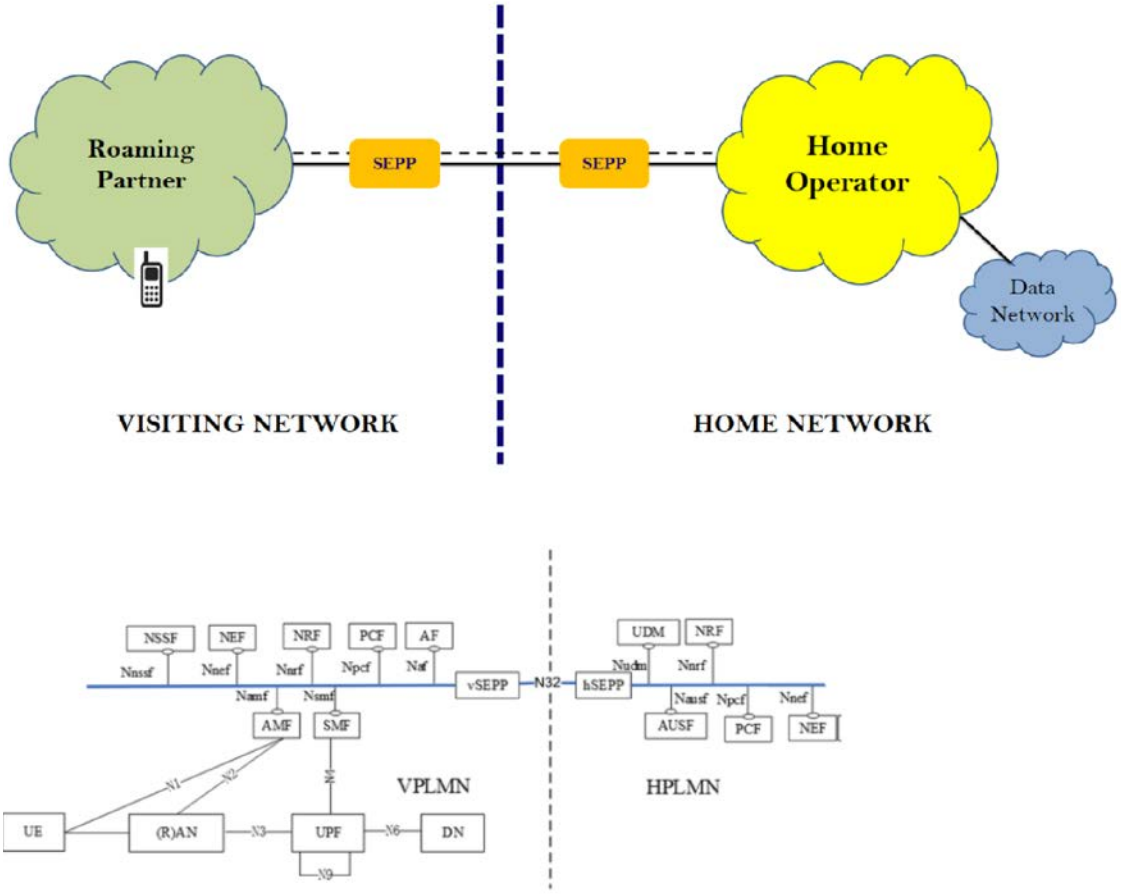
11. NEF - Network Exposure Function: proporciona un mitjà per exposar, de manera segura, els serveis i les capacitats oferts per les funcions de xarxa de 5G.

12. 5G-EIR-5G - Equipment Identity Register: és una funcionalitat opcional que ofereix la capacitat de revisar l'estatus de la identitat del terminal (IMEI) i comprovar que no sigui en una llista negra.

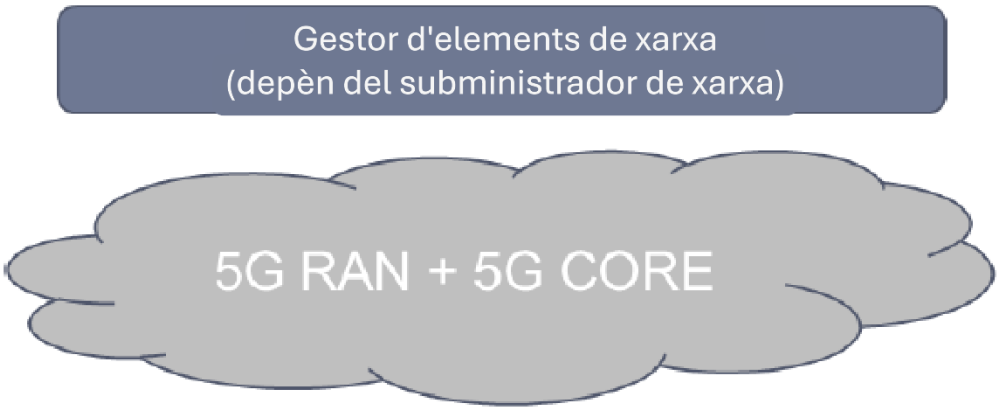
c) Transport-Backhaul (SecGW): el Security Gateway (SecGW) proporciona el xifratge del trànsit del pla de control i del pla d'usuari entre els entorns d'accés ràdio i de nucli de xarxa i, a més, evita exposicions innecessàries d'elements crítics.

d) Interconnexió itinerància: l'entorn d'Interconnexió itinerància és necessari per a la comunicació amb la resta dels operadors de cara a permetre que un usuari de 5G es pugui moure de manera internacional sense interrompre el seu servei de veu o banda ampla.

La figura següent (figura 3) conté la representació d'un entorn d'interconnexió d'itinerància:



e) Sistemes de control, gestió i operació i serveis de suport: el procés d'assegurament del nucli de xarxa 5G es basa en un conjunt de sistemes de suport a l'operació (OSS) que es mostren en la figura següent (figura 4).



Aquests sistemes OSS no formen part de la prestació del servei i, per tant, les fallades en el seu funcionament no afecten de manera directa la disponibilitat de la xarxa ni la qualitat del servei prestat sobre aquesta. Tanmateix, la indisponibilitat d'aquests sistemes pot afectar la capacitat de supervisió, anàlisi, configuració i planificació de la xarxa que descriu el punt anterior. Des del punt de vista de la seguretat, aquests sistemes gestors estan segmentats segons el subministrador i, per tant, una incidència

de seguretat en un d'aquests no afecta les funcions de xarxa que no estiguin sota l'empara d'aquest OSS.

4. Entorns de xarxa secundaris

Dins dels entorns de xarxa secundaris, hi ha les plataformes de virtualització, la infraestructura física, l'*Edge-Computing* i el *Network Slicing.*

a) Plataformes de virtualització i orquestració: molts dels elements d'una xarxa 5G són funcions «programari» que es despleguen sobre una infraestructura de virtualització (que, al seu torn, consta de maquinari i programari de virtualització), la qual pot ser exclusiva i específica per a una funció de xarxa, o comuna per a diverses funcions (fins i tot funcions de xarxa de diversos subministradors). En aquest context, la infraestructura per allotjar les funcions de xarxa virtualitzades està diversificada tant geogràficament com per subministradors diferents.

b) Infraestructura física: els elements i les funcions de xarxa pertanyents als diferents entorns requereixen una infraestructura física on emplaçar-los, la naturalesa, disponibilitat i seguretat dels quals depèn òbviament de la criticitat de l'actiu en concret. Aquesta infraestructura física atorga als elements i les funcions de xarxa les necessitats bàsiques per a un funcionament correcte.

c) MultiAccess Edge-Computing (MEC): l'*edge computing* multiaccés és un tipus d'arquitectura o entorn de xarxa que pretén portar les funcions de processament de trànsit d'usuari i *cloud computing* TI a l'extrem de la xarxa amb l'objectiu de garantir el funcionament de nous casos d'ús que requereixen una latència mínima.

En concepte, es defineix en termes més amplis com una evolució del *cloud computing* que utilitza les tecnologies mòbils i de núvol per separar els allotjadors d'aplicacions del centre de dades on són i traslladar-los cap a l'extrem de la xarxa. Això no només permet que els usuaris finals estiguin més a prop de les aplicacions, sinó també que els serveis informàtics estiguin més a prop de les dades que aquestes generen.

En aquest *Edge-Computing* conviuen tant aplicacions de tercers, com funcions de xarxa per processar en l'*Edge* el trànsit d'usuari.

d) Network Slicing: es tracta d'una forma d'arquitectura que ofereix la possibilitat de crear, sobre una infraestructura física de virtualització comuna compartida, diverses xarxes virtuals personalitzades i aïllades de manera lògica entre si, i atorga a cadascuna una criticitat determinada en funció de les necessitats específiques d'aplicacions, serveis, dispositius, clients o operadors.

Es preveu que, amb aquesta tecnologia, els operadors de xarxes i serveis 5G puguin implementar una segmentació de xarxa per crear múltiples xarxes virtuals amb diferents mides de connectivitat, adaptar-se a les necessitats de connexió dels diferents usuaris, i assignar de forma específica els recursos necessaris per garantir el servei correcte.

En línies generals, dins del concepte *network slicing,* cada xarxa virtual (o porció de la xarxa) engloba un conjunt independent de funcions lògiques de xarxa que suporten els requeriments del cas d'ús particular. Cadascun d'aquests s'optimitza per brindar els recursos i raonaments matemàtics de xarxa per al servei i el trànsit que s'utilitza en la segmentació.

En el cas de la tecnologia 5G-SA, capacitat, connectivitat, varietat, velocitat, cobertura i seguretat s'assignen per satisfer les demandes específiques de cada cas d'ús.

ANNEX II

Anàlisi de riscos en l'àmbit nacional

1. Metodologia utilitzada

Una anàlisi de riscos té com a objectiu identificar i categoritzar les principals amenaces sobre les xarxes i els serveis 5G, amb la finalitat de determinar mesures correctives que puguin disminuir-ne les conseqüències o fins i tot evitar-les.

Coneixent aquesta finalitat, el pas lògic següent és establir els mitjans per assolir aquest objectiu. Una anàlisi de riscos s'ha de fer amb una metodologia estandarditzada, holística i un ordre conseqüent i lògic, i cal detallar cadascun dels aspectes de manera qualitativa i quantitativa. En cas contrari, el nivell de risc calculat es pot desvirtuar i també els criteris i les prioritats en les mesures de protecció o accions clau que cal dur a terme.

A continuació es mostren les fases seguides per a l'anàlisi efectuada, així com les fonts d'informació utilitzades per a la metodologia emprada.

a) Identificació i descripció de l'arquitectura 5G, els entorns de xarxa existents en aquesta i els actius que la componen, tot això subjecte a l'evolució tecnològica (vegeu annex I).

b) Identificació de criticitat per als actius dins de cadascuna de les parts o elements d'una xarxa 5G, siguin parts o elements crítics o no de la xarxa 5G en els termes que indiquen l'article 6, apartats 2 i 3, del Reial decret llei 7/2022, de 29 de març, i els articles 5 i 6 i l'annex I d'aquest esquema: per poder identificar l'impacte d'una amenaça en la xarxa, primer cal determinar la criticitat de cadascun dels actius, d'acord amb les cinc dimensions de seguretat (confidencialitat, integritat, traçabilitat, autenticitat i disponibilitat).

c) Identificació dels riscos de la tecnologia 5G i el seu impacte en els actius identificats: determinar les amenaces potencials presents en aquest entorn específic, classificar-les per actiu i identificar-ne el nivell de risc.

d) Identificació de les mesures de seguretat tècniques, organitzatives i estratègiques, per pal·liar o reduir el nivell de risc de les amenaces identificades per a cada entorn de xarxa. La seva efectivitat és directament proporcional al grau de disminució del nivell de risc per a una amenaça i actiu determinats.

e) Gestió dels riscos i riscos romanents, en les amenaces el nivell de les quals sigui considerable i no es pugui reduir amb cap mesura addicional des del disseny (vegeu annex III).

2. Dimensions de seguretat que afecten la criticitat d'un actiu

De manera estandarditzada i àmpliament reconeguda, es consideren cinc dimensions de seguretat a l'hora d'avaluar la criticitat dels actius dins de cadascuna de les parts o elements d'una xarxa 5G, siguin parts o elements crítics o no de la xarxa 5G en els termes que indiquen l'article 6, apartats 2 i 3, del Reial decret llei 7/2022, de 29 de març, i els articles 5 i 6 i l'annex I d'aquest esquema, quan cal avaluar la seguretat d'una solució.

Les cinc dimensions de seguretat són confidencialitat, integritat, traçabilitat, autenticitat i disponibilitat.

a) Confidencialitat: la confidencialitat en un actiu o una xarxa valora la capacitat d'evitar que la informació que conté l'actiu, o que està en trànsit en la xarxa, s'exposi a usuaris no autoritzats, els quals no hi han de tenir accés i la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.

Les mesures de seguretat per garantir la confidencialitat són diverses, des de la segmentació i el control d'accés, fins al xifratge robust de la informació. El factor principal a l'hora de valorar la importància de la confidencialitat en un actiu és la sensibilitat de la informació que emmagatzema o transita per aquest. És important tenir en compte, quan

es considera aquest factor, l'impacte que pot tenir per a la resta de la xarxa el fet que es comprometi aquell actiu.

Exemples de riscos que puguin comprometre la confidencialitat són els següents: espiar o interceptar el trànsit o les dades d'usuari en la xarxa (*Man in the Middle*, *Eavesdropping*), o obtenir les credencials dels operadors, ja sigui a causa d'una configuració errònia de la xarxa, a l'absència de polítiques de segmentació i de control d'accés als actius, o, per exemple, a l'absència de xifratge en interfícies exposades.

b) Integritat: la integritat és la capacitat de garantir que les dades d'un actiu, usuari o xarxa durant el seu cicle de vida, sigui en trànsit o emmagatzemades, només les modifiquen agents autoritzats per a això, i s'evita que fonts no desitjades puguin canviar o manipular aquestes dades, és a dir, que no s'alterin de manera no autoritzada. Algunes mesures per garantir la integritat poden ser la segmentació i el control d'accés, la comprovació del *hash* en els paquets, la verificació d'integritat de les versions per instal·lar o emmagatzemades, etc.

Exemples de riscos que comprometin la integritat són: manipulació del trànsit o de les dades (en trànsit o emmagatzemades) en interfícies exposades de la xarxa 5G.

c) Traçabilitat: propietat o característica que consisteix en el fet que les actuacions d'una entitat (actiu, usuari, xarxa, persona, procés) es poden traçar de forma indiscutible fins aquesta entitat.

Exemples de riscos que poden comprometre la traçabilitat són els següents: pèrdua de control de la cadena de generació d'informació o de dades o la manipulació o esborrament dels registres i *logs*.

d) Autenticitat: propietat o característica consistent en el fet que una entitat (actiu, usuari, xarxa, persona, procés) és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.

Exemples de riscos que poden comprometre l'autenticitat són els següents: falsificació d'informació o de paquets de dades.

e) Disponibilitat: la disponibilitat es basa en el principi de garantir que els usuaris legítims tinguin accés ininterromput als serveis i les dades dins de l'entorn per al seu funcionament correcte, i les entitats o processos autoritzats hi tenen accés quan ho requereixen. Aquest concepte pretén jutjar la importància de l'actiu i la seva solució en la continuïtat de negoci d'un servei, recurs o infraestructura determinats. El nivell de risc d'afectació a la disponibilitat se sol unir al nombre i al tipus d'usuaris afectats que pot comportar la caiguda del servei.

Per garantir la disponibilitat es poden prendre diverses mesures entre les quals hi ha la creació de solucions de *backup,* la redundància o resiliència dels actius, la capacitat de mitigació davant d'atacs DDoS, o els procediments eficaços de restauració del servei després de la caiguda.

Dins de l'entorn, alguns riscos que poden comprometre la disponibilitat són els següents: atacs com ara denegació de servei a la funció de xarxa, a la infraestructura de virtualització, o la infraestructura física, o catàstrofes naturals, terrorisme, etc.

3. Determinació de la criticitat dels actius

En aquest apartat, s'identifica la criticitat dels actius d'una xarxa 5G-SA, d'acord amb les cinc dimensions de seguretat que descriu l'apartat anterior.

1. Es defineixen tres categories de criticitat dels actius: BÀSICA, MITJANA i ALTA.

a) Un actiu és de categoria ALTA si alguna de les seves dimensions de seguretat assoleix el nivell de seguretat ALT.

b) Un actiu és de categoria MITJANA si alguna de les seves dimensions de seguretat assoleix el nivell de seguretat MITJÀ, i cap no assoleix un nivell de seguretat superior.

c) Un actiu és de categoria BÀSICA si alguna de les seves dimensions de seguretat assoleix el nivell BAIX, i cap no assoleix un nivell superior.

a) Xarxa d'accés.

– gNB: criticitat mitjana.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Xarxa d'accés	gNB	2 - Mitjana	2 - Mitjana	1 - Baixa	2 - Mitjana	2 - Mitjana	2 - Mitjana

Una gran majoria dels nodes d'accés ràdio se situen en emplaçaments en llocs públics no segurs. Això fa que la seva exposició a atacs *in situ* augmenti. L'afectació d'una cel·la pot comportar la interrupció de servei en una àrea reduïda, i afectar una quantitat petita d'usuaris, i a més el seu trànsit el pot suportar alguna altra estació base pròxima, per la qual cosa es considera que la criticitat és baixa pel que fa a disponibilitat.

Aquests nodes no emmagatzemen dades d'usuari. Malgrat això, si es produeix un atac *Man in the Middle* (*MitM*), el trànsit no xifrat es pot veure compromès (i afectar només els pocs usuaris connectats a aquest node), a més de poder manipular els paquets en curs si no hi ha verificació d'integritat. A causa de la dificultat d'efectuar aquest atac en l'escenari descrit, a la confidencialitat, la integritat i l'autenticitat s'atorga una criticitat mitjana.

b) Nucli de xarxa.

– AUSF, UDM i UDR: criticitat alta.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Nucli de xarxa	UDM	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		UDR	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		AUSF	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta

Un atemptat contra la confidencialitat o integritat en aquests actius pot comportar l'exposició d'informació crítica de l'usuari en la xarxa (claus d'autenticació, integritat i xifratge, dades de provisió dels usuaris i les seves identitats, etc.).

L'obtenció d'aquesta informació pot tenir un impacte molt alt pel fet que és informació associada directament a la targeta SIM dels clients, i la seva exfiltració pot comportar no només una exposició de les comunicacions dels usuaris, sinó també la pèrdua d'imatge de l'operador de xarxes i serveis 5G, i pot implicar la substitució de les targetes SIM compromeses. Per aquests motius, la criticitat de l'actiu pel que fa a confidencialitat i integritat és alta.

A més, atès que és un element centralitzat que rep les peticions d'autenticació de tots els usuaris de la xarxa, en cas que no es desplegui amb una solució correcta que garanteixi la seva resiliència i continuïtat de negoci, una disrupció en aquest pot provocar la caiguda completa de la xarxa. Per tant, pel que fa a disponibilitat, també té una criticitat alta.

En el cas de l'autenticitat i la traçabilitat, se li atorga una criticitat alta.

– AMF, NRF i NEF: criticitat alta.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Nucli de xarxa	AMF	3 - Alta	2 - Mitjana	2 - Mitjana	2 - Mitjana	2 - Mitjana	3 - Alta
		NRF	3 - Alta	3 - Alta	1 - Baixa	3 - Alta	3 - Alta	3 - Alta
		NEF	2 - Mitjana	2 - Mitjana	1 - Baixa	2 - Mitjana	2 - Mitjana	2 - Mitjana

• NRF: criticitat alta.

Aquest element disposa d'un mapa de tota la xarxa, els nodes i els serveis. Un accés no autoritzat pot donar el detall del desplegament de la xarxa, els encaminaments, DNS, *slices*, serveis, etc. A més, l'alteració de la seva configuració pot provocar errors de

comunicacions internes en la xarxa. Ateses aquestes raons, la confidencialitat i la integritat de l'NRF es consideren de criticitat alta.

Tanmateix, com que en casos de caiguda de l'NRF, l'AMF guarda en la memòria cau els destins de forma indefinida, això fa que la seva criticitat pel que fa a disponibilitat sigui baixa.

En el cas de l'autenticitat i la traçabilitat, se li atorga una criticitat alta.

- AMF: criticitat alta.

Atès que és l'encarregat de gestionar la mobilitat dels usuaris, un atac o accés no autoritzat pot permetre obtenir o exfiltrar informació delicada (identitats de l'usuari, localització en l'àmbit de *Tracking Area*, i fins i tot l'identificador del node on és el client quan el terminal està en mode connectat).

Per aquest motiu, en riscos d'exfiltració més que d'alteració d'informació, es considera alta la criticitat pel que fa a confidencialitat, i mitjana pel que fa a integritat.

D'altra banda, atès que únicament afecta una part dels usuaris de la xarxa, es considera que la criticitat pel que fa a disponibilitat és mitjana.

En el cas de l'autenticitat i la traçabilitat, se li atorga una criticitat mitjana.

- NEF: criticitat mitjana.

Aquest element és el responsable de garantir l'autenticació, la confidencialitat i la integritat de les comunicacions d'entitats externes al nucli de xarxa, contra alguna de les funcions internes del nucli de xarxa (interfície *SBI*). Un accés no autoritzat pot permetre la modificació d'alguna política de seguretat entre les funcions externes al nucli de xarxa i les internes. Tanmateix, aquesta funció de xarxa no s'utilitza per a la prestació de servei generalista als usuaris 5G. Per aquest motiu, la confidencialitat i la integritat tenen una valoració mitjana.

Si tenim en compte la disponibilitat, la caiguda d'aquest equip, en cas de no tenir redundància, només pot afectar els serveis que necessitin comunicació externa amb els elements del nucli de xarxa, cosa que no té una afectació considerable, i per això es considera baixa.

En el cas de l'autenticitat i la traçabilitat, se li atorga una criticitat mitjana.

– SMF/UPF i PCF: criticitat baixa.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Nucli de xarxa	SMF/UPF	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa
		PCF	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa

En aquesta categoria s'agrupen els elements següents, en què, en general, una afectació d'aquests no té un impacte notable en la prestació del servei 5G, per la qual cosa la seva valoració de criticitat és baixa.

- SMF/UPF: criticitat baixa.

L'SMF s'encarrega de l'establiment de les sessions, i la UPF s'encarrega de la gestió del pla d'usuari: desencapsula el trànsit de l'usuari que arriba de l'accés ràdio i l'encamina a altres xarxes de dades. Un accés no autoritzat pot desactivar la sessió d'un usuari, però es pot establir en un altre SMF/UPF. A més, l'ús del SecGW entre la xarxa d'accés i el nucli de xarxa impossibilita un MiTM, cosa que fa que la seva criticitat, tenint en compte la confidencialitat, la integritat, l'autenticitat i la traçabilitat, sigui baixa.

D'altra banda, tenint en compte la disponibilitat, la seva criticitat es considera baixa igualment, pel fet que un usuari no pot estar més que en un AMF, però les seves sessions sí que poden estar en diversos SMF/UPF.

• PCF: criticitat baixa.

Aquest element no és especialment crític per als serveis de dades, sempre que, a més, els terminals siguin de tipus *data-centric*. Encara que disposa de les polítiques relacionades amb els serveis i la tarifació, els AMF/SMF sempre es configuren per poder donar servei sense aquest element. Un efecte normal de caiguda de PCF en servei de dades és no poder tarifar en línia els clients. L'afectació eventual sobre el servei de veu es pot mitigar mitjançant un servei de veu per 2G/3G. Per aquests motius, la seva criticitat, tenint en compte els diferents criteris, es considera baixa.

c) Transport-Backhaul.

– SecGW: criticitat alta.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Transport - Backhaul	SecGW	3 - Alta	2 - Mitjana	2 - Mitjana	2 - Mitjana	2 - Mitjana	3 - Alta

La xarxa de transport connecta els elements del nucli amb els de la xarxa d'accés. Un possible tall d'aquesta en un dels seus trams fa que només la zona de nodes d'accés ràdio en què es produeix aquest tall estigui afectada i, de forma temporal, es pot forçar que el trànsit no passi per aquest element en aquesta zona, amb la qual cosa la disponibilitat té una criticitat mitjana.

D'altra banda, comprometre un lloc o interceptar el trànsit comporta una fuga d'informació important, atès que és l'element encarregat de xifrar la informació en trànsit que arriba des d'una gran quantitat de nodes. Per això, tenint en compte la confidencialitat, se li assigna una criticitat alta. Atès que aquesta comunicació està xifrada, alterar-la és complicat, per la qual cosa la criticitat pel que fa a integritat, autenticitat i traçabilitat es considera mitjana.

d) Interconnexió itinerància.

– SEPP: criticitat alta.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Interconnexió roaming	SEPP	3 - Alta	2 - Mitjana	2 - Mitjana	2 - Mitjana	2 - Mitjana	3 - Alta

Aquest element permet l'intercanvi de senyalització amb altres xarxes en escenaris d'itinerància. Malgrat que és un element exposat a altres xarxes, únicament transporta trànsit d'usuaris d'itinerància, i no el dels usuaris nacionals. Aquest fet fa que la criticitat pel que fa a disponibilitat, autenticitat i traçabilitat sigui mitjana.

D'altra banda, la confidencialitat de les comunicacions i la seva integritat sí que són aspectes importants (sobretot la primera), ja que és un entorn en què, en cas de no disposar de les proteccions adequades, es pot obtenir o exfiltrar informació delicada dels usuaris, fins i tot dels que no estan en itinerància. Això fa que la criticitat pel que fa a confidencialitat sigui alta.

És un entorn que la indústria i els organismes d'estandardització s'ha pres molt seriosament, en què, de manera nativa, els fabricants inclouen capacitats de configuració de xifratge i integritat, i això fa més complicat atemptar contra la integritat si el trànsit està xifrat i, per tant, s'hi atorga una criticitat mitjana.

e) Sistemes de control i gestió i serveis de suport.

– GER: criticitat alta.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Sistemes de gestió/operació i serveis de suport	GER	3 - Alta	3 - Alta	1 - Baixa	3 - Alta	3 - Alta	3 - Alta

Aquests elements permeten una operació correcta dels elements que conformen l'entorn de xarxa 5G. Poden gestionar tot un entorn de xarxa i intercanviar missatges de configuració que poden donar ordres fraudulentes als equips o, fins i tot, transportar credencials.

Per tant, es considera que la integritat, la confidencialitat, l'autenticitat i la traçabilitat d'aquest element és alta.

Tanmateix, una interrupció o falta de comunicació amb la xarxa per part dels sistemes de gestió no ocasiona una caiguda d'aquesta i, per tant, es considera que la disponibilitat és de criticitat baixa.

f) Infraestructura de virtualització o orquestració.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Secundaris	Infraestructura de virtualització/ orquestració	Infraestructura de virtualització	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta
Secundaris		Gestió/orquestració de virtualització	3 - Alta	3 - Alta	1 - Baixa	3 - Alta	3 - Alta	3 - Alta

– Infraestructura de virtualització: criticitat alta.

Tots els elements del nucli de xarxa 5G estan desplegats sobre una infraestructura virtualitzada. Això implica que qualsevol atac que aconsegueixi una disrupció del seu funcionament, poder controlar els nodes d'aquesta, interceptar-ne el trànsit, modificar-ne el funcionament, etc., pot tenir conseqüències greus en la prestació del servei i, fins i tot, arribar a la interrupció total. Pels motius descrits, la criticitat pel que fa a confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat és alta, i es considera un actiu crític dins la xarxa.

– Gestió o orquestració de la virtualització: criticitat alta.

De forma anàloga als sistemes de gestió o operació i serveis de suport, el més crític en aquest actiu són la confidencialitat i la integritat de les comunicacions i accessos, qualificades de criticitat alta, ja que des dels orquestradors de la virtualització es controlen tots els elements de la plataforma de virtualització, els quals es poden vulnerar o poden patir atemptats (per exemple, eliminació de CNF, apagada de maquinari, etc.). Així mateix, s'atorga a autenticitat i traçabilitat una criticitat alta.

Tanmateix, una interrupció o falta de comunicació amb la xarxa per part de l'orquestrador no ocasiona una caiguda de les plataformes de virtualització i, així, es considera que la criticitat pel que fa a disponibilitat és baixa.

g) Infraestructura física.

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Secundaris	Infraestructura física	Infraestructura física	1 - Baixa	1 - Baixa	3 - Alta	1 - Baixa	1 - Baixa	3 - Alta

– Infraestructura física: criticitat alta.

La infraestructura física és especialment vulnerable als atacs que provoquen danys físics en l'equipament, robatori, talls d'energia, etc. La disponibilitat d'aquesta és fonamental per al funcionament de les xarxes i els serveis, ja que s'utilitza de base per situar-hi moltes funcions de xarxa i sistemes de gestió de tota la xarxa, per la qual cosa el valor de criticitat, pel que fa a disponibilitat, és alt.

La confidencialitat, la integritat, l'autenticitat i la traçabilitat d'aquest actiu es consideren baixes, atès que no representa un risc per a la informació o les comunicacions en si mateixa, i depèn fonamentalment dels protocols i mecanismes de control lògics implementats en les capes superiors (infraestructura de virtualització, aplicacions, etc.), amb l'objecte d'evitar l'obtenció d'informació si algú aconsegueix el control d'un actiu.

Quadre resum: taula de criticitat d'actius

Descripció de l'actiu			Dimensió de seguretat					Criticitat
Tipus	Domini	Actiu	Confidencialitat	Integritat	Disponibilitat	Autenticitat	Traçabilitat	
Primari	Xarxa d'accés	gNB	2 - Mitjana	2 - Mitjana	1 - Baixa	2 - Mitjana	2 - Mitjana	2 - Mitjana
Primari	Nucli de xarxa	SMF/UPF	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa
		PCF	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa	1 - Baixa
Primari	Nucli de xarxa	UDM	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		UDR	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta
		AUSF	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta
Primari	Nucli de xarxa	AMF	3 - Alta	2 - Mitjana	2 - Mitjana	2 - Mitjana	2 - Mitjana	3 - Alta
		NRF	3 - Alta	3 - Alta	1 - Baixa	3 - Alta	3 - Alta	3 - Alta
		NEF	2 - Mitjana	2 - Mitjana	1 - Baixa	2 - Mitjana	2 - Mitjana	2 - Mitjana
Primari	Transport - Backhaul	SecGW	3 - Alta	2 - Mitjana	2 - Mitjana	2 - Mitjana	2 - Mitjana	3 - Alta
Primari	Interconnexió roaming	SEPP	3 - Alta	2 - Mitjana	2 - Mitjana	2 - Mitjana	2 - Mitjana	3 - Alta
Primari	Sistemes de gestió/operació i serveis de suport	GER	3 - Alta	3 - Alta	1 - Baixa	3 - Alta	3 - Alta	3 - Alta
Secundaris	Infraestructura de virtualització/orquestració	Infraestructura de virtualització	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta	3 - Alta
Secundaris		Gestió/orquestració de virtualització	3 - Alta	3 - Alta	1 - Baixa	3 - Alta	3 - Alta	3 - Alta
Secundaris	Infraestructura física	Infraestructura física	1 - Baixa	1 - Baixa	3 - Alta	1 - Baixa	1 - Baixa	3 - Alta

4. Classificació d'actius en funció de la criticitat

D'acord amb les anàlisis anteriors i les aportacions efectuades pels operadors de xarxes i serveis 5G, s'ha identificat un conjunt d'elements que es qualifiquen d'importància crítica per a l'operació de les xarxes 5G, per a la seva configuració o gestió, o dels serveis prestats per aquestes.

Tal com recull l'apartat anterior, tots els actius de criticitat alta de l'entorn primari de xarxa pertanyen al nucli de xarxa. No obstant això, des del punt de vista de la criticitat, no és possible considerar el nucli de xarxa com un bloc homogeni. Per això, es considera aplicable un tractament diferenciat amb relació a les mesures conduents a garantir la disponibilitat dels serveis que ofereixen.

Així doncs, el nucli de xarxa està compost de diverses funcions de xarxa (o *Network Functions,* NF) que es despleguen en infraestructures virtualitzades independents de la funció pròpia de xarxa. La classificació considera quines d'aquestes entitats són més crítiques no només des del punt de vista de redundància, sinó també del possible impacte d'accessos no autoritzats o atacs des d'altres xarxes.

A més, es tenen en compte els possibles accessos no autoritzats a la infraestructura virtualitzada sobre la qual es despleguen aquestes funcions de xarxa, i s'estableix una importància relativa entre les diferents entitats, i es recalca que, per obtenir un servei complet, totes són necessàries.

a) Criticitat alta.

El risc que més pot comprometre el servei 5G és un accés no autoritzat en l'entorn AUSF/UDM/UDR. En l'AUSF hi ha les claus d'autenticació que permeten l'accés a qualsevol comunicació de ràdio xifrada, i en la UDM/UDR hi ha totes les dades de provisió dels usuaris i les seves identitats, i precisament el 3GPP inclou l'ús del SUCI (identitat IMSI xifrada) per evitar que aquesta identitat viatgi per la interfície ràdio, ja que disposar del SUPI d'un usuari és el primer pas per a qualsevol altre atac. Es considera, sens dubte, que aquestes són les funcions de xarxa més crítiques, atès que l'impacte d'obtenir les claus i les entitats és durador (atès que està associat a les claus de la SIM dels clients). La pèrdua d'imatge d'un operador de xarxes i serveis 5G davant d'una intrusió en aquestes funcions de xarxa pot ser enorme i pot implicar la substitució de les SIM compromeses. No obstant això, el disseny de xarxa permet prestar servei sense cap impacte davant d'una fallada doble d'instàncies de qualsevol d'aquests nodes.

A més dels anteriors, es consideren de criticitat alta, entre d'altres, les funcions següents:

i. NRF: aquest element disposa d'un mapa de tota la xarxa, nodes i serveis. Amb la informació de l'NRF, es disposa de tot el detall del desplegament de la xarxa, encaminaments, DNN, *slices,* serveis, etc. A més, un accés no autoritzat permet aturar el servei 5G, ja que totes les funcions de xarxa consulten aquesta entitat per conèixer les funcions de xarxa de destinació que disposen del servei requerit. No obstant això, les funcions de xarxa tenen la informació de l'NRF emmagatzemada a la memòria cau, cosa que permet mitigar temporalment l'atac. A més, el disseny de xarxa permet prestar el servei sense cap impacte davant de la fallada doble d'instàncies d'aquest node.

ii. SEPP: permet l'intercanvi de senyalització amb altres xarxes per a escenaris d'itinerància en la xarxa pròpia, o en la d'altres xarxes de tercers. És un element exposat, encara que els subministradors 5G han desenvolupat un nombre elevat de funcionalitats per garantir-ne la seguretat i integritat. Addicionalment, s'ha de garantir l'aïllament entre els dominis interns i externs.

iii. AMF: és l'encarregat de la gestió de la mobilitat. Un atac o accés no autoritzat a aquest pot permetre obtenir informació molt delicada (identitat de l'usuari, localització en *Tracking Area,* i fins i tot gNB-id on és el client quan el seu terminal està en mode *connected)*, amb possibilitat de rastrejar el moviment d'usuaris, i els seus procediments de senyalització relacionats amb la mobilitat i la gestió de sessions. Aquests elements es despleguen en mode *pool* i es dimensionen per suportar de forma simultània una fallada d'un node de cada *pool*.

b) Criticitat mitjana.

En aquesta categoria de criticitat mitjana s'inclou la funció NEF.

c) Criticitat baixa.

En aquesta categoria, novament, de més a menys criticitat, s'indica:

i. SMF/UPF: l'SMF s'encarrega de la gestió de les sessions (establiment, modificació i alliberament), la gestió i assignació d'IP als terminals dels usuaris, etc. També és responsable d'interactuar amb el pla d'usuari, i crea, actualitza o esborra sessions PDU, així com administra el context de la sessió amb la UPF, mentre que la UPF gestiona el pla d'usuari. Aquests elements estan molt més redundats que els AMF anteriorment descrits, i un accés no autoritzat pot desactivar la sessió d'un usuari, encara que aquesta es pot establir en un altre SMF/UPF. El pla d'usuari o trànsit real de clients

s'encamina, en general, a altres xarxes (internet/intranet) que són de seguretat més baixa, per la qual cosa un atacant de pla d'usuari té més fàcil comprometre el servei atacant el servidor de destinació o, fins i tot, el terminal.

ii. PCF: no és especialment crític, ja que els AMF/SMF es configuren per poder donar servei sense aquest element, i pot afectar, eventualment, la tarifació en línia dels clients.

d) No crítics.

Els elements CHF, NWADF i 5G-EIR no es consideren crítics per a la prestació del servei 5G pel fet que, en cas de caiguda o indisponibilitat parcial o total de qualsevol d'aquests, el servei als clients no ha d'estar afectat.

5. Identificació d'amenaces i riscos en la tecnologia 5G

L'article 9 del Reial decret llei 7/2022, de 29 de març, especifica la necessitat d'identificar els factors de risc per analitzar en funció de l'evolució tecnològica, la incorporació de nous avenços, funcionalitats i estàndards tecnològics, la situació del mercat de comunicacions electròniques i del de subministraments i de l'aparició de noves amenaces i vulnerabilitats.

Els apartats següents recullen les tasques efectuades.

5.1 Criteri d'identificació del risc d'un atac.

Per calcular el nivell de risc de seguretat que introdueix una amenaça, utilitzem tres factors d'acord amb les fórmules següents:

$$\text{nivell de risc} = (\text{probabilitat d'ocurrència}) \times (\text{impacte en la xarxa})$$

en què, al seu torn,

$$(\text{impacte en la xarxa}) = (\text{criticitat de l'actiu}) \times (\text{factor d'escalat})$$

Es defineixen, tot seguit, els conceptes utilitzats:

a) Probabilitat d'ocurrència: es fa una valoració d'acord amb els paràmetres següents:

i. Grau d'exposició de l'actiu a la vulnerabilitat: aporta una mesura de l'exposició de l'element analitzat a escala física o lògica, i el nivell d'accessibilitat o facilitat que pot tenir l'atacant de cara a executar l'amenaça.

ii. Complexitat o coneixements per desenvolupar l'atac: la probabilitat d'ocurrència augmenta en cas que l'atac es pugui fer sense gaires coneixements tècnics i l'entorn d'atac sigui senzill d'implementar o s'utilitzin eines automatitzades.

iii. Coneixement públic de la vulnerabilitat: un atac és més probable com més conegut és en la comunitat. En cas que la vulnerabilitat estigui poc difosa o es manegi només en certs cercles (com per exemple subministradors 5G o operadors de xarxes i serveis 5G), la seva explotació és menys probable.

iv. Rastre que deixa l'atac: en cas que l'atac sigui de força bruta o deixi traçabilitat en les xarxes, la probabilitat que hi hagi atacants disposats a aprofitar la vulnerabilitat és més baixa. Són casos en els quals no es pot fer suplantació d'identitat.

v. Benefici obtingut amb l'èxit de l'atac: valor econòmic, reconeixement, rellevància, etc., de la consecució de l'atac.

Els possibles valors de la probabilitat d'ocurrència són molt alt, alt, mitjà, baix.

b) Impacte en la xarxa: de manera similar a la probabilitat d'ocurrència, s'utilitza una valoració qualitativa per mesurar l'impacte que pot tenir l'atac en la xarxa.

Per avaluar el servei i donar una valoració de l'impacte s'utilitzen els paràmetres següents:

i. Criticitat de l'actiu: concepte esmentat anteriorment, que engloba la confidencialitat, la integritat, la disponibilitat, l'autenticitat i la traçabilitat.

ii. Factor d'escalat: identifica la importància o l'abast de l'atac en l'àmbit d'afectació de la xarxa. Pren en consideració tant l'abast (nombre d'usuaris que poden ser impactats), com el tipus d'impacte de l'atac (fuga de credencials, disminució de disponibilitat, etc.).

Els possibles valors de l'impacte en la xarxa de l'atac són: molt alt, alt, mitjà, baix, tenint en compte els criteris anteriors.

c) Nivell de risc: és el resultat de les dues variables anteriors d'acord amb la fórmula descrita més amunt.

Els possibles valors del nivell de risc són: crític, alt, mitjà, baix.

5.2 Matriu de riscos.

Tenint en compte les consideracions de l'apartat anterior, es presenta la matriu genèrica que caracteritza els nivells de risc que s'analitzen posteriorment en aquest document.

Impacte a la xarxa					
Molt alt (4)	**4**	**8**	**12**	**16**	**Crític**
Alt (3)	**3**	**6**	**9**	**12**	**Alt**
Mitjà (2)	**2**	**4**	**6**	**8**	**Mitjà**
Baix (1)	**1**	**2**	**3**	**4**	**Baix**
	Baixa (1)	Mitjana (2)	Alta (3)	Molt alta (4)	
	Probabilitat d'ocurrència				***Nivell de risc***

6. Amenaces o riscos en una xarxa 5G SA

Una vegada identificats els actius i caracteritzada la seva criticitat, el pas següent en l'anàlisi de riscos és avaluar les amenaces o els possibles atacs als quals estan exposats cadascun d'aquests actius de xarxa 5G SA.

És important destacar que una mateixa amenaça pot tenir un nivell de risc diferent en funció de l'actiu o l'entorn sobre el qual s'avaluï, de cara a establir les prioritats correctes d'accions mitigadores que permetin incrementar, en una mateixa línia temporal, la seguretat de la solució de la manera més eficient possible.

A continuació, es detallen les amenaces o riscos en una xarxa 5G SA:

a) Activitats malicioses degudes a accessos indeguts o maliciosos a la gestió, extracció d'informació delicada o modificació no autoritzada de parametrització que provoqui la indisponibilitat de l'element.

Són les accions dutes a terme per atacants interns o externs adreçades als elements o funcions de xarxa i infraestructura amb la intenció de robar informació, alterar-la o destruir, mitjançant una configuració, un objectiu específic.

En aquest bloc s'engloben, entre d'altres, les amenaces següents:

i. Intrusions en la xarxa amb l'objectiu d'obtenir informació, a través d'accessos maliciosos, moviments laterals, escalat de privilegis, per manca de polítiques de seguretat robustes (absència de control d'accés, autenticació, autorització, segmentació, *hardening,* etc.). Destaca, entre altres, l'obtenció de credencials d'usuaris operadors, informació delicada de clients (dades, identificadors d'usuari, claus d'autenticació, xifratge i integritat), o informació útil de configuració de xarxa (ports, versions, etc.), que serveixi com a vector d'informació addicional per fer atacs de més impacte.

ii. Modificació malintencionada i no autoritzada de parametrització o configuració de xarxa que pot provocar indisponibilitat parcial o total del servei en l'actiu o la xarxa, així com afavorir l'exfiltració de trànsit comentada en el punt anterior.

A. Manipulació de configuració o parametrització que afecti el funcionament de l'equip (polítiques d'encaminament o de trànsit, configuració de DNS, sessions d'usuari, imatges de funcions de xarxa virtuals, etc.).
B. Manipulació de configuració de seguretat de l'equip (polítiques de seguretat, serveis oferts en l'aplicació i sistema operatiu, algoritmes criptogràfics, regles d'accés) i creació de portes del darrere.
C. Execució de forma intencionada o inconscient de programari o codi maliciós (SQL, XSS *injection*, *rootkits*, *malware* o *ransomware*, etc.).

iii. Explotació de vulnerabilitats en maquinari o programari, que permetin un accés simple i eficaç per poder executar les amenaces comentades en els dos punts anteriors (vulnerabilitats conegudes o CVE, noves vulnerabilitats i de *zero-day*).

b) Compromís de les comunicacions o dades d'usuari a través de la captura, la intercepció, el segrest de trànsit de servei o la seva modificació:

Aquesta categoria recull les accions efectuades per espiar, interrompre o alterar les comunicacions o dades d'usuari en el pla de servei, sense el seu consentiment.
Les principals amenaces dins d'aquesta categoria són:

i. Espionatge de comunicacions d'un determinat usuari en entorns amb un alt nivell d'exposició com és el cas de l'accés ràdio o la interconnexió d'itinerància.
ii. Obtenció d'informació delicada dels usuaris (identificadors d'usuari, localització, serveis, etc.) en interfícies exposades que es puguin utilitzar com a vectors d'informació per fer atacs de més impacte.
iii. Manipulació de les comunicacions en interfícies exposades a través d'activitats *Man in The Middle* (MiTM) o de les dades d'usuari, i possibilitat de provocar accions il·legals com ara frau, suplantació d'identitat, etc.

c) Denegació de servei (DoS).

Aquesta categoria recull les accions, activitats o incidències malintencionades o no que poden provocar una disrupció total o parcial en l'equip i causar una afectació als usuaris de la xarxa. Les principals amenaces dins d'aquesta categoria són:

i. Atacs volumètrics de denegació de servei (DoS/DDoS): inundació de trànsit en les interfícies exposades dels actius (dispositius d'usuari, interconnexions, etc.) amb l'objectiu de sobrecarregar les capacitats dels elements i provocar un mal funcionament o disrupció en la xarxa.
ii. Atacs adreçats a usuaris específics amb l'objectiu de provocar la seva indisponibilitat en la xarxa (per exemple, atacs d'interferència o desregistrament de la xarxa).
iii. Danys no intencionats pels operadors per errors de configuració: Recull les accions no intencionades per part d'un operador amb accés a la gestió d'un actiu que poden provocar una fallada o la reducció de funcionalitat d'aquest, com, per exemple, la configuració pobra o errònia dels actius de xarxa i les seves capacitats de seguretat (aïllament, reforçament del sistema, segmentació, etc.) o error en la seva gestió o manipulació per desconeixement o falta de formació o diligència.
iv. Mal funcionament de l'element: Engloba el mal funcionament «natiu» (per causes alienes a la configuració de l'actiu) que pot provocar una disrupció total o parcial del seu servei.

d) Amenaces físiques.

Té com a objectiu destruir, inutilitzar, alterar o robar actius físics de la infraestructura física que allotja les funcions o elements de xarxa.

Entre les amenaces principals destaquen el sabotatge o terrorisme contra els elements crítics d'equipament de xarxa, les catàstrofes naturals, el mal funcionament de la xarxa d'energia i la possible sostracció d'equipament de xarxa per a l'extracció d'informació delicada i la seva posterior explotació.

e) Escassa formació i conscienciació dels empleats en matèria de ciberseguretat, així com mala praxi en la gestió de l'evolució dels riscos identificats.

D'una banda, el fet que els empleats no estiguin conscienciats en matèria de seguretat augmenta la probabilitat d'ocurrència d'incidents com ara atacs *ransomware* i un altre tipus de *malware*. La falta de formació en matèria de seguretat i operació augmenta la probabilitat d'errors de configuració per desconeixement que exposin els actius a riscos innecessaris.

A més de tot això, si no es duu a terme un bon procediment de gestió de riscos i es controla la seva evolució en la xarxa, és impossible plantejar un pla de prioritats i executar les mesures de seguretat de manera eficient.

ANNEX III

Gestió de riscos en l'àmbit nacional

Una vegada identificades en l'annex II les diferents amenaces que afecten detalladament les xarxes i els serveis 5G, i amb això la situació inicial de risc, la fase següent és preveure les mesures de seguretat necessàries per resoldre, disminuir o pal·liar els riscos identificats.

Aquestes mesures són:

1. Mesures de seguretat genèriques:

1.1 Configuracions de seguretat per a l'equipament:

1.1.1 Configuracions relacionades amb la identificació, l'autenticació, el control, l'auditoria i el monitoratge en l'accés al pla de gestió dels nodes. Els nodes s'han de configurar amb:

a) Polítiques de gestió d'identitat que permetin garantir tant l'autenticació (verificar que qui hi accedeix és qui diu ser), com l'autorització (accedir-hi només amb els privilegis que siguin estrictament necessaris) quan s'accedeix als nodes.

b) Polítiques de gestió del cicle de vida de l'usuari.

c) Capacitats de traçabilitat i polítiques d'auditoria que permetin que quedin registrats tots els accessos (qui i quan es connecta i desconnecta dels nodes), així com els comandaments executats i les alarmes que identifiquen una possible fallada en l'equip.

d) Bones pràctiques de seguretat quan es defineixen i gestionen les credencials i els accessos dels usuaris, i sempre amb el requisit que les credencials siguin robustes.

e) Capacitat de configurar-los de manera que no donin informació detallada en el cas que falli l'accés i s'estableixin polítiques de bloqueig que dificultin l'obtenció de credencials.

1.1.2 Reforçament del sistema:

a) Autoprotecció dels nodes i assegurar que només estiguin actius els serveis necessaris per al seu funcionament correcte.

b) Els nodes han de tenir la capacitat de separar la interfície de gestió del de servei, a través d'una interfície física o lògica.

c) Els nodes han de ser capaços de detectar i manejar els paquets que estiguin mal formats per mantenir els serveis sense afectació.

d) Els nodes han de ser capaços de fer front a alts volums o moments punta de trànsit amb mecanismes d'autoregulació per evitar el col·lapse de la seva CPU.

e) Capacitat addicional de protegir la informació crítica i delicada que estigui emmagatzemada.

f) Els nodes o elements de la xarxa s'han de configurar de manera que no es permeti iniciar a través de dispositius de memòria no autoritzats.

g) Els nodes s'han de configurar de manera que no es pugui fer una explotació maliciosa de les API que exposin.

1.1.3 Realització de proves de seguretat periòdiques. Són necessàries per estudiar si han aparegut noves vulnerabilitats per als components de l'actiu.

1.2 Seguretat arquitectònica i funcional.

1.2.1 Plans de xarxa diferents, així com àrees o ambients de xarxa amb un nivell d'exposició diferent, s'han d'aïllar.

1.2.2 Control de flux: Capacitat de limitar el trànsit a certes adreces IP, protocols, aplicacions, per evitar sobrecarregar l'enllaç i fer que un atac sigui més complicat de dur a terme.

1.3 Mesures de seguretat en la infraestructura física:

a) Registre, validació i control de les autoritzacions d'accés físic als emplaçaments crítics.

b) Controls d'accessos físics, mitjançant mitjans electrònics o mecànics, a les centrals de xarxa i edificis rellevants.

c) Vigilància física i seguretat electrònica de l'emplaçament crític.

d) Sistemes de seguretat electrònics instal·lats i mantinguts en emplaçaments crítics.

1.4 Conscienciació de seguretat cap als empleats i la cadena de comandament.

1.5 Formació d'empleats en tecnologia, seguretat i processos.

1.6 Implementació de processos clars de gestió d'incidents, amb un registre de l'històric d'incidents propis i amb el coneixement actualitzat amb els incidents de la indústria.

2. Mesures de seguretat específiques relacionades amb una xarxa 5G.

2.1 Control de programari:

a) Garantir la integritat de l'actualització del programari abans d'instal·lar-la i evitar la injecció de codis maliciosos, troians o versions no legítimes (manipulades per un tercer).

b) Garantir que no hi hagi portes del darrere.

c) Garantir que no hi hagi vulnerabilitats (CVE) explotables conegudes d'alt risc en el moment de desplegament del producte en planta.

d) Compliment de certificacions de seguretat reconegudes internacionalment per als equips.

2.2 S'ha de configurar el xifratge i la integritat de les comunicacions entre el terminal i la xarxa a ambdós nivells AS (Access Stratum) / NAS (non Access Stratum), per protegir la privacitat de l'usuari en la interfície aèria. Aquesta mesura s'activa tant en la RAN (AS), com en el nucli de xarxa (NAS).

2.3 S'ha de configurar el xifratge i la integritat de les comunicacions en el pla de control i en el pla d'usuari entre el node d'accés ràdio (RAN) i el nucli de xarxa.

2.4 La privacitat dels usuaris s'ha de garantir en la interfície aèria.

2.5 S'han de corroborar les millores en els algoritmes d'autenticació entre el terminal de l'usuari i la xarxa que venen de manera nativa amb la tecnologia 5G SA.

2.6 Millores natives en els algoritmes d'autenticació entre el dispositiu de l'usuari i la xarxa, per garantir mútuament que la comunicació és legítima.

2.7 Els diferents elements que manegen el trànsit de senyalització han de tenir mesures per evitar la suplantació dels elements de xarxa propis en la xarxa d'itinerància, així com la dels usuaris que no estan en itinerància.

2.8 La confidencialitat, la integritat i l'autenticació s'han de garantir en les comunicacions entre un operador d'origen i de destinació, i utilitzar protocols, equipaments, solucions segures (SEPP). La implementació d'aquest requisit i el seu abast depèn de l'estandardització final del protocol que s'utilitza.

2.9 Cal establir les polítiques de seguretat corresponents de cara a exposar en la interconnexió únicament les interfícies i els missatges necessaris per al servei, i evitar donar informació innecessària que es pugui utilitzar de forma fraudulenta.

2.10 Aïllament de funcions de xarxa virtualitzades: classificació dels diferents elements virtualitzats en la infraestructura d'acord amb diferents nivells d'exposició i la criticitat de l'element.

2.11 Aïllament de trànsits: disseny segur de l'arquitectura de virtualització per garantir el trànsit necessari per al funcionament de la capa de virtualització. D'aquesta manera, es garanteixen l'operació o el funcionament de la xarxa.

2.12 Cal seguir les pautes dels requisits o les configuracions de seguretat de l'equipament i seguretat arquitectònica per a tots i cadascun dels elements que componen l'arquitectura de virtualització.

2.13 Monitoratge i detecció: monitoratge de la traçabilitat d'accessos i comandaments executats en els elements crítics de la xarxa, de cara a poder identificar activitats il·legítimes en el moment de la seva realització i també de cara a l'anàlisi forense de possibles atacs.

2.14 Mitigació: capacitats que permetin mitigar possibles atacs volumètrics que tinguin com a objectiu la denegació de servei en les interfícies molt exposades.

2.15 Entorns crítics: les proves de funcionament de redundància o recuperació (*backup*) en entorns crítics s'han de dur a terme abans del desplegament de la solució.