MINISTRY OF DIGITAL
TRANSFORMATION

REF.:
REF.C.M.:

Chapter Item (To be completed in the 'Official State Gazette')	

DRAFT ROYAL DECREE APPROVING THE NATIONAL SECURITY SCHEME FOR 5G NETWORKS AND SERVICES

Fifth generation or 5G mobile communications are a new paradigm of electronic communications with great transformative potential for the benefit of society and the economy, as they open up the possibility of incorporating new functionalities that will have a great impact such as network computing, they will allow for the creation of virtual networks, offer low latency and provide services with high added value for society and the economy in areas such as medicine, transport and energy. Therefore, the European Union and Spain, directly and through the Recovery and Resilience Facility, are promoting the rapid deployment of 5G networks and the implementation of projects demonstrating their usefulness for different sectors through the provision of 5G services.

5G networks and services have comparative security advantages over previous generations. However, they also present specific risks arising, for example, from their more complex, open and disaggregated network architecture, and from their ability to transport huge volumes of information and to enable the simultaneous interaction of multiple people and things. Their interconnection with other networks and the transnational nature of many of the threats have an impact on their security, and the foreseeable widespread use of these networks for essential economic and societal functions will increase the potential impact of the security incidents they suffer.

These new specific security risks of 5G mobile communications were addressed in regulatory terms through Royal Decree-Law 7/2022 of 29 March 2022 on requirements to ensure the security of fifth generation electronic communications networks and services, which fully incorporates European Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, as well as the recommendations that the European Commission's Communication of 29 January 2020 on Secure 5G deployment in the EU - Implementing the EU toolbox (COM/2020/50 final) provided Member States with regard to the use of the toolbox.

Royal Decree-Law 7/2022 of 29 March 2022 has recently been amended by the seventh final provision of the Royal Decree-Law approving urgent measures for the implementation of the Recovery, Transformation and Resilience Plan in the areas of public justice service, civil service, local government and patronage, with the aim of strengthening the controls to be carried out by the Government and the Ministry of Digital Transformation on the conditions under which the installation of the different equipment, elements, functions and systems of 5G technology, the deployment of 5G networks and the provision of 5G electronic communications services are being carried out, in order to achieve the ultimate objective pursued by said Royal Decree, which is, as indicated in its Article 1, to establish security requirements for the installation, deployment and operation of electronic communications networks and the provision of electronic and wireless communications services based on fifth generation (5G) technology.

The aforementioned Royal Decree-Law 7/2022 of 29 March 2022 provides for its regulatory development through the National Security Scheme for 5G Networks and Services. Thus, Article 21 of Royal Decree-Law 7/2022 of 29 March 2022 establishes that the Government shall approve, by Royal Decree, on the proposal of the Ministry of Digital Transformation, following a report by the National Security Council, a National Security Scheme for 5G Networks and Services.

In turn, Article 20 of Royal Decree-Law 7/2022 of 29 March 2022 establishes that the National Security Scheme for 5G Networks and Services shall carry out a comprehensive and holistic treatment of the security of 5G networks and services, taking into account the contributions to the reach of each agent of the 5G value chain in order to ensure the continued and secure functioning of the 5G network and services. To this end, the National Security Scheme for 5G Networks and

Services shall carry out a risk analysis at national level on the security of 5G networks and services, and shall identify, specify and develop measures at national level to mitigate and manage the risks analysed.

Finally, to complete the reference framework, it should be mentioned that Article 5(3) of Royal Decree-Law 7/2022 of 29 March 2022 establishes that the National Security Scheme for 5G Networks and Services shall carry out a comprehensive treatment of the security of 5G networks and services, taking into account the contributions to the reach of each agent of the 5G value chain, as well as the regulations, recommendations and technical standards of the European Union, the International Telecommunication Union (ITU) and other international organisations, in order to guarantee the ultimate objective of secure use and operation of 5G networks and services in Spain.

To comply with this mandate, this Royal Decree approves the National Security Scheme for 5G Networks and Services.

The principle of necessity is fulfilled, since this Royal Decree is issued to guarantee a good of general interest, such as security and trust in electronic communications. It complies with the principle of proportionality as the measures are appropriate to the risks identified in each case. It is in line with the principle of legal certainty because the existing regulatory framework on security is recognised and only requirements and controls appropriate to the uniqueness of 5G networks and services and their risks are added. The principle of transparency is respected, as stakeholders have been able to participate in the procedure for drawing up the Royal Decree. Finally, it complies with the principle of efficiency since administrative burdens have been limited to the minimum necessary to achieve the intended aim of ensuring the security of 5G networks and services.

This Royal Decree has undergone the procedure for the provision of information in the field of technical regulations and of rules on Information Society services, set out in Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

This Royal Decree is issued under the provisions of Article 149(1)(21) and Article 149(1)(29) of the Spanish Constitution, which confer on the State, respectively, exclusive competence in matters of the general system of telecommunications and in matters of public safety.

By virtue thereof, in compliance with the provisions of Article 21 of Royal Decree-Law 7/2022 of 29 March 2022 on requirements to ensure the security of fifth generation electronic communications networks and services, on the proposal of the Minister of Digital Transformation, following a report by the National Security Council and opinion of the Council of State, and after deliberation by the Council of Ministers at its meeting on xx xxxxxx 2024,

THE FOLLOWING IS DECREED:

Single Article. Approval of the National Security Scheme for 5G Networks and Services.

The National Security Scheme for 5G Networks and Services is approved, which is inserted below.

First additional provision. Review of the National Security Scheme for 5G Networks and Services.

The Government, by Royal Decree, on the proposal of the Ministry of Digital Transformation, following a report by the National Security Council, shall review the National Security Scheme for 5G Networks and Services when circumstances so require and, in any case, every 4 years.

Second additional provision. Application of Royal Decree-Law 7/2022 of 29 March 2022 and the National Security Scheme for 5G Networks and Services to successive generations of electronic communications.

Royal Decree-Law 7/2022 of 29 March 2022 on requirements to ensure the security of fifth generation electronic communications networks and services and the National Security Scheme for 5G Networks and Services that is approved shall apply to generations of electronic communications after the fifth generation while there is no specific standard for these.

First final provision. Attribution of powers

This Royal Decree and the Scheme it approves are issued under the provisions of Article 149(1)(21) and Article 149(1)(29) of the Spanish Constitution, which confer on the State, respectively, exclusive competence in matters of the general system of telecommunications and in matters of public safety.

Second final provision. Supplementary application of the regulations on security and integrity of electronic communications networks.

1. In all matters not regulated in this Royal Decree and the Scheme it approves, the provisions of Law 11/2022 of 28 June 2022 on General Telecommunications, and its implementing regulations, shall be of supplementary application.

2. In all matters not regulated in Law 11/2022 of 28 June 2022 on General Telecommunications, and its implementing regulations, Royal Decree-Law 12/2018 of 7 September 2018 on the security of networks and information systems and Law 8/2011 of 28 April 2011 establishing measures for the protection of critical infrastructure, as well as their respective implementing regulations, shall be of supplementary application.

Third final provision. Empowerment for regulatory development and amendment of annexes.

1. The head of the Ministry of Digital Transformation is empowered to develop the provisions of this Royal Decree and the Scheme it approves.

2. The head of the Ministry of Digital Transformation is empowered to amend by Order the contents of the annexes of the National Security Scheme for 5G Networks and Services according to the evolution of technological progress, the approval of new technical standards and certification schemes for telecommunications equipment and connected products, and the development of different configurations and technical parameters of 5G networks and services and future generations of electronic communications.

Fourth final provision. Entry into force.

This Royal Decree and the Scheme it approves shall enter into force on the day following its publication in the 'Official State Gazette'.

TO BE SUBMITTED TO THE COUNCIL OF MINISTERS

Madrid, XX xxxxxx 2024

THE MINISTER OF DIGITAL TRANSFORMATION

José Luis Escrivá Belmonte

NATIONAL SECURITY SCHEME FOR 5G NETWORKS AND SERVICES

Chapter I

General provisions

Article 1 National Security Scheme for 5G Networks and Services

The National Security Scheme for 5G Networks and Services (hereinafter ENS5G) is approved in development of the provisions of Royal Decree-Law 7/2022 of 29 March 2022 on requirements to ensure the security of fifth generation electronic communications networks and services, in particular, in application of Chapter IV thereof.

Article 2. Objectives.

The ENS5G has the following objectives:

a) Carry out a comprehensive and holistic treatment of the security of 5G networks and services, taking into account the contributions to the reach of each agent of the 5G value chain.
b) Ensure the continued and secure functioning of the 5G network and services.
c) Drive end-to-end security of the ecosystem generated by 5G technology.
d) Strengthen security in the installation and operation of 5G electronic communications networks and in the provision of mobile and wireless communications services supported by 5G networks.
e) Promote a sufficiently diversified supplier market in 5G electronic communications networks and services in order to ensure security based on technical, strategic and operational reasons and to avoid, for those reasons, the presence of suppliers with a high-risk or medium-risk classification in certain network elements or areas.
f) Strengthen the protection of national security.
g) Strengthen the industry and foster national RDI activities in cybersecurity related to 5G technology.

Article 3. Definitions.

For the purposes of the ENS5G, the definitions set out in Royal Decree-Law 7/2022 of 29 March 2022 on requirements to ensure the security of fifth generation electronic communications networks and services shall be used, as well as the definitions set out in Law 11/2022 of 28 June 2022 on General Telecommunications and the European Electronic Communications Code.

Article 4 Scope of application.

The ENS5G applies to the following obliged parties:

a) 5G operators.
b) 5G suppliers.
c) 5G corporate users that have been granted rights to use the public radio domain to install, deploy or operate a 5G private network, or to provide 5G services for professional purposes or self-provision.

Article 5. 5G network.

1. A 5G electronic communications network is composed of at least the following elements, infrastructure and resources:

a) Those relating to the functions of the network core.
b) Transport and transmission functions.
c) The access network.
d) Control and management systems and support services.
e) The functions of edge computing, network virtualisation and management of components.

f) Those relating to traffic exchanges or interconnection with external networks and the Internet.

g) Other components and functions referred to in Annex I.

2. The detailed description of the elements, infrastructure and resources that make up a 5G network is set out in Annex I.

3. The following are critical elements of a 5G network:

a) Those relating to the functions of the network core.

b) Control and management systems and support services.

c) The access network in those geographical areas and locations to be determined.

4. Critical elements of a 5G network must be located within the national territory. However, certain elements, functions and systems of both the network core and the control and management systems and support services may be located outside the national territory, provided that the Ministry of Digital Transformation can exercise the powers conferred on it by Royal Decree-Law 7/2022 of 29 March 2022, in particular, the powers of inspection and penalty system provided for in Chapter V thereof, so that it can carry out a comprehensive verification of the functioning, operability and conditions of use of said critical elements of a 5G network and, where appropriate, be able to adopt precautionary or definitive measures on said elements, functions and systems or the equipment used in the exercise of the powers conferred on the Ministry of Digital Transformation by Royal Decree-Law 7/2022 of 29 March 2022 and Law 11/2022 of 28 June 2022 on General Telecommunications.

In the event that the Ministry of Digital Transformation concludes that the elements, functions and systems of both the network core and the control and management systems and support services located outside the national territory affect, either for reasons of implementation of technical measures or strategic measures, the security or integrity of the 5G network or significantly impair the exercise of its supervisory powers and inspection powers, it may require the 5G network owner to locate such elements, functions and systems within national territory. For this purpose, the relocation of the elements, functions and systems must take place within the period indicated

by the Ministry of Digital Transformation in its resolution, after hearing the 5G network owner. This period may not be less than 3 months.

Article 6. Comprehensive security treatment.

1. Security is understood as an end-to-end process consisting of all human, material, technical, legal and organisational elements related to the 5G network or service. The ENS5G aims to carry out a comprehensive treatment of the security of 5G networks and services.

2. For this purpose, the ENS5G has taken into account and must take into account in future updates or modifications the regulations, recommendations and technical standards of the European Union, the International Telecommunication Union (ITU) and other international organisations.

Likewise, the ENS5G has taken into account and must take into consideration in future updates or modifications the contributions, risk analyses, risk mitigation plans and supply chain diversification strategies that have been provided and that must be provided by the obliged parties in compliance with the obligations established in Royal Decree-Law 7/2022 of 29 March 2022, in this Scheme and in the rest of the regulations.

3. In this context of end-to-end security, the obliged parties must carry out a comprehensive treatment of the security of the networks, elements, infrastructure, resources, facilities and services for which they are responsible. For this, they must carry out, by means of a holistic method, an analysis of the vulnerabilities, threats and risks affecting them as economic agents and of the aforementioned components, as well as an adequate and comprehensive management of those risks through the use of techniques and measures that are appropriate to achieve their mitigation or elimination and to achieve the ultimate objective of secure use and operation of 5G networks and services.

Article 7. Risk-based security management.

1. Risk analysis and management is an essential part of the security process, and should be an ongoing activity that is continuously updated.

2. Risk management shall allow the maintenance of a controlled environment in the 5G network or service, minimising risks to acceptable levels. The reduction to these levels shall be carried out by appropriate application of security measures, in a balanced manner and proportionate to the nature and characteristics of the network, the services to be provided and the risks to which they are exposed.

Article 8. Continuous monitoring and periodic reassessment.

1. Continuous monitoring shall allow for the detection of anomalous activities or behaviour and a timely response.

2. The ongoing assessment of the security status of 5G networks and services shall allow for measuring their evolution, detecting vulnerabilities and identifying configuration deficiencies.

3. The security measures shall be reassessed and updated periodically, adapting their effectiveness to the evolution of risks and protection systems, and possibly leading to a security review if necessary.

Chapter II
Risk analysis and management at national level

Article 9. Risk analysis at national level.

1. The risk analysis at national level to be carried out by the ENS5G is as set out in Annex II to this Scheme.

2. In carrying out this analysis, account has been taken of:

a) The overall risk analysis of 5G networks and services, taking into consideration the information collected from the obliged parties.

b) The examination of vulnerabilities linked to the supply chain of 5G networks and services.

c) The assessment of the degree of dependence of suppliers on all 5G networks and services in Spain, taking into account the risk analyses and supplier diversification strategies submitted by operators, as well as the risk of supply interruption due to economic, corporate or commercial circumstances affecting suppliers.

d) The assessment of the effectiveness of the security measures implemented until the approval of each national risk analysis to mitigate the risks highlighted by such analysis.

Article 10. Risk management at national level.

1. The criteria, requirements, conditions and periods for obliged parties to design and implement risk mitigation techniques and measures are those set out in Annex III to this Scheme.

2. In determining these risk management criteria and requirements, account has been taken of the national risk analysis incorporated in this strategy and the assessment of the effectiveness of the measures previously implemented by the obliged parties to mitigate and manage risks in 5G networks and services.

Chapter III

Specific measures to ensure the security of 5G networks and services

Article 11. Declaration of high-risk and medium-risk 5G suppliers.

1. The Government, by means of an agreement adopted by the Council of Ministers, following a report by the National Security Council and after hearing the 5G operators and 5G suppliers concerned for a period of 15 working days, may classify certain 5G suppliers as high risk.

To this end, the Government shall analyse both the technical guarantees for the functioning and operability of their equipment, products and services and their exposure to external interference.

2. In relation to the analysis of the technical measures and the technical guarantees for the functioning and operability of their equipment, products and services, aspects relating to compliance with standards or technical specifications, their verification by means of certification schemes, or the passing of security tests or audits carried out by independent entities shall be assessed.

3. In relation to the analysis of strategic measures and exposure to external interference, the following aspects shall be assessed:

a) The links of suppliers and their supply chain with third country governments.

b) The composition of their share capital and the structure of their governing bodies.

c) The power of a third State to exert pressure on the action or location of the company.

d) The characteristics of the cyber defence legislation and policy, and respect for international law and United Nations resolutions and agreements of that third State.

e) Cooperation agreements on security, cybersecurity, computer-related crime or data protection signed with the third country concerned, as well as international treaties on those matters to which that State is a party.

f) The degree of alignment of the third State's legislation on the protection of personal data with that of Spain, with the General Data Protection Regulation approved by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, adopted by the European Union, and with any other applicable legislation on the security of information and telecommunications networks and systems.

4. The Agreement of the Council of Ministers classifying certain 5G suppliers as high-risk suppliers shall determine the period within which 5G operators must carry out the replacement of the equipment, products and services provided by that supplier in the network and services of the 5G operator, where necessary, taking into account the market situation of the suppliers, the alternatives for the supply of viable replacement equipment and products, the deployment of such equipment and products in the operator's 5G network, especially in critical elements of the 5G network and depending on the specific critical elements affected, the intrinsic difficulty in carrying out equipment replacement, equipment upgrade cycles, migration from non-standalone to standalone 5G networks, as well as the economic impact.

In determining the replacement period, the Agreement of the Council of Ministers classifying certain 5G suppliers as high-risk suppliers may establish a different period for the various critical elements of the 5G public network depending on the criticality of that element or part of it, its impact on the functioning and operability of the network, and the availability of equipment at that time in the telecommunications equipment market. In no case may this period be less than 1 year for any critical element of the 5G public network.

The Agreement of the Council of Ministers classifying certain 5G suppliers as high-risk suppliers may establish a different period for the replacement of equipment, products and services for the various 5G operators concerned on the basis of the impact that such replacement has on the network of each operator, the effect of replacing the various elements or parts of the 5G network,

the contracts for the supply of equipment signed and the existing supply capacity in the telecommunications equipment market.

5. The Agreement of the Council of Ministers classifying certain 5G suppliers as high-risk suppliers puts an end to the administrative procedure and may be directly appealed before the administrative court, without prejudice to the possibility of lodging an internal appeal prior to the administrative appeal.

6. High-risk suppliers whose telecommunications equipment, hardware, software or ancillary services provided are used solely and exclusively in 5G private networks or for the provision of 5G services under self-provision are classified as medium-risk suppliers.

Article 12. Determination of locations where equipment of suppliers classified as high risk may not be installed.

1. The National Security Council, following a report by the Ministry of Digital Transformation, may determine the locations, areas and centres where equipment of suppliers classified as high risk may not be installed.

2. The determination of these locations, areas and centres shall include nuclear power plants, centres linked to National Defence and the locations, areas and centres that, due to their link to national security or to the maintenance of certain essential services for the community or strategic sectors, are determined by National Security Council.

3. At radio stations that provide coverage to these locations, areas and centres, 5G operators may not use in the access network of a 5G public network telecommunications equipment, transmission systems, switching or routing equipment and other resources, enabling the transport of signals, hardware, software or ancillary services from suppliers that have been classified as high risk.

4. Likewise, for the installation, modification or adaptation of radio stations that provide coverage to these previously declared locations, areas and centres, taking into account their link to national security or to the maintenance of certain essential services for the community or strategic sectors, 5G operators must request authorisation from the State Secretariat for Telecommunications and Digital Infrastructure. The granting of this authorisation shall take into account telecommunications equipment, transmission systems, switching or routing equipment and other resources, enabling the transport of signals, hardware, software or ancillary services that are to be installed, the technical conditions for the use of the public radio domain, and the intrinsic characteristics and purposes to be protected in those previously declared locations, areas and centres.

In the granting of these authorisations, the State Secretariat for Telecommunications and Digital Infrastructure may assess the plans that 5G operators may submit for the technological renewal or replacement of radio transmission equipment and in the access network, which affect the previously declared locations, areas and centres for which authorisation is requested.

The deadline for the granting of these authorisations is 3 months, with the request being understood to have been rejected in the absence of an express decision. The decision, whether express or presumed, ends the administrative procedure and may be directly appealed before the administrative court, without prejudice to the possibility of lodging an internal appeal prior to the administrative appeal.

5. The determination and dissemination of these locations shall be treated as classified material in accordance with the regulations established in Law 9/1968 of 5 April 1968 on official secrets.

Article 13. Diversification in the supply chain.

1. 5G operators must design a strategy for diversification in the supply chain of telecommunications equipment, transmission systems, switching or routing equipment and other resources enabling the transport of signals in a 5G public network.

2. In the access network, 5G operators must have radio transmission equipment that is provided by at least two different suppliers in order to promote the continuity of 5G services, easier substitutability of equipment and to avoid sole dependence on a single supplier.

For this purpose, suppliers are deemed not to be different if they all belong to the same group of companies, in accordance with the criteria set out in Article 42 of the Commercial Code.

3. At the network core and in the control and management systems and support services, there may be a single supplier.

4. In the event that, as a result of business mergers, the number of suppliers included in the supply chain diversification strategy is reduced, which means that the minimum limit of two different suppliers established in the previous section is not met, the 5G operator must notify the Ministry of Digital Transformation. The Ministry shall encourage the Government, by means of an agreement adopted by the Council of Ministers, after hearing the 5G operators and 5G suppliers concerned, to decide whether it is possible to maintain a single supplier, taking into account the specific conditions of the merger, the market situation of the suppliers, the alternatives for the supply of viable replacement equipment and products, the deployment of such equipment and products in the operator's 5G network, especially in critical elements of the 5G network, the classification of the supplier as high risk, the intrinsic difficulty in carrying out equipment replacement, equipment upgrade cycles, the migration from non-standalone to standalone 5G networks, as well as the economic impact.

5. The Ministry of Digital Transformation, if it considers that continuity in the provision of 5G services and the physical or logical integrity of the 5G network are not guaranteed, that there is extensive exposure to equipment installed by a supplier that in certain circumstances may jeopardise the functionality and operability of the 5G network, or in order to ensure security in the provision of services used by National Security, National Defence or different Public Administrations, and taking into account whether there is a classification of high-risk suppliers, alternatives for the supply of viable replacement equipment and products, the deployment of such equipment and products in the operator's 5G network, especially in critical elements of the 5G

network, and equipment upgrade cycles, may modify the supply chain diversification strategy of a 5G operator.

Before approving the modification, a hearing procedure must be carried out with the 5G operator and 5G supplier(s) concerned for a period of 15 working days. The decision ends the administrative procedure and may be directly appealed before the administrative court, without prejudice to the possibility of lodging an internal appeal prior to the administrative appeal.

Chapter IV

Risk analysis by obliged parties

Article 14. Risk analysis by 5G operators.

1. 5G operators must analyse the risks of 5G networks and services, detecting vulnerabilities and threats that affect them both as an economic agent and through the network elements, infrastructure, resources, facilities and services that they use or provide in the installation, deployment and operation of 5G networks or in the provision of 5G services.

2. 5G operators that own or manage network elements of a 5G public network must, in their risk analysis, carry out a detailed and individualised study of the threats and vulnerabilities affecting the elements, infrastructure and resources that make up a 5G network and which are set out in Annex I.

3. The risk analysis carried out by a 5G operator shall take into account at least the following factors:

a) Parameterisation and configuration of network elements and functions.
b) Software integrity and updating policies.
c) Permission strategies to access physical and logical assets.
d) Dependence on certain suppliers for critical elements of the 5G network.

e) External agents, including organised groups capable of attacking the network.
f) Computer equipment and devices connected to the network.
g) Elements of corporate users and external networks connected to the 5G network.
h) The interrelationship with other services essential to society.

4. In order to carry out a comprehensive treatment of the security of 5G networks and services, the 5G operator shall collect from its suppliers the security practices and measures adopted in the products and services they have supplied, taking into account the risk factors indicated in this chapter and the risk profile of the supplier. This information must be provided by the suppliers and its treatment shall be confidential, so that it can only be used by 5G operators to carry out risk analysis and management, and by the Ministry of Digital Transformation and the other public bodies responsible for the implementation of the provisions of Royal Decree-Law 7/2022 of 29 March 2022 and this Scheme for the exclusive purposes thereof.

5. The risk analysis of the 5G operator shall include a prioritisation and hierarchy of risks based on the following parameters:

a) Impact on a critical element of the 5G public network.
b) Type of resource, infrastructure and service that may be affected.
c) Impact on the integrity and technical maintenance of the network or the continuity of service.
d) Detection and recovery capacity.
e) Number and type of users affected.
f) Type of information whose integrity may have been compromised.

6. A new risk analysis by the 5G operator must be carried out and submitted to the Ministry of Digital Transformation by 1 October 2024 and every 2 years thereafter.

Article 15. Risk analysis by 5G suppliers.

1. 5G suppliers must analyse the risks of telecommunications equipment, hardware and software and ancillary services involved in the functioning or operation of 5G networks or in the provision of 5G services, detecting vulnerabilities and threats that affect both the company's management and such equipment, hardware, software and services.

2. 5G suppliers must provide this risk analysis to the Ministry of Digital Transformation, upon request.

3. Notwithstanding the provisions of the previous section, 5G suppliers that have been classified as high risk or medium risk must submit to the Ministry of Digital Transformation a risk analysis of their equipment, products or services involved in 5G networks and services within 6 months of being classified as high risk or medium risk.

4. 5G suppliers that are classified as high risk or medium risk must carry out the risk analysis every 2 years and submit it to the Ministry of Digital Transformation.

Article 16. Risk analysis by 5G corporate users.

1. 5G corporate users that have been granted rights to use the public radio domain to install, deploy or operate a 5G private network, or to provide 5G services for professional purposes or self-provision, must analyse the risks of 5G networks and services, detecting vulnerabilities and threats affecting network elements, infrastructure, resources, facilities and services that they use or provide in the installation, deployment and operation of 5G private networks or in the self-provision of 5G services.

2. The 5G corporate users mentioned in the previous section must provide this risk analysis to the Ministry of Digital Transformation, upon request.

Article 17. Confidentiality of risk analysis information.

1. The Ministry of Digital Transformation may collect from the obliged parties the information necessary for the risk analysis.

2. The obliged parties must provide the information within 15 working days from the day following notification of the information request.

3. Failure to comply with the information requests formulated in accordance with the previous section when 1 month has passed since the end of the period given for compliance is classified as a serious infringement.

4. The information that the obliged parties provide on the risk analysis is considered confidential and may not be used for a purpose other than the fulfilment of the objectives and obligations established in Royal Decree-Law 7/2022 of 29 March 2022, in this Scheme and in the acts that are issued in implementation of both provisions.

Chapter V
Risk management by obliged parties

Article 18. Duty to manage security risks.

The obliged parties must take appropriate technical and organisational measures to manage the risks involved in the installation, deployment and operation of 5G networks and in the provision of 5G services, based on Royal Decree-Law 7/2022 of 29 March 2022, this Scheme and the acts that are issued in implementation of both provisions.

Article 19. Security management by 5G operators.

1. 5G operators must ensure the secure installation, deployment and operation of 5G public networks and the secure provision of publicly available 5G services, by implementing operating

and monitoring techniques and procedures to ensure the security of 5G networks and services, as well as compliance with regulations in this area.

2. 5G operators have the following security obligations aimed at mitigating risks:

a) Adopt technical and operational measures to ensure the physical and logical integrity of 5G networks or any of their elements, infrastructure and resources, as well as continuity in the provision of 5G services.
b) Adopt specific contingency plans and measures to ensure the continuity of other services essential to society that depend on 5G networks and services.
c) Select and identify persons who can access the physical and logical assets of the network, and perform the maintenance of access logs.
d) Maintain user credentials for network access in the possession of the operator.
e) Use only products, resources, services or systems certified for the operation of 5G networks, or in any parts or elements thereof.
   In particular, the GSMA Network Equipment Security Assurance Scheme (NESAS) applies.
f) Comply with the standards or technical specifications applicable to networks and information systems.
   In particular, the technical standard ISO/IEC 27001: Information Security Management applies.
g) Comply with European certification schemes for products, services or systems, whether or not specific to 5G technology, which are used in the operation of 5G networks and services.
h) Undergo, at their own expense, a security audit carried out by a public entity or a private entity accredited for this purpose.
   In particular, 5G operators must submit to the Ministry of Digital Transformation on an annual basis an audit on the implementation of the GSMA Network Equipment Security Assurance Scheme (NESAS) and the technical standard ISO/IEC 27001: Information Security Management.
i) Require their suppliers to comply with security standards, from the design of products and services to their commissioning.
j) Control their own supply chain and the diversification strategy they have designed.

3. In particular, 5G operators that own or operate critical elements of a 5G public network additionally have the following additional obligations:

a) They must design a strategy for diversification in the supply chain of telecommunications equipment, transmission systems, switching or routing equipment and other resources enabling the transport of signals in a 5G public network, in compliance with the provisions of Article 13.
b) They may not use in the critical network elements telecommunications equipment, transmission systems, switching or routing equipment and other resources, enabling the transport of signals, hardware, software or ancillary services from suppliers that have been classified as high risk in accordance with the provisions of Article 11.
c) They may not use in the access network of a 5G public network telecommunications equipment, transmission systems, switching or routing equipment and other resources, enabling the transport of signals, hardware, software or ancillary services from suppliers that have been classified as high risk, at those radio stations that provide coverage in the locations, areas and centres that have been identified in accordance with the provisions of Article 12.
d) They must locate the critical elements of a 5G public network within the national territory, without prejudice to the provisions of Article 5(4).

4. 5G operators that own or operate critical elements of a 5G public network must submit a new supply chain diversification strategy to the Ministry of Digital Transformation by 1 October 2024.

In addition, the supply chain diversification strategy must be submitted to the Ministry of Digital Transformation each time it is subject to modification.

Likewise, 5G operators that own or operate critical elements of a 5G public network must submit information on the state of implementation of the supply chain diversification strategy to the Ministry of Digital Transformation by 1 October of each year.

5. 5G operators must submit to the Ministry of Digital Transformation a new description of the technical and organisational measures designed and implemented to manage and mitigate risks by 1 October 2024 and every 2 years thereafter.

Article 20. Security management by 5G suppliers.

1. 5G suppliers must ensure the security of the telecommunications equipment, hardware, software or ancillary services they provide and which are used by 5G networks and services.

2. 5G suppliers have the following security obligations aimed at mitigating risks:

a) Comply with security standards, from the design of equipment, products and services to their commissioning.
   In particular, the technical standard ISO/IEC 27001: Information Security Management applies.
b) Strengthen software integrity, updating and patch management.
c) Accredit the certification of information technology products and services that are used in 5G networks and services.
   In particular, the GSMA Network Equipment Security Assurance Scheme (NESAS) applies.
d) Ensure the implementation of standard technical and organisational security measures through a certification system.
e) Perform a security audit of their equipment, products and services.
   In particular, 5G suppliers must submit to the Ministry of Digital Transformation on an annual basis an audit on the implementation of the GSMA Network Equipment Security Assurance Scheme (NESAS) and the technical standard ISO/IEC 27001: Information Security Management
f) Provide information on possible interferences by third parties in the design, operation and functioning of their equipment, products and services.
g) Collaborate with 5G operators and 5G corporate users by providing information and certifying compliance with the security standards for the equipment, products and services they provide.

3. 5G suppliers must provide the Ministry of Digital Transformation with a description of the technical and organisational measures designed and implemented to manage and mitigate risks, upon request.

4. Notwithstanding the provisions of the previous paragraph, 5G suppliers that have been classified as high risk or medium risk must submit to the Ministry of Digital Transformation a report on the technical and organisational measures designed and implemented to manage and mitigate risks within 6 months of being classified as high risk or medium risk.

5. Every 2 years, high-risk and medium-risk 5G suppliers must submit to the Ministry of Digital Transformation a description of the technical and organisational measures designed and implemented to manage and mitigate risks.

Article 21. Security management by 5G corporate users.

1. 5G corporate users that have been granted rights to use the public radio domain to install, deploy or operate a 5G private network, or to provide 5G services for professional purposes or self-provision, must ensure the secure installation, deployment and operation of 5G private networks and the secure self-provision of 5G services, by implementing operating and monitoring techniques and procedures to ensure the security of 5G networks and services.

2. The aforementioned 5G corporate users may not use in the critical network elements telecommunications equipment, transmission systems, switching or routing equipment and other resources, enabling the transport of signals, hardware, software or ancillary services from suppliers that have been classified as medium risk.

3. The aforementioned 5G corporate users must provide the Ministry of Digital Transformation with a description of the technical and organisational measures designed and implemented to manage and mitigate risks, upon request.

Article 22. Security management by public administrations.

1. Public administrations must take appropriate technical and organisational measures to manage the risks involved in the installation, deployment and operation of 5G networks and in the provision of 5G services.

2. In particular, public administrations wishing to carry out the installation, deployment and operation of 5G networks, whether public or private, or the provision of 5G services, whether publicly available or for self-provision, may not, for reasons of national security, use equipment, products and services provided by high-risk or medium-risk suppliers.

Article 23. Conditions for compliance with the obligations.

In compliance with the obligations laid down in the previous articles, the obliged parties shall take into account and apply that which is established in Royal Decree-Law 7/2022 of 29 March 2022, in this Scheme and in the acts that are issued in implementation of both provisions.

Article 24. Confidentiality of risk management information.

1. The Ministry of Digital Transformation may collect from the obliged parties the information necessary for risk management.

2. The obliged parties must provide the information within 15 working days from the day following notification of the information request.

3. Failure to comply with the information requests formulated in accordance with the previous section when 1 month has passed since the end of the period given for compliance is classified as a serious infringement.

4. The information that the obliged parties provide on risk management is considered confidential and may not be used for a purpose other than the fulfilment of the objectives and obligations established in Royal Decree-Law 7/2022 of 29 March 2022, in this Scheme and in the acts that are issued in implementation of both provisions.

Chapter VI

Other compliance measures for the security of 5G networks and services

Article 25. Duty of cooperation in the modification and implementation of the ENS5G.

All obliged parties, as well as public administrations, manufacturers, importers, distributors and those who place on the market and sell terminal equipment and devices to connect to a 5G network and to be able to provide 5G services must cooperate and submit the information required for modification and implementation of the ENS5G.

Article 26. Certification of equipment and products.

By Order of the head of the Ministry of Digital Transformation, the use of a specific piece of equipment, system, programme or service by obliged parties may be made subject to prior certification under Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on cybersecurity, or under certification schemes and technical standards for the certification of 5G equipment and products that may be approved at European or international level.

Article 27. Compliance with foreign investment and competition law.

The obligations laid down in Royal Decree-Law 7/2022 of 29 March 2022, in this Scheme and in the acts that are issued in implementation of both provisions are understood to be without prejudice to the application of the control instruments on foreign direct investments for obliged parties of Spanish nationality, as well as to the application of competition law.

Article 28. Terminal equipment.

The manufacture, import, distribution, placing on the market and selling of terminal equipment and devices to connect to a 5G network and to be able to provide 5G services shall be conditional on compliance with the security requirements for digital products and the applicable essential requirements related to cybersecurity, adopted in accordance with European legislation, in particular in relation to the protection of personal data, privacy and protection against fraud.

Article 29. International cooperation.

1. The Ministry of Digital Transformation shall cooperate closely with the institutions of other Member States of the European Union and with the institutions of the European Union in the proposal to modify and implement the National Security Scheme for 5G Networks and Services and, in general, shall collaborate with the various specialised international organisations in order to be able to carry out a comprehensive and holistic treatment of the security of 5G networks and services.

2. In particular, the Ministry of Digital Transformation may share information related to the analyses carried out by the institutions of the European Union and with other Member States of the European Union while preserving, as required by law, the security, commercial interests and confidentiality of the information collected in the preparation of the analysis, and may use the information sent to it by other States or the institutions of the European Union for implementation. It may also carry out these analyses jointly with other Member States of the European Union.

Chapter VII
Implementation of the ENS5G

Article 30. Competence for implementation of the ENS5G.

1. The Ministry of Digital Transformation shall be the department responsible for implementing the ENS5G and performing the other functions conferred on it by Royal Decree-Law 7/2022 of 29 March 2022.

2. The Ministry of Digital Transformation shall coordinate with the other bodies responsible for cybersecurity and critical infrastructure to ensure consistent implementation of the ENS5G.

Article 31. Powers for implementation of the ENS5G.

The Ministry of Digital Transformation, in the exercise of the functions assigned to it by Royal Decree-Law 7/2022 of 29 March 2022 and the ENS5G, may exercise, among others, the following powers:

a) Develop, specify and detail the content of the ENS5G.
b) Authorise the installation, modification or adaptation of radio stations that provide coverage to certain locations, areas and centres under the terms set out in Article 12(4).
c) Formulate information requests to the obliged parties, which must be answered within 15 working days from the day following its notification, in order to be able to exercise the functions assigned to it by Royal Decree-Law 7/2022 of 29 March 2022, the ENS5G and their implementing regulations and, in particular, to verify and control compliance with the respective obligations imposed on the obliged parties.
d) Carry out audits or order them to verify and control compliance with the respective obligations that Royal Decree-Law 7/2022 of 29 March 2022, the ENS5G and their implementing regulations impose on the obliged parties.

e) Carry out inspections by civil servants assigned to the State Secretariat for Telecommunications and Digital Infrastructure and exercise the power to impose penalties under the terms indicated in the following chapter.
f) Grant public aid.
g) Exercise its other functions under the applicable legislation.

Chapter VIII
Inspection and penalty system

Article 32. Powers of inspection.

In the implementation and supervision of the provisions of Royal Decree-Law 7/2022 of 29 March 2022, the ENS5G and their implementing regulations, the Ministry of Digital Transformation shall exercise all the powers of the inspection function provided for in said regulations and in Title VIII of Law 11/2022 of 28 June 2022 on General Telecommunications.

Article 33. Penalty system.

The penalty system laid down in Articles 30 and 31 of Royal Decree-Law 7/2022 of 29 March 2022 shall apply.

ANNEX I

Elements, infrastructure and resources that make up a 5G network

1. Description of the 5G-SA network architecture.

For the analysis required in this National Security Scheme for 5G Networks and Services, a reference network architecture is used, following the recommendation of the 3GPP and specification ETSI TS 123 501.

The following figure shows a simplified schema of a 5G-SA architecture for non-roaming scenarios (which will be used generically as a basis). Elements not shown in the figure are UDR, UDSF, UCMF, CHF, 5G-EIR, NWDAF and SEPP.

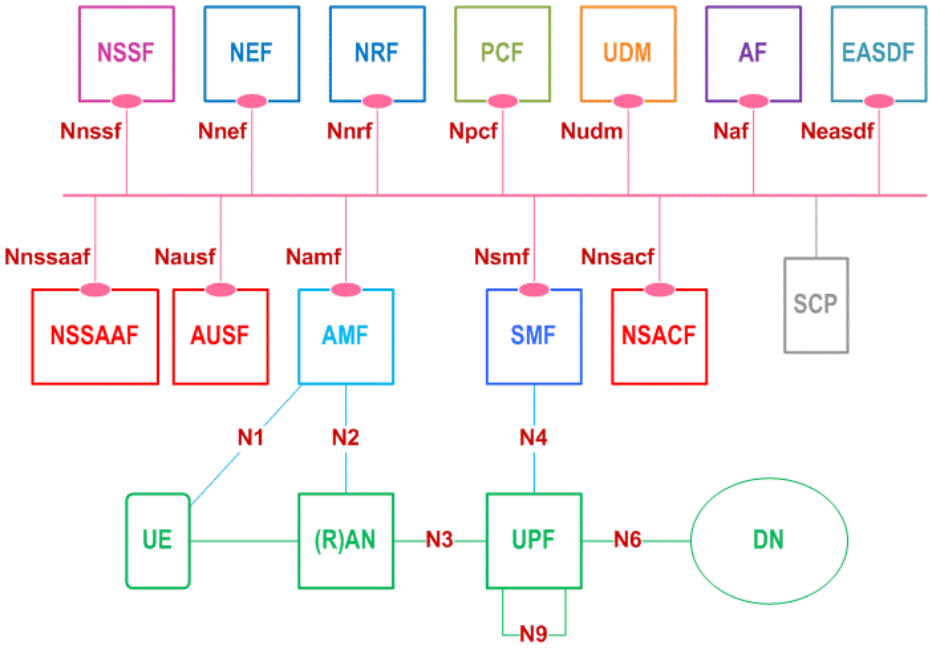


Figure 1: 5G architecture according to specification ETSI TS 123 501

These network elements are software functions that are deployed over a virtualisation infrastructure (itself composed of virtualisation software and hardware), which can be dedicated and specific to a network function, or common for several functions, including network functions of several 5G suppliers. In this scenario, the infrastructure to host the virtualised network functions

can be diversified both geographically and by different 5G suppliers, as will be described later in this document.

In addition to the network elements, a set of systems for the operation and management of the GER network (also called OSS, Operations Support System) are deployed.

2. Identification and description of 5G-SA network environments.

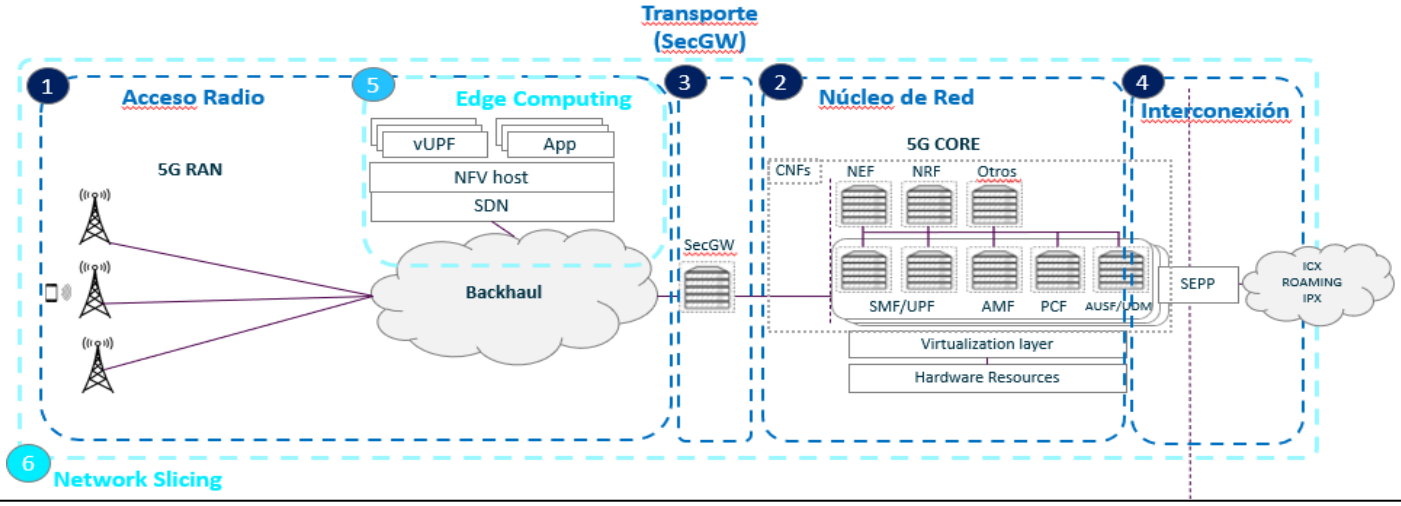
In order to break down the complexity of the architecture of a 5G-SA network, it is divided into network environments.

A network environment is a pool of assets that have a particular role and characteristics within the network that differentiate them from other environments.

Two types of environment can be distinguished:

a) Primary Environments: Primary environments are considered to be those that are specific to the technology or nature of 5G that would not exist without its deployment.
b) Secondary Environments: Secondary environments are considered to be those that are common in a telecommunications operator.

The following figure (Figure 2) shows a classification of the 5G-SA network by environment:



Acceso Radio	Radio Access
Transporte (SecGW)	Transport (SecGW)
Núcleo de Red	Network Core
Interconexión	Interconnection

3. Primary network environments.

Primary network environments include Radio Access, Network Core, Transport-Backhaul (SecGW), Roaming Interconnection and Network Control, Management and Operation Systems.

a) Radio Access: The radio access environment (RAN) is responsible for providing coverage to terminals so that they can connect to the network. The following functions in the environment stand out:

   i) Operation and maintenance of the radio site. The software allows each site to be configured with a number of cells per technology to be able to provide service to users and, during the operation of the base station, monitors its status to detect possible problems or faults, the occurrence of which would report an alarm to the management system so that the operator is aware and resolves the problem.
   ii) Signalling. In order for users to register on the network and establish bearer services for their communications, signalling is necessary between the terminals, the base station, and the network core, and part of these functions are performed by the base station software.
   iii) Radio-resource management. The radio resources of a given cell are shared between different users and the software of the base station is responsible for distributing them among those users (quality of each user's radio link, speed demand, etc.). The software can also distribute the users between the cells of its base station (or even with cells from neighbouring sites), so that the distribution of users is more homogeneous between neighbouring cells.
   iv) Mobility. The base station software manages the transfer of user communications between different cells, from their site or neighbouring sites, as users move across the network.

v) Transport. Physical communication with the rest of the network is carried out by means of IP, electrical or optical links, and the base station has to be responsible for managing these links (prioritisation between the different types of traffic going through these links, VLAN configuration, link monitoring, etc.).

The 5G network, in the radio access network (RAN), is implemented with a single type of network element generically called gNodeB (gNB). Most 5G radio access network suppliers have different gNB models, adapted to different types of scenarios.

Generically, the following types exist:

i) Macro gNB: provide greater coverage area and traffic capacity. They are typically installed on rooftops of buildings or places with high radio visibility, with the aim of providing overall capacity and coverage.

ii) Micro gNB: lower power, aimed at providing coverage in specific locations, either small public spaces (such as squares) or indoor spaces (such as event venues, small offices, etc.), or to provide complementary capacity to the general or macro layer. They are installed mainly at points of high capacity demand, to absorb such demand.

iii) Indoor gNB systems: specialised in covering large indoor spaces, with numerous low power radiating points, to distribute 5G coverage through said indoor space. They are typically installed in large office buildings, sports stadiums, metros, etc.

In this context, a 5G radio access network site will consist of a baseband and several remote heads and/or active antennas. The number of remote heads and active antennas will depend on the number of bands present at the site, and the number of sectors.

The gNB software is common to the baseband, remote heads and active antennas, and is also common among the various mobile communications systems present at the site

(2G, 3G, 4G and/or 5G). The base station communicates with the network core through the NG interface and with the mobile terminals through the air interface.

b) Network Core: The core of the 5G-SA network consists of a number of 3GPP-standardised network functions that communicate with each other by SBI (Service Based Interfaces) connections, allowing full meshing according to the needs of each of them.

The key principles of this 5G-SA architecture are:

i) Separate user plane (UP) functions from control plane (CP) functions, allowing for independent scalability, evolution and flexible implementations, e.g. centralised location or distributed (remote) location.

ii) Modularise the design of the function, e.g. to allow flexible and efficient network slicing.

iii) Allow each network function (and its associated services) to interact with other network functions, directly or indirectly through a proxy.

iv) Integrate different types of access, e.g. 3GPP access and non-3GPP access.

v) Support a unified authentication framework.

vi) Decouple in network functions the stateless logic functions related to computational capacity from the stateful functions related to storage capacities.

vii) Enable network data exposure in a secure way for the development of new services based on the data.

viii) Support simultaneous access to local services (with low latency requirements) and centralised services.

ix) Allow and accept traffic roaming with other networks, according to different architecture models.

The set of network core functions defined by 3GPP is as follows:

i. AMF – Access and Mobility Management Function: 5G network control plane function. Its main functions are registration management, mobility management, connection management, and management of various aspects related to security and access authorisation.

ii. SMF – Session Management Function: control plane function that is responsible for session management (establishment, modification and release), management and allocation of IPs to user terminals. In short, it is responsible for interacting with the user plane by creating, updating or deleting PDU sessions, while managing the context of the session with the UPF.

iii. UPF – User Plane Function: responsible for packet forwarding, routing and inspection, as well as for quality of service management. It represents the point of interconnection to the data network.

iv. PFC – Policy Control Function: responsible for providing policy rules to control plane network functions, including network slicing, roaming, mobility management and 5G quality of service policies. For the implementation of policies, it accesses the UDR subscription information.

v. NRF – Network Repository Function: responsible for service discovery, and maintains the profile and network instances available. Its main functions are service management, service discovery and access token, allowing two 5G network elements to communicate.

vi. SEPP – Security Edge Protection Proxy: the network function that allows secure interconnection between 5G networks, ensuring end-to-end confidentiality and/or integrity between the source network and destination network, for all 5G interconnection roaming messages.

vii. UDM – Unified Data Management: control plane function whose main missions are the generation of authentication credentials, user identity management, subscription management, access authorisation based on subscription data, and storage and management of the network functions that serve the user. The UDM uses the subscription data stored in the UDR.

viii. UDR – Unified Data Repository: unified repository of user data. These data are structured in different categories or types, and are accessible to the various network functions through a series of services exposed for their management and consultation (e.g. UDM, PCR, NRF, etc.).

ix. AUSF – Authentication Server Function: 5G network control plane function that is responsible for user authentication.

x. CHF – Charging Function: the charging functionality lies in the Converged Charging System (CCS), which offers online and offline charging functionalities. Its functions include the OCF (Online Charging Function) to carry out the online control of data sessions, the CDF (Charging Data Function) to build a CDR with the network information received, the ABMF (Account Balance Management Function) for balance management and consumption controls, the RF (Rating Function) to set a price for the usage received (both online and offline), and the CGF (Charging Gateway Function) to generate priced CDRs.

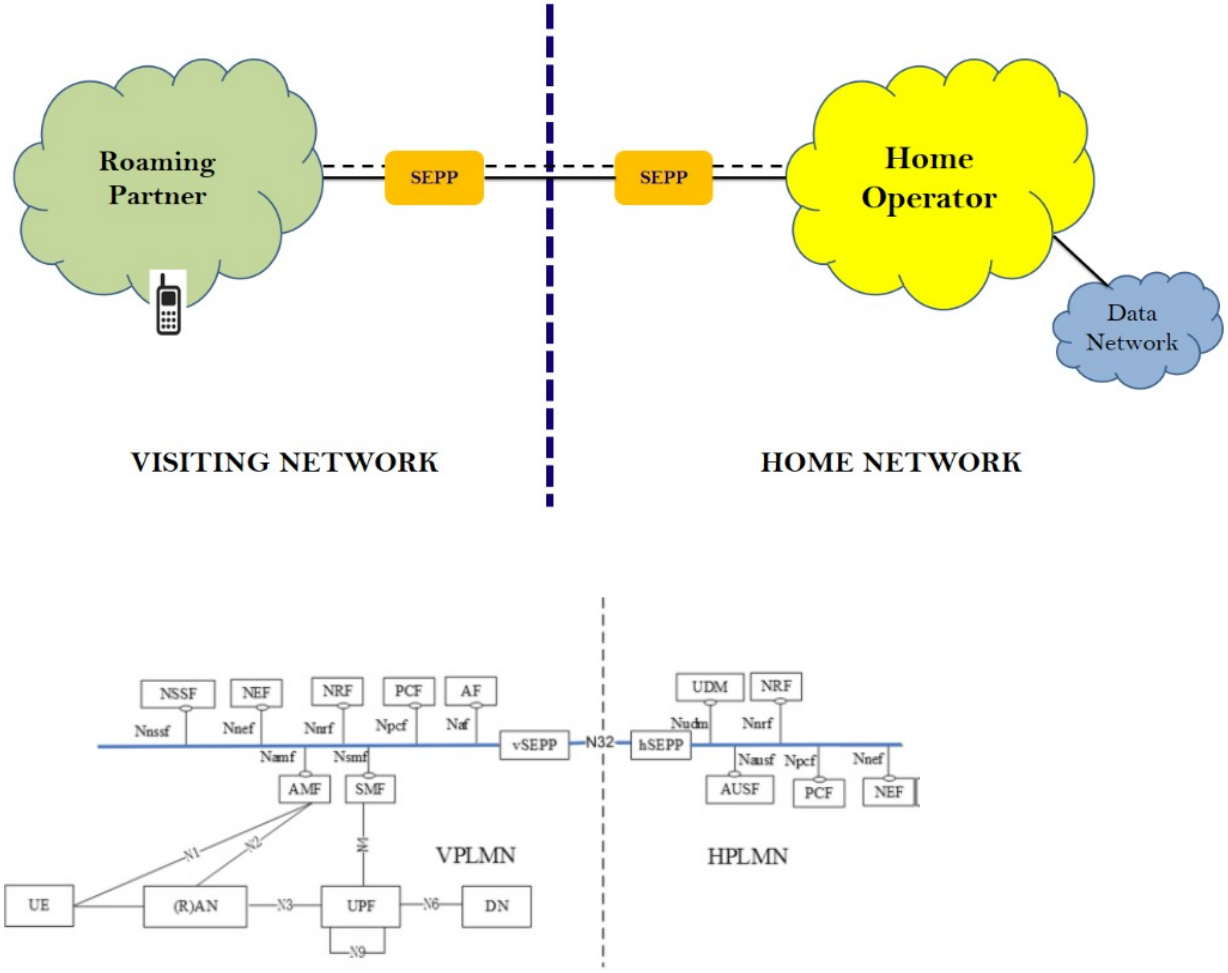
xi. NEF – Network Exposure Function: provides a means to securely expose the services and capabilities offered by 5G network functions.

xii. 5G-EIR – 5G-Equipment Identity Register: an optional functionality that offers the ability to check the identity status of the terminal (IMEI) and verify that it is not blacklisted.

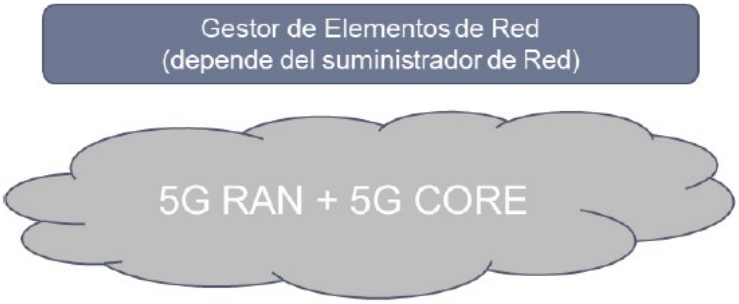
c) Transport-Backhaul (SecGW): The Security Gateway (SecGW) provides encryption of control plane and user plane traffic between Radio Access and Network Core environments, while also avoiding unnecessary exposure of critical elements.

d) Roaming Interconnection: The Roaming Interconnection environment is necessary for communication with other operators in order to allow a 5G user to roam internationally without interrupting their voice or broadband service.

The following figure (Figure 3) features the representation of a Roaming Interconnection Environment:



e) Control, Management and Operation Systems and Support Services: The 5G network core assurance process is supported by a set of operation support systems (OSS) shown in the figure below (Figure 4).



Gestor de Elementos de Red (depende del suministrador de Red)	Network Element Manager (depends on the network provider)

These OSS systems are not part of the service provision and, therefore, failures in their operation do not directly affect the availability of the network or the quality of the service provided on it. However, the unavailability of these systems would affect the capacity for monitoring, analysis, configuration and planning of the network described in the previous point. From the point of view of security, these managing systems are segmented according to the supplier and therefore a security incident in one of them would not affect the network functions that are not covered by this OSS.

4. Secondary network environments.

Secondary network environments include Virtualisation Platforms, Physical Infrastructure, Edge Computing and Network Slicing.

a) Virtualisation and Orchestration Platforms: Many of the elements of a 5G network are 'software' functions that are deployed over a virtualisation infrastructure (itself composed of virtualisation software and hardware), which can be dedicated and specific to a network function, or common for several functions (including network functions of several suppliers). In this context, the infrastructure to host the virtualised network functions is diversified both geographically and by different suppliers.

b) Physical infrastructure: The network elements and functions belonging to the different environments require a physical infrastructure where to place them, whose nature, availability and security will obviously depend on the criticality of the specific asset. This physical infrastructure provides the network elements and functions with the basic needs for proper functioning.

c) Multi-Access Edge Computing (MEC): Multi-access edge computing is a type of network architecture or environment that aims to bring user traffic processing and IT cloud computing functions to the edge of the network in order to ensure the operation of new use cases that require minimal latency.

In concept, it is defined in broader terms as an evolution of cloud computing that uses mobile and cloud technologies to separate application hosts from the data centre where they are located and move them to the edge of the network. This not only allows end-users to be closer to applications, but also allows computer services to be closer to the data they generate.

In this Edge Computing, both third-party applications and network functions to process user traffic at the edge coexist.

d) Network Slicing: This is a form of architecture that offers the possibility of creating, on a common shared physical virtualisation infrastructure, several virtual networks that are customised and logically isolated from each other, giving each of them a specific criticality according to the specific needs of applications, services, devices, customers or operators.

It is anticipated that, with this technology, 5G network and service operators can implement network segmentation to create multiple virtual networks with different connectivity sizes, adapting to the connection needs of the different users, specifically allocating the necessary resources to ensure the correct service.

In general, within the concept of network slicing, each virtual network (or portion of the network) encompasses an independent set of network logic functions that support the requirements of the particular use case. Each of them will be optimised to provide the network resources and mathematical reasoning for the service and traffic that will be used in the segmentation.

In the case of 5G-SA technology, capacity, connectivity, variety, speed, coverage and security will be allocated to meet the specific demands of each use case.

ANNEX II

RISK ANALYSIS AT NATIONAL LEVEL

1. Methodology used.

A risk analysis aims to identify and categorise the main threats to 5G networks and services, in order to determine corrective measures that can reduce their consequences or even prevent them.

Knowing this purpose, the next logical step is to establish the means to achieve this aim. A risk analysis must be carried out using a standardised, holistic methodology and in a consistent and logical order, detailing each of the aspects qualitatively and quantitatively. Otherwise, the calculated risk level could become distorted and with it, the criteria and priorities in the protection measures and/or key actions to be carried out.

The steps followed for the analysis carried out are shown below, as well as the sources of information used for the methodology used.

1) Identification and description of the 5G architecture, the existing network environments within it and the assets that comprise it, all subject to technological developments (see Annex I).
2) Identification of criticality for assets: in order to identify the impact of a threat on the network, it is necessary first to determine the criticality of each of the assets, based on the three main security axes (**CIA**: *Confidentiality*, *Integrity* and *Availability*).
3) Identification of 5G technology risks and their impact on identified assets: determining the potential threats present in this specific environment, classifying them by asset and identifying their risk level.
4) Identification of technical, organisational and strategic security measures to mitigate or reduce the risk level of the threats identified for each network environment. The effectiveness will be directly proportional to the degree of decrease in the risk level for a given threat and asset.

5) Management of the risks and remaining risks, in those threats whose level is considerable and cannot be reduced by any additional measure from design (see Annex III).

2. Factors that affect the criticality of an asset.

In a standardised and widely recognised way, three key factors or concepts are considered when assessing the criticality of the assets of a given scenario, when assessing the security of a solution is what applies.

The three main factors or concepts are confidentiality, integrity and availability (CIA triad).

a) Confidentiality: Confidentiality in an asset or network assesses the ability to prevent information contained in the asset, or in transit in the network, from being exposed to unauthorised users, who should not have access to it. The security measures to ensure confidentiality are diverse, from segmentation and access control, to robust encryption of information. The main factor when assessing the importance of confidentiality in an asset is the sensitivity of the information it stores or which transits through it. When addressing this factor, it is important to take into account the impact that compromising the asset can have on the rest of the network.

   Examples of risks that may compromise confidentiality are as follows: Spying on/intercepting user traffic/data on the network (Man-in-the-Middle/Eavesdropping), or obtaining operator credentials, either due to misconfiguration of the network, the absence of segmentation and access control policies, or, for example, the absence of encryption in highly exposed interfaces.

b) Integrity: Integrity is the ability to ensure that the data of an asset/user/network during its life cycle, whether in transit or storage, maintains its authenticity and is modified only by the agents authorised to do so, preventing unwanted sources from changing or manipulating such data. Measures to ensure integrity may include segmentation and

access control, checking hash in packets, checking integrity of versions to be installed or stored, etc.

Examples of risks that compromise integrity are: Manipulation of traffic/data (in transit or stored) on highly exposed 5G network interfaces.

c) Availability: Availability is based on the principle of ensuring that legitimate users have uninterrupted access to services and data within the environment for proper functioning. This concept aims to judge the importance of the asset and its solution in the business continuity of a particular service, resource or infrastructure. The level of availability impact that a risk has is usually anchored to the number and type of users affected by the downtime of the service caused by the attack.

To ensure availability, various measures can be taken, including the creation of backup solutions, the redundancy/resilience of assets, the ability to mitigate DDoS attacks, and effective service restoration procedures after downtime.

Within the environment, some risks that may compromise availability are as follows: Attacks such as, for example, denial of service to the network function, virtualisation infrastructure or physical infrastructure, or natural disasters, terrorism, etc.

3. Determination of the criticality of assets.

In this section, the criticality of the identified 5G-SA network assets is identified, taking into account the key factors and concepts (CIA triad) described in the previous section.

a) Access network.

- **gNB**: Medium criticality

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Red de acceso	Access network
Evaluación CIA	CIA evaluation
Criticidad	Criticality
2-Media	2-Media

Radio access nodes are located, for the most part, at sites in unsecured public places. This increases their exposure to on-site attacks. The impact on a cell may mean the interruption of service in a limited area, affecting a small number of users, and its traffic may be supported by another base station nearby. Therefore, the criticality is considered to be **low** as regards **availability**.

These nodes do not store user data. Despite this, if a *Man-in-the-Middle* (*MITM*) attack occurs, unencrypted traffic could be compromised (affecting only the few users connected to that node), as well as the possibility of manipulating ongoing packets if there is no integrity check. Due to the difficulty of carrying out this attack in the described scenario, **confidentiality** and **integrity** are assigned **medium** criticality.

b) Network core.

- **AUSF, UDM and UDR:** High criticality

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Núcleo de red	Network core
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Alta	High

An attack on confidentiality/integrity in these assets may involve the exposure of critical user information on the network (authentication, integrity and encryption keys, user provisioning data and their identities, etc.).

Obtaining this information would have a very high impact because it is information directly associated with customers' SIM cards, and its exfiltration can lead not only to an exposure of user communications, but also to the loss of image of the 5G network and service operator, and may involve the replacement of compromised SIM cards. For these reasons, the criticality of the asset in terms of **confidentiality** and **integrity** is **high**.

In addition, being a centralised element that receives authentication requests from all users of the network, in case it is not deployed with a correct solution that guarantees its resilience and business continuity, a disruption in it can cause a complete collapse of the network. Therefore, as regards **availability**, its criticality is also **high**.

- **AMF**, **NRF** and **NEF**: Medium criticality

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Núcleo de red	Network core
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Alta	High
Media	Medium
Baja	Low

- **NRF**: Medium criticality

  This element has a map of the entire network, nodes and services. Unauthorised access may give details of network deployment, routing, DNNs, slices, services, etc. In addition, altering configuration can lead to internal communications errors in the network. For these reasons, the **confidentiality** and **integrity** of NRF are considered to be of **high** criticality.

  However, the fact that the service can be configured so that, in the event of a failure of the element, there is temporary continuity of the service between the network functions means that its **criticality** as regards availability is **low**.

- **AMF**: Medium criticality

  By being in charge of managing the mobility of users, an attack or unauthorised access can allow sensitive information (user identities, location at Tracking Area level, and even the identifier of the node

where the customer is located when the terminal is in connected mode) to be obtained or exfiltrated.

For this reason, for risks of exfiltration rather than alteration of information, the criticality is considered to be **high** as regards **confidentiality**, and **medium** as regards **integrity**.

On the other hand, since it serves only a part of the network users, the criticality in terms of **availability** is considered to be **medium**.

- **NEF**: Medium/low criticality

  This element is responsible for ensuring the authentication, confidentiality and integrity of the communications from entities external to the network core, against any of the internal functions of the network core (*SBI* interface). Unauthorised access may allow the modification of a security policy between the functions external to the network core and the internal ones. However, this network function is not used for the provision of general service to 5G users. For that reason, **confidentiality** and **integrity** are considered to be **medium**.

  As regards **availability**, the failure of this equipment, in case of no redundancy, would only affect those services that need external communication with the elements of the network core, which would not have a considerable impact and that is why it is considered to be **low**.

- **SMF/UPF** and **PCF**: Low criticality

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

Descripción del activo	Description of the asset

Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Núcleo de red	Network core
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Baja	Low

In this category, the following elements are grouped, in which, in general, an impact on them does not have a noticeable impact on the provision of the 5G service. Therefore, their criticality assessment is low.

- **SMF/UPF**: Low criticality

  The SMF is responsible for session establishment, and the UPF is responsible for user plane management: it decapsulates user traffic coming from radio access and routes it to other data networks. Unauthorised access can disable a user's session, but it would be established in another SMF/UPF. In addition, the use of the SecGW between the access network and the network core makes an *MITM* impossible, which means its criticality in terms of **confidentiality** and **integrity** is **low**.

  In addition, in terms of **availability**, its criticality is also considered to be **low**. This is because a user can only be in one AMF, but their sessions can be in various SMFs/UPFs.

- **PCF**: Low criticality

  This element is not particularly critical for data services. Although it has policies related to services and pricing, AMFs/SMFs are always configured to be able to provide service without this element. A normal effect of PCF failure in data service is not being able to

charge customers online. The possible impact on the voice service can be mitigated by 2G/3G voice service. For these reasons, its criticality with regard to the **different criteria** would be **low**.

c) Transport-Backhaul.

- **SecGW**: Medium criticality

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Transporte - Backhaul	Transport-Backhaul
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Media	Medium

The transport network connects the elements of the core with those of the access network. A possible outage of this in one of its sections means that only the area of radio access nodes in which such an outage occurs is affected and, temporarily, it is possible to force the traffic to not pass through this element in said area. Therefore, as regards **availability**, the criticality is **medium**.

On the other hand, compromising a site or intercepting traffic leads to significant information leakage, since it is the element in charge of encrypting information in transit that arrives from a large number of nodes. For this reason, as regards **confidentiality**, it is assigned a **high** criticality. As this communication is encrypted, altering it is complicated. Therefore, the criticality in terms of **integrity** is considered to be **medium**.

d) Roaming Interconnection.

- **SEPP**: Medium criticality

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Interconexión Roaming	Roaming Interconnection
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Alta	High
Media	Medium
Baja	Low

This element allows the exchange of signalling with other networks in roaming scenarios. Although it is an element exposed to other networks, it only transports traffic of roaming users, and not that of domestic users. This fact means that the criticality as regards **availability** is **medium**.

On the other hand, the confidentiality of communications and their integrity are important aspects (especially the former), since it is an environment in which, in the absence of adequate protections, sensitive information can be obtained or exfiltrated from users, even those who are not roaming. This means that the criticality as regards **confidentiality** is **high**.

It is an environment that the industry and standardisation bodies have taken very seriously, where, natively, manufacturers are going to include

encryption and integrity configuration capabilities. This means that, if traffic is encrypted, attacking the **integrity** is more complicated. For all these reasons, it is assigned **medium** criticality.

e) Control and management systems and support services.

- **GER**: Medium criticality

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Sistemas de gestión/operación y servicios de soporte	Management/operation systems and support services
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Alta	High
Media	Medium
Baja	Low

These elements allow the correct operation of the elements that make up the 5G network environment. They can manage an entire network environment, exchanging configuration messages that can give fraudulent orders to equipment, or even transport credentials.

Therefore, the **integrity** and **confidentiality** of this element are considered to be **high**.

However, an interruption or lack of communication with the network by the management systems does not lead to a failure in the network, and the criticality as regards **availability** is considered to be **low**.

f) Virtualisation/orchestration infrastructure.

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Infraestructura de virtualización/orquestación	Virtualisation/orchestration infrastructure
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Alta	High
Media	Medium
Baja	Low

- **Virtualisation infrastructure**: High criticality

  All elements of the 5G network core are deployed over a virtualised infrastructure. This means that any attack that manages to disrupt its operation, be able to control its nodes, intercept traffic, modify the operation, etc., can have serious consequences on the provision of the service, even leading to its total interruption. For the reasons described, the criticality as regards **confidentiality**, **integrity** and **availability** is **high**, and this is considered a critical asset within the network.

- **Virtualisation management/orchestration**: Medium criticality

In a similar way to management/operation systems and support services, the most critical aspects of this asset are the **confidentiality** and **integrity** of communications and access, considered to be of **high** criticality. This is because the *virtualisation orchestrators* control all elements of the virtualisation platform, which could be breached or attacked (e.g. removal of *CNFs*, hardware shutdown, etc.).

However, an interruption or lack of communication with the network by the orchestrator does not cause a failure in virtualisation platforms, and the criticality in terms of **availability** is considered to be **low**.

g) Physical infrastructure.

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Infraestructura Física	Physical Infrastructure
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Alta	High
Media	Medium
Baja	Low

- **Physical infrastructure**: Medium criticality

  Physical infrastructure is especially vulnerable to attacks that cause physical damage to equipment, theft, and power outages, etc. The availability of this is fundamental to the operation of networks and

services, since it will be used as a basis for many network functions and management systems throughout the network. Therefore, the criticality value, in terms of **availability**, is **high**.

The **confidentiality** and **integrity** of this asset are considered to be **low**, since it does not represent a risk to the information or communications itself, depending mainly on the protocols and logical control mechanisms implemented in the upper layers (virtualisation infrastructure, applications, etc.) in order to prevent information from being obtained if someone gets hold of an asset.

Summary Table: Asset Criticality Table

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

Descripción del activo	Description of the asset
Entorno de red	Network environment
Dominio	Domain
Activo	Asset
Primario	Primary
Secundario	Secondary
Infraestructura Física	Physical Infrastructure
Red de acceso	Access network

Núcleo de red	Network core
Transporte - Backhaul	Transport-Backhaul
Interconexión Roaming	Roaming Interconnection
Sistemas de gestión/operación y servicios de soporte	Management/operation systems and support services
Infraestructura de virtualización/orquestación	Virtualisation/orchestration infrastructure
Evaluación CIA	CIA evaluation
Criticidad	Criticality
Alta	High
Media	Medium
Baja	Low

4. Classification of assets according to criticality.

Based on the previous analyses and the contributions made by 5G network and service operators, a set of elements has been identified as critically important for the operation of 5G networks, for their configuration or management, or the services provided by them.

As stated in the previous section, all high criticality assets in the primary network environment belong to the network core. However, from the point of view of criticality, it is not possible to consider the network core as a homogeneous block. Therefore, a differentiated treatment is considered applicable in relation to the measures to guarantee the availability of the services they offer.

Thus, the network core is composed of various network functions (NF) that are deployed in virtualised infrastructures independent of the network function itself. The classification considers which of these entities are most critical not only from the point of view of redundancy, but also of the possible impact of unauthorised access or attacks from other networks.

In addition, it takes into account possible unauthorised access to the virtualised infrastructure on which these network functions are deployed, and establishes a relative importance between the different entities, stressing that, in order to obtain a complete service, all of them are necessary.

a) High criticality

The risk that would most compromise the 5G service would be unauthorised access to the AUSF/UDM/UDR environment. The AUSF has the authentication keys that allow access to any encrypted radio communication, and the UDM/UDR has all the user provisioning data and their identities, and precisely the 3GPP has included the use of SUCI (encrypted IMSI identity) to prevent that identity from travelling through the radio interface, since having a user's SUPI is the first step for any other attack. These are undoubtedly considered to be the most critical network functions since the impact of obtaining keys and entities is long-lasting (being associated with the SIM keys of customers). The loss of image of a 5G network and service operator due to an intrusion into these network functions would be enormous and could involve the replacement of compromised SIMs. However, the network design allows for provision of the service without any impact in the face of double failure of instances of any of these nodes.

b) Medium criticality

This category, from highest to lowest criticality, includes:

i. NRF: this element has a map of the entire network, nodes and services. With the NRF information, all the details of network deployment, routing, DNNs, slices, services, etc. are available. In addition, unauthorised access would make it possible to paralyse the 5G service since all network functions consult this entity to find out which destination network functions have the required service. However, the network functions have the NRF information cached, which would temporarily mitigate the attack. Furthermore, the network design allows for provision of the service without any impact in the face of double failure of instances of this node.

ii. SEPP: allows the exchange of signalling with other networks for roaming scenarios on the home network, or on other third-party networks. It is an exposed element, although 5G suppliers have developed a large number of functionalities to ensure its security and integrity. In addition, isolation between internal and external domains must be ensured.

iii. AMF: responsible for mobility management. An attack or unauthorised access to it would make it possible to obtain very sensitive information (user identity, location at Tracking Area level, and even gNB-ID of where the customer is located when their terminal is in connected mode), with the possibility of tracking the movement of users, and their signalling procedures related to mobility and session management. These elements are deployed in pool mode and are sized to simultaneously support failure of one node in each pool.

c) Low criticality

This category, again from highest to lowest criticality, includes:

i. SMF/UPF: SMF is responsible for session management (establishment, modification and release), management and allocation of IPs to user terminals, etc. It is also responsible for interacting with the user plane by creating, updating or deleting PDU sessions, as well as managing the context of the session with the UPF, while the UPF manages the user plane. These elements are much more redundant than the AMFs described above, and unauthorised access could disable a user's session, although this would be established in another SMF/UPF. The user plane or actual customer traffic is routed, in general, to other networks (internet/intranet) that are of lower security, so a user plane attacker has an easier time compromising the service by attacking the target server or even the terminal.

ii. PCF: not particularly critical, since the AMF/SMF are configured to be able to provide service without this element, affecting, eventually, the online pricing of customers.

d) Non-critical

The CHF, NEF, NWADF and 5G-EIR elements are not considered critical for the provision of the 5G service because, in the event of a partial or total failure or unavailability of any of them, customers should not be affected in the service.

5. Identification of threats and risks in 5G technology.

Article 9 of Royal Decree-Law 7/2022 of 29 March 2022 specifies the need to identify the risk factors to be analysed according to technological developments, the incorporation of new technological advances, functionalities and standards, the situation of the electronic communications market and supply market, and the emergence of new threats and vulnerabilities.

The following sections cover the tasks performed.

5.1. Criteria for identifying the risk of an attack

To calculate the level of security risk that a threat introduces, we use three factors based on the following formulas:

Risk level = (Likelihood of occurrence) x (Impact on the network)

where, in turn,

(Impact on the network) = (Criticality of the asset) x (Scaling factor)

The concepts used are defined below:

a) Likelihood of occurrence: An assessment is made based on the following parameters:

i. *Degree of exposure of the asset to the vulnerability*: gives a measure of how exposed the analysed element is at a physical or logical level, and the level of accessibility/ease that the attacker may have in order to execute the threat.

ii. *Complexity or knowledge to develop the attack*: the likelihood of occurrence increases in the event that the attack can be carried out without much technical knowledge and the attack environment is simple to implement or automated tools are used.

iii. *Public knowledge of the vulnerability*: an attack is more likely the more known it is at the community level. In the event that the vulnerability is not widely known or handled only in certain circles (such as 5G suppliers or 5G network and service operators), its exploitation will be less likely.

iv. *Trace of the attack*: if the attack is carried out by brute force or leaves traceability on the networks, it is less likely that there will be attackers willing to exploit the vulnerability. These are cases in which impersonation cannot be carried out.

v. *Benefit from the success of the attack*: economic value, recognition, relevance, etc., of the achievement of the attack.

The possible values of the ***likelihood of occurrence*** are **Very High**, **High**, **Medium**, **Low**.

b) Impact on the network: similar to the *likelihood of occurrence*, a qualitative assessment is used to measure the impact the attack could have on the network.

The following parameters are used to evaluate the service and give an impact assessment:

i. *Criticality of the asset*: concept referred to above, encompassing *confidentiality*, *integrity* and *availability*.

ii. *Scaling factor*: identifies the importance and/or scope of the attack at the level of network impact. It takes into consideration both the scope (number of users that can be impacted) and the type of impact of the attack (credential leakage, decreased availability, etc.).

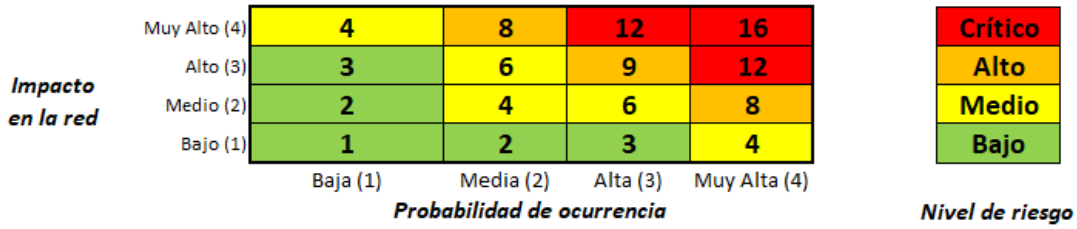
The possible values of the network impact of the attack are: **Very High**, **High**, **Medium**, **Low**, taking into account the above criteria.

c) ***Risk level***: This is the result of the two previous variables following the formula described above.

The possible values of the risk level are: **Critical**, **High**, **Medium**, **Low**.

5.2. Risk matrix

Taking into account the considerations of the previous section, the generic matrix that characterises the risk levels analysed later in this document is presented.



Impacto en la red	Impact on the network
Muy alto	Very high
Alto	High
Medio	Medium
Bajo	Low
Probabilidad de ocurrencia	Likelihood of occurrence
Baja	Low
Media	Medium
Alta	High
Muy alta	Very high
Nivel de riesgo	Risk level
Crítico	Critical
Alto	High
Medio	Medium
Bajo	Low

6. Threats or risks in a 5G-SA network.

Once assets have been identified and their criticality characterised, the next step in the risk analysis is to assess the threats or possible attacks to which each of these 5G-SA network assets are exposed.

It is important to emphasise that the same threat may have a different risk level depending on the asset or environment being assessed, in order to establish the correct priorities for mitigating actions that allow for increasing, within the same timeline, the security of the solution in the most efficient way possible.

The threats or risks in a 5G-SA network are detailed below:

a) Malicious activities due to improper or malicious access to management, extraction of sensitive information or unauthorised modification of parameterisation that causes unavailability of the element.

   These are those actions carried out by internal or external attackers that target network and infrastructure elements with the intention of stealing information, altering it or destroying, through configuration, a specific objective.

   This block includes, among others, the following threats:

   i. Network intrusions with the aim of obtaining information, through malicious access, lateral movements, escalation of privileges, due to lack of robust security policies (absence of access control, authentication, authorisation, segmentation, hardening, etc.). These include, among others, obtaining operator user credentials, sensitive customer information (data, user identifiers, and authentication, encryption and integrity keys), or useful network configuration information (ports, versions, etc.) that serves as a vector of additional information to carry out attacks of greater impact.

ii. Malicious and unauthorised modification of network configuration or parameterisation that may cause partial or total unavailability of the service in the asset or the network, as well as encouraging the exfiltration of traffic mentioned in the previous point.

A. Manipulation of configuration or parameterisation that affects the operation of the equipment (traffic routing policies, DNS configuration, user sessions, images of virtual network functions, etc.).
B. Manipulation of the equipment's security configuration (security policies, services offered in the application and operating system, cryptographic algorithms, access rules) and creation of backdoors.
C. Intentional or unintentional execution of malicious software/code (SQL or XSS injection, rootkits, malware/ransomware, etc.).

iii. Exploitation of vulnerabilities in hardware or software, which allow simple and effective access to be able to execute the threats discussed in the two previous points (known vulnerabilities/CVEs, new vulnerabilities and zero-day vulnerabilities).

b) Compromise of user communications or data through the capture, interception, hijacking of service traffic or its modification:

This category includes the actions taken to eavesdrop on, interrupt or alter user communications or data in the service plane, without the user's consent.

The main threats within this category would be:

i. Eavesdropping on communications of a certain user in environments with high level of exposure such as radio access or roaming interconnection.
ii. Obtaining sensitive information from users (user identifiers, location, services, etc.) in exposed interfaces that can be used as information vectors to carry out attacks of greater impact.

iii. Manipulation of communications in exposed interfaces through Man-in-the-Middle (MITM) activities and/or user data, with illegal actions such as fraud, impersonation, etc. being possible.

c) Denial of Service (DoS).

This category includes those actions, activities or incidents, malicious or not, that can cause a total or partial disruption to the equipment, affecting users of the network. The main threats within this category would be:

i. Volumetric denial-of-service attacks (DoS/DDoS): Flooding of traffic to the exposed interfaces of the assets (user devices, interconnections, etc.) seeking the overload of the capabilities of the elements, with the aim of causing a malfunction/disruption in the network.
ii. Targeted attacks on specific users with the aim of causing their unavailability on the network (e.g. jamming attacks or network deregistration).
iii. Unintentional damage by operators due to configuration errors: This covers unintentional actions by an operator with access to the management of an asset that may result in a failure or reduced functionality of the asset such as, for example, poor/erroneous configuration of network assets and their security capabilities (isolation, hardening, segmentation, etc.) or error in management or manipulation due to lack of knowledge, training or diligence.
iv. Malfunction of the element: This includes 'native' malfunction (for reasons beyond the configuration of the asset) that may cause a total or partial disruption of its service.

d) Physical threats.

These are aimed at destroying, rendering useless, altering or stealing physical assets from the physical infrastructure that hosts the network functions/elements.

Among the main threats are sabotage or terrorism against critical elements of network equipment, natural disasters, malfunctioning of the energy network and possible theft of

network equipment for the extraction of sensitive information and its subsequent exploitation.

e) Little training and awareness among employees on cybersecurity, as well as malpractice in managing the evolution of identified risks.

   Indeed, a lack of security awareness among employees increases the likelihood of occurrence of incidents such as ransomware attacks and other malware. Lack of security and operational training increases the likelihood of configuration errors due to lack of knowledge, exposing assets to unnecessary risks.

   In addition to all this, if a good risk management procedure is not carried out, monitoring its evolution in the network, it will be impossible to formulate a priority plan and implement security measures efficiently.

ANNEX III

RISK MANAGEMENT AT NATIONAL LEVEL

Once the different threats that affect 5G networks and services have been identified in Annex II, and with this, the initial risk situation, the next step is to envisage the security measures necessary to address, reduce or mitigate the identified risks.

These measures are:

1. Generic security measures:

1.1. Security configurations for equipment:

1.1.1. Configurations related to identification, authentication, control, auditing and monitoring of access to nodes. Nodes must be configured with:

a) Identity management policies, allowing to guarantee both authentication (verifying that whoever accesses is who they claim to be) and authorisation (accessing only with the privileges that are strictly necessary) when accessing the nodes.
b) User lifecycle management policies.
c) Traceability capabilities and auditing policies, allowing all accesses (who connects to and disconnects from nodes and when) to be recorded, as well as the executed commands and alarms that identify possible equipment failure.
d) Good security practices when defining and managing user credentials and access, always forcing credentials to be robust.
e) Ability to be configured in such a way that no detailed information is provided in the event that access fails and blocking policies are established that make it difficult to obtain credentials.

1.1.2. Hardening:

a) Self-protection of the nodes, ensuring that only the services necessary for their proper functioning are active.

b) Nodes must have the ability to separate the management interface from the service interface, either through a physical or logical interface.
c) Nodes must be able to detect and handle malformed packets while keeping services unaffected.
d) Nodes must be able to cope with high volumes/peaks of traffic by having self-regulating mechanisms to prevent their CPU from crashing.
e) Ability to protect stored data and information.
f) Network nodes/elements must be configured in such a way that booting via unauthorised memory devices is not allowed.
g) Nodes must be configured in such a way that malicious exploitation of the APIs they expose is not possible.

1.1.3. Conducting periodic security tests. These are necessary to study whether new vulnerabilities have appeared for the components of the asset.

1.2. Architectural and functional security.

1.2.1. Different network planes, as well as network areas or environments with different exposure levels, must be isolated.

1.2.2. Flow control: Ability to limit traffic to certain IP addresses, Protocols, Applications, to avoid overloading the link, making an attack more complicated to carry out.

1.3. Security Measures in Physical Infrastructure:

a) Registration, validation and control of physical access authorisations to sites.
b) Physical access controls, by electronic and/or mechanical means, to network plants and relevant buildings.
c) Physical surveillance and electronic security of the site.
d) Electronic security systems installed and maintained.

1.4. Security awareness for employees and the chain of command.

1.5. Training of employees in technology, security and processes.

1.6. Implementation of clear incident management processes, having a record of own incident history and updated knowledge of industry incidents.

2. Specific security measures related to a 5G network.

2.1. Software control:

a) Ensure the integrity of the software update before it is installed, avoiding the injection of malicious code, Trojans or non-legitimate versions (manipulated by a third party).
b) Ensure that there are no backdoors.
c) Ensure that there are no known high-risk vulnerabilities (CVEs) at the time of deployment of the product on site.
d) Comply with internationally recognised security certifications for equipment.

2.2. Encryption and integrity of communications between the terminal and network must be configured at both AS (Access Stratum) and NAS (Non-Access Stratum) levels to protect user privacy in the air interface. This measure is activated both in the RAN (AS) and in the Network Core (NAS).

2.3. Encryption and integrity of control plane and user plane communications between the radio access node (RAN) and the Network Core must be configured.

2.4. User privacy must be guaranteed in the air interface.

2.5. Improvements in authentication algorithms between the user's terminal and the network that come natively with 5G-SA technology must be corroborated.

2.6. Native improvements in authentication algorithms between the user's device and the network, to mutually ensure that communication is legitimate.

2.7. The different elements that handle signalling traffic must have measures to prevent impersonation of the network elements themselves in the roaming network, as well as of users who are not roaming.

2.8. Confidentiality, integrity and authentication must be ensured in communications between a source and destination operator, using protocols/equipment/secure solutions (SEPP).

2.9. It is necessary to establish the corresponding security policies in order to expose in the interconnection only the interfaces and messages necessary for the service, avoiding giving unnecessary information that could be used fraudulently.

2.10. Isolation of virtualised network functions: Classification of the different virtualised elements in the infrastructure according to different levels of exposure and criticality of the element.

2.11. Isolation of traffic: Secure design of the virtualisation architecture to guarantee the traffic necessary for the functioning of the virtualisation layer, so that the operation/functioning of the network will be guaranteed.

2.12. It is necessary to follow the guidelines of the Equipment Security and Architectural Security Requirements/Configurations for each and every one of the elements that make up the virtualisation architecture.

2.13. Monitoring and Detection: Monitoring the traceability of accesses and commands executed on critical network elements, in order to be able to identify illegitimate activities at the time of their execution and also for the forensic analysis of possible attacks.

2.14. Mitigation: Capabilities to mitigate possible volumetric attacks aimed at denial of service in highly exposed interfaces.

2.15. Critical environments: Redundancy/recovery (backup) performance tests in critical environments must be carried out prior to deployment of the solution.