MINISTÈRE DE LA
TRANSFORMATION
NUMÉRIQUE

| |
|---|
| RÉF.: |
| RÉF.C.M.: |

| | |
|---|---|
| Chapitre<br>Texte<br><br>(À compléter dans le «Journal officiel de l'État») | |

**PROJET DE DÉCRET ROYAL APPROUVANT LE RÉGIME NATIONAL DE SÉCURITÉ POUR LES RÉSEAUX ET SERVICES 5G**

Les communications mobiles de cinquième génération ou 5G constituent un nouveau paradigme des communications électroniques avec un grand potentiel de transformation au bénéfice de la société et de l'économie, car elles ouvrent la possibilité d'intégrer de nouvelles fonctionnalités qui auront un grand impact comme l'informatique en réseau, elles permettront la création de réseaux virtuels, offriront une faible latence et fourniront des services à forte valeur ajoutée pour la société et l'économie dans des domaines tels que la médecine, les transports et l'énergie. Par conséquent, l'Union européenne et l'Espagne, directement et par l'intermédiaire de la facilité pour la reprise et la résilience, encouragent le déploiement rapide des réseaux 5G et la mise en œuvre de projets démontrant leur utilité pour différents secteurs grâce à la fourniture de services 5G.

Les réseaux et services 5G présentent des avantages comparatifs en matière de sécurité par rapport aux générations précédentes. Cependant, ils présentent également des risques spécifiques découlant, par exemple, de leur architecture de réseau plus complexe, ouverte et désagrégée, et de leur capacité à transporter d'énormes volumes d'informations et à permettre l'interaction simultanée de personnes et de choses multiples. Leur interconnexion avec d'autres réseaux et le caractère transnational d'un grand nombre de menaces ont un impact sur leur sécurité, et l'utilisation généralisée prévisible de ces réseaux pour des fonctions économiques et sociétales essentielles augmentera l'impact potentiel des incidents de sécurité dont ils souffrent.

Ces nouveaux risques spécifiques pour la sécurité des communications mobiles 5G ont été traités en termes réglementaires par le décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à garantir la sécurité des réseaux et services de communications électroniques de cinquième génération, qui intègre pleinement la recommandation (UE) 2019/534 de la Commission européenne du 26 mars 2019 sur la cybersécurité des réseaux 5G, ainsi que les recommandations que la communication de la Commission européenne du 29 janvier 2020 sur le déploiement sécurisé de la 5G dans l'Union — Mise en œuvre de la boîte à outils de l'Union (COM/2020/50 final) a fourni aux États membres en ce qui concerne l'utilisation de cette boîte à outils.

Le décret-loi royal 7/2022 du 29 mars 2022 a récemment été modifié par la septième disposition finale du décret-loi royal approuvant des mesures urgentes pour la mise en œuvre du plan pour la reprise, la transformation et la résilience dans les domaines du service public de justice, de la fonction publique, du gouvernement local et du patronage, dans le but de renforcer les contrôles à effectuer par le gouvernement et le ministère de la transformation numérique sur les conditions dans lesquelles l'installation des différents équipements, les éléments, fonctions et systèmes de la technologie 5G, le déploiement des réseaux 5G et la fourniture de services de communications électroniques 5G sont réalisés, afin d'atteindre l'objectif ultime poursuivi par ledit décret royal, qui est, comme indiqué à son article 1er, d'établir des exigences de sécurité pour l'installation, le déploiement et l'exploitation de réseaux de communications électroniques et la fourniture de services de communications électroniques et sans fil basés sur la technologie de cinquième génération (5G).

Le décret-loi royal nº 7/2022 du 29 mars 2022, précité, prévoit son développement réglementaire par le biais du régime national de sécurité pour les réseaux et services 5G. Ainsi, l'article 21 du décret-loi royal 7/2022 du 29 mars 2022 prévoit que le gouvernement approuve, par décret royal, sur proposition du ministère de la transformation numérique, à la suite d'un rapport du Conseil national de sécurité, un système national de sécurité pour les réseaux et services 5G.

À son tour, l'article 20 du décret-loi royal 7/2022 du 29 mars 2022 dispose que le régime national de sécurité des réseaux et services 5G procède à un traitement global et global de la sécurité des

réseaux et services 5G, en tenant compte des contributions à la portée de chaque agent de la chaîne de valeur 5G afin d'assurer le fonctionnement continu et sécurisé du réseau et des services 5G. À cette fin, le système national de sécurité des réseaux et services 5G procède à une analyse des risques au niveau national en ce qui concerne la sécurité des réseaux et services 5G, et identifie, précise et élabore des mesures au niveau national pour atténuer et gérer les risques analysés.

Enfin, pour compléter le cadre de référence, il convient de mentionner que l'article 5, paragraphe 3, du décret-loi royal 7/2022 du 29 mars 2022 dispose que le système national de sécurité des réseaux et services 5G procède à un traitement complet de la sécurité des réseaux et services 5G, en tenant compte des contributions à la portée de chaque agent de la chaîne de valeur 5G, ainsi que des réglementations, recommandations et normes techniques de l'Union européenne, de l'Union internationale des télécommunications (UIT) et d'autres organisations internationales, afin de garantir l'objectif ultime d'utilisation et d'exploitation sécurisées des réseaux et services 5G en Espagne.

Pour se conformer à ce mandat, le présent décret royal approuve le régime national de sécurité pour les réseaux et services 5G.

Le principe de nécessité est respecté, puisque ce décret royal est émis pour garantir un bien d'intérêt général, tel que la sécurité et la confiance dans les communications électroniques. Il respecte le principe de proportionnalité, étant donné que les mesures sont adaptées aux risques recensés dans chaque cas. Il est conforme au principe de sécurité juridique parce que le cadre réglementaire existant en matière de sécurité est reconnu et que seuls des exigences et des contrôles appropriés au caractère unique des réseaux et services 5G et à leurs risques sont ajoutés. Le principe de transparence est respecté, car les parties prenantes ont pu participer à la procédure d'élaboration du décret royal. Enfin, il respecte le principe d'efficacité puisque les charges administratives ont été limitées au minimum nécessaire pour atteindre l'objectif visé d'assurer la sécurité des réseaux et des services 5G.

La présente disposition a été soumise à la procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information

prévue par la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information.

Ce décret royal est pris en vertu des dispositions de l'article 149, paragraphe 1, point 21, et de l'article 149, paragraphe 1, point 29, de la Constitution espagnole, qui confèrent à l'État, respectivement, une compétence exclusive en matière de système général de télécommunications et en matière de sécurité publique.

En vertu de cette disposition, conformément aux dispositions de l'article 21 du décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à assurer la sécurité des réseaux et services de communications électroniques de cinquième génération, sur proposition du ministre de la transformation numérique, à la suite du rapport du Conseil national de sécurité et de l'avis du Conseil d'État, et après délibération du Conseil des ministres lors de sa réunion du xx xxxxxx 2024,

DÉCRÈTE:

Article unique. Approbation du système national de sécurité pour les réseaux et services 5G.

Le régime national de sécurité pour les réseaux et services 5G est approuvé, lequel est inséré ci-dessous.

Première disposition additionnelle. Examen du régime national de sécurité pour les réseaux et services 5G.

Le gouvernement, par décret royal, sur proposition du ministère de la transformation numérique, à la suite d'un rapport du Conseil national de sécurité, examine le régime national de sécurité pour

les réseaux et services 5G lorsque les circonstances l'exigent et, en tout état de cause, tous les quatre ans.

Deuxième disposition additionnelle. Application du décret-loi royal 7/2022 du 29 mars 2022 et du régime national de sécurité pour les réseaux et services 5G aux générations successives de communications électroniques.

Le décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à assurer la sécurité des réseaux et services de communications électroniques de cinquième génération et le système national de sécurité pour les réseaux et services 5G approuvé s'appliquent aux générations de communications électroniques après la cinquième génération, alors qu'il n'existe pas de norme spécifique pour ceux-ci.

Première disposition finale. Attribution des pouvoirs

Ce décret royal et le régime qu'il approuve sont pris en vertu des dispositions de l'article 149, paragraphe 1, point 21, et de l'article 149, paragraphe 1, point 29, de la Constitution espagnole, qui confèrent à l'État, respectivement, une compétence exclusive en matière de système général de télécommunications et en matière de sécurité publique.

Deuxième disposition finale. Application complémentaire du règlement sur la sécurité et l'intégrité des réseaux de communications électroniques.

1. Dans toutes les matières non régies par le présent décret royal et le régime qu'il approuve, les dispositions de la loi 11/2022 du 28 juin 2022 sur les télécommunications générales et ses règlements d'application s'appliquent.

2. Dans toutes les matières non régies par la loi 11/2022 du 28 juin 2022 sur les télécommunications générales et ses règlements d'application, le décret-loi royal 12/2018 du 7

septembre 2018 relatif à la sécurité des réseaux et des systèmes d'information et la loi 8/2011 du 28 avril 2011 établissant des mesures de protection des infrastructures critiques, ainsi que leurs règlements d'application respectifs, s'appliquent.

Troisième disposition finale. Habilitation pour l'élaboration de la réglementation et la modification des annexes.

1. Le ministre de la transformation numérique est habilité à mettre en œuvre les dispositions du présent décret royal et le régime qu'il approuve.

2. Le chef du ministère de la transformation numérique est habilité à modifier par arrêté le contenu des annexes du système national de sécurité des réseaux et services 5G en fonction de l'évolution du progrès technologique, de l'approbation de nouvelles normes techniques et de nouveaux systèmes de certification pour les équipements de télécommunications et les produits connectés, et du développement de différentes configurations et paramètres techniques des réseaux et services 5G et des générations futures de communications électroniques.

Quatrième disposition finale. Entrée en vigueur.

Le présent décret royal et le régime qu'il approuve entrent en vigueur le jour suivant celui de leur publication au «Journal officiel de l'État».

À SOUMETTRE AU CONSEIL DES MINISTRES

Madrid, le XX xxxxxx 2024

LE MINISTRE DE LA TRANSFORMATION NUMÉRIQUE

José Luis Escrivá Belmonte

**RÉGIME NATIONAL DE SÉCURITÉ POUR LES RÉSEAUX ET SERVICES 5G**

Chapitre premier

Dispositions générales

Article premier — Régime national de sécurité pour les réseaux et services 5G

Le régime national de sécurité pour les réseaux et services 5G (ci-après l'«ENS5G») est approuvé dans le cadre de l'élaboration des dispositions du décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à assurer la sécurité des réseaux et services de communications électroniques de cinquième génération, notamment en application du chapitre IV de celui-ci.

Article 2. Objectifs.

L'ENS5G poursuit les objectifs suivants:

a) Effectuer un traitement complet et global de la sécurité des réseaux et services 5G, en tenant compte des contributions à la portée de chaque agent de la chaîne de valeur 5G.
b) Assurer le fonctionnement continu et sécurisé du réseau et des services 5G.
c) Assurer la sécurité de bout en bout de l'écosystème généré par la technologie 5G.
d) Renforcer la sécurité dans l'installation et l'exploitation des réseaux de communications électroniques 5G et dans la fourniture de services de communications mobiles et sans fil soutenus par les réseaux 5G.
e) Promouvoir un marché des fournisseurs suffisamment diversifié pour les réseaux et services de communications électroniques 5G afin de garantir la sécurité sur la base de raisons techniques, stratégiques et opérationnelles et éviter, pour ces raisons, la présence de fournisseurs ayant une cote de risque élevée ou moyenne dans certains éléments ou domaines du réseau.
f) Renforcer la protection de la sécurité nationale.

g) Renforcer l’industrie et encourager les activités nationales de RDI dans le domaine de la cybersécurité liées à la technologie 5G.

Article 3. Définitions.

Aux fins de l’ENS5G, les définitions figurant dans le décret-loi royal 7/2022 du 29 mars 2022 relatif aux exigences visant à assurer la sécurité des réseaux et services de communications électroniques de cinquième génération sont utilisées, ainsi que les définitions figurant dans la loi 11/2022 du 28 juin 2022 sur les télécommunications générales et le code européen des communications électroniques.

Article 4 Champ d’application.

L’ENS5G s’applique aux entités réglementées suivantes:

a) Opérateurs 5G.
b) Fournisseurs 5G.
c) Les entreprises utilisatrices de la 5G qui se sont vu accorder le droit d’utiliser le domaine radiophonique public pour installer, déployer ou exploiter un réseau privé 5G, ou pour fournir des services 5G à des fins professionnelles ou à des fins propres.

Article 5. Réseau 5G.

1. Un réseau de communications électroniques 5G comprend au moins les éléments, infrastructures et ressources suivants:

a) Ceux relatives aux fonctions du noyau de réseau.
b) Les fonctions de transport et de transmission.
c) Le réseau d’accès.

d) Les systèmes de contrôle et de gestion et les services de soutien.

e) Les fonctions de l'informatique de périphérie, la virtualisation du réseau et la gestion des composants.

f) Ceux relatifs aux échanges de trafic ou à l'interconnexion avec les réseaux externes et Internet.

g) Autres composants et fonctions visés à l'annexe I.

2. La description détaillée des éléments, infrastructures et ressources qui composent un réseau 5G figure à l'annexe I.

3. Les éléments suivants sont des éléments critiques d'un réseau 5G:

a) Ceux relatives aux fonctions du noyau de réseau.

b) Les systèmes de contrôle et de gestion et les services de soutien.

c) Le réseau d'accès dans ces zones géographiques et les emplacements à déterminer.

4. Les éléments critiques d'un réseau 5G doivent être situés sur le territoire national. Toutefois, certains éléments, fonctions et systèmes tant du noyau du réseau que des systèmes de contrôle et de gestion et des services d'appui peuvent être situés en dehors du territoire national, à condition que le ministère de la transformation numérique puisse exercer les pouvoirs qui lui sont conférés par le décret-loi royal 7/2022 du 29 mars 2022, en particulier les pouvoirs d'inspection et de sanction prévus au chapitre V de celui-ci, afin qu'il puisse procéder à une vérification complète du fonctionnement, de l'opérabilité et des conditions d'utilisation desdits éléments critiques d'un réseau 5G et, le cas échéant, être en mesure d'adopter des mesures conservatoires ou définitives sur lesdits éléments, fonctions et systèmes ou sur les équipements utilisés dans l'exercice des pouvoirs conférés au ministère de la transformation numérique par le décret-loi royal 7/2022 du 29 mars 2022 et la loi 11/2022 du 28 juin 2022 sur les télécommunications générales.

Si le ministère de la transformation numérique conclut que les éléments, fonctions et systèmes du cœur du réseau ainsi que les systèmes de contrôle et de gestion et les services de soutien situés en dehors du territoire national affectent, soit pour des raisons de mise en œuvre de mesures techniques ou de mesures stratégiques, la sécurité ou l'intégrité du réseau 5G ou nuisent de

manière significative à l'exercice de ses pouvoirs de surveillance et de ses pouvoirs d'inspection, il peut exiger du propriétaire du réseau 5G qu'il implante ces éléments, fonctions et systèmes sur le territoire national. À cet effet, la délocalisation des éléments, fonctions et systèmes doit avoir lieu dans le délai indiqué par le ministère de la transformation numérique dans sa résolution, après avoir entendu le propriétaire du réseau 5G. Cette période ne peut être inférieure à trois mois.

Article 6. Traitement exhaustif de la sécurité.

1. La sécurité est comprise comme un processus de bout en bout composé de tous les éléments humains, matériels, techniques, juridiques et organisationnels liés au réseau ou service 5G. L'ENS5G vise à réaliser un traitement exhaustif de la sécurité des réseaux et des services 5G.

2. À cette fin, l'ENS5G a pris en compte et doit tenir compte dans les futures mises à jour ou modifications des règlements, recommandations et normes techniques de l'Union européenne, de l'Union internationale des télécommunications (UIT) et d'autres organisations internationales.

De même, l'ENS5G a pris en compte et doit prendre en considération dans les futures mises à jour ou modifications les contributions, analyses de risques, plans d'atténuation des risques et stratégies de diversification de la chaîne d'approvisionnement qui ont été fournis et qui doivent être fournis par les entités obligées conformément aux obligations établies par le décret-loi royal 7/2022 du 29 mars 2022, dans ce régime et dans le reste de la réglementation.

3. Dans ce contexte de sécurité de bout en bout, les entités obligées doivent procéder à un traitement complet de la sécurité des réseaux, éléments, infrastructures, ressources, installations et services dont elles sont responsables. Pour cela, ils doivent effectuer, au moyen d'une méthode globale, une analyse des vulnérabilités, des menaces et des risques qui les affectent en tant qu'agents économiques et des composantes susmentionnées, ainsi qu'une gestion adéquate et globale de ces risques grâce à l'utilisation de techniques et de mesures appropriées pour atteindre leur atténuation ou leur élimination et pour atteindre l'objectif ultime d'une utilisation et d'une exploitation sécurisées des réseaux et services 5G.

Article 7. Gestion de la sécurité basée sur les risques.

1. L'analyse et la gestion des risques sont un élément essentiel du processus de sécurité et devraient être une activité continue qui est constamment mise à jour.

2. La gestion des risques permet de maintenir un environnement contrôlé dans le réseau ou le service 5G, en minimisant les risques à des niveaux acceptables. La réduction à ces niveaux est effectuée par l'application appropriée de mesures de sécurité, de manière équilibrée et proportionnée à la nature et aux caractéristiques du réseau, aux services à fournir et aux risques auxquels ils sont exposés.

Article 8. Suivi continu et réévaluation périodique.

1. Une surveillance continue permet de détecter les activités ou comportements anormaux et de réagir en temps utile.

2. L'évaluation en cours de l'état de sécurité des réseaux et services 5G permet de mesurer leur évolution, de détecter les vulnérabilités et d'identifier les défaillances de configuration.

3. Les mesures de sécurité sont réévaluées et mises à jour périodiquement, en adaptant leur efficacité à l'évolution des risques et des systèmes de protection, et éventuellement conduire à un réexamen de la sécurité si nécessaire.

## Chapitre II

## Analyse et gestion des risques au niveau national

Article 9. Analyse des risques au niveau national.

1. L’analyse des risques à effectuer au niveau national par l’ENS5G est celle qui figure à l’annexe II du présent régime.

2. Dans le cadre de cette analyse, il a été tenu compte des éléments suivants:

a) L’analyse globale des risques des réseaux et services 5G, en tenant compte des informations recueillies auprès des entités obligées.

b) L’examen des vulnérabilités liées à la chaîne d’approvisionnement des réseaux et services 5G.

c) L’évaluation du degré de dépendance des fournisseurs vis-à-vis de l’ensemble des réseaux et services 5G en Espagne, en tenant compte des analyses de risques et des stratégies de diversification des fournisseurs présentées par les opérateurs, ainsi que du risque d’interruption de l’approvisionnement en raison de circonstances économiques, corporatives ou commerciales affectant les fournisseurs.

d) L’évaluation de l’efficacité des mesures de sécurité mises en œuvre jusqu’à l’approbation de chaque analyse nationale des risques afin d’atténuer les risques mis en évidence par cette analyse.

Article 10. Gestion des risques au niveau national.

1. Les critères, exigences, conditions et délais pour les entités obligées de concevoir et de mettre en œuvre des techniques et des mesures d’atténuation des risques sont ceux énoncés à l’annexe III du présent régime.

2. Lors de la détermination de ces critères et exigences de gestion des risques, il a été tenu compte de l’analyse nationale des risques incorporée dans la présente stratégie et de l’évaluation de l’efficacité des mesures précédemment mises en œuvre par les entités obligées pour atténuer et gérer les risques dans les réseaux et services 5G.

## Chapitre III

## Mesures spécifiques visant à assurer la sécurité des réseaux et services 5G

### Article 11. Déclaration des fournisseurs de 5G à haut risque et à risque moyen.

1. Le gouvernement, au moyen d'un accord adopté par le Conseil des ministres, à la suite d'un rapport du Conseil national de sécurité et après avoir entendu les opérateurs 5G et les fournisseurs 5G concernés pour une période de quinze jours ouvrables, peut qualifier certains fournisseurs 5G de risques élevés.

À cette fin, le gouvernement analysera à la fois les garanties techniques de fonctionnement et de fonctionnement de leurs équipements, produits et services et leur exposition à des interférences extérieures.

2. En ce qui concerne l'analyse des mesures techniques et des garanties techniques relatives au fonctionnement et au fonctionnement de leurs équipements, produits et services, les aspects liés au respect des normes ou des spécifications techniques, à leur vérification au moyen de systèmes de certification ou à la réussite d'essais de sécurité ou d'audits effectués par des entités indépendantes sont évalués.

3. En ce qui concerne l'analyse des mesures stratégiques et de l'exposition aux interférences extérieures, les aspects suivants seront évalués:

a) Les liens entre les fournisseurs et leur chaîne d'approvisionnement avec les gouvernements de pays tiers.

b) La composition de leur capital social et la structure de leurs organes de direction.

c) Le pouvoir d'un État tiers d'exercer une pression sur l'action ou l'emplacement de l'entreprise.

d) Les caractéristiques de la législation et de la politique en matière de cyberdéfense, ainsi que le respect du droit international et des résolutions et accords des Nations Unies de cet État tiers.

e) Les accords de coopération en matière de sécurité, de cybersécurité, de criminalité informatique ou de protection des données signés avec le pays tiers concerné, ainsi que des traités internationaux sur ces questions auxquels cet État est partie.

f) Le degré d'alignement de la législation de l'État tiers sur la protection des données à caractère personnel sur celle de l'Espagne, avec le règlement général sur la protection des données approuvé par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, adoptée par l'Union européenne, ainsi qu'avec toute autre législation applicable en matière de sécurité des réseaux et systèmes d'information et de télécommunications.

4. L'accord du Conseil des ministres classant certains fournisseurs 5G en tant que fournisseurs à haut risque détermine la période pendant laquelle les opérateurs de la 5G doivent procéder au remplacement des équipements, produits et services fournis par ce fournisseur dans le réseau et les services de l'opérateur 5G, le cas échéant, compte tenu de la situation du marché des fournisseurs, des alternatives pour la fourniture d'équipements et de produits de remplacement viables, du déploiement de ces équipements et produits dans le réseau 5G de l'opérateur, en particulier dans les éléments critiques du réseau 5G et en fonction des éléments critiques spécifiques concernés, de la difficulté intrinsèque à effectuer le remplacement des équipements, des cycles de mise à niveau des équipements, de la migration des réseaux non autonomes vers les réseaux 5G autonomes, ainsi que de l'impact économique.

Pour déterminer la période de remplacement, l'accord du Conseil des ministres classant certains fournisseurs 5G en tant que fournisseurs à haut risque peut établir une période différente pour les différents éléments critiques du réseau public 5G en fonction du caractère critique de cet élément ou d'une partie de celui-ci, de son impact sur le fonctionnement et l'opérabilité du réseau et de la disponibilité d'équipements à ce moment sur le marché des équipements de télécommunications.

En aucun cas cette période ne peut être inférieure à un an pour un élément critique du réseau public 5G.

L'accord du Conseil des ministres classant certains fournisseurs 5G en tant que fournisseurs à haut risque peut fixer une période différente pour le remplacement d'équipements, de produits et de services pour les différents opérateurs 5G concernés en fonction de l'incidence qu'un tel remplacement a sur le réseau de chaque opérateur, de l'effet du remplacement des différents éléments ou parties du réseau 5G, des contrats de fourniture d'équipements signés et de la capacité d'approvisionnement existante sur le marché des équipements de télécommunications.

5. L'accord du Conseil des ministres classant certains fournisseurs 5G en tant que fournisseurs à haut risque met fin à la procédure administrative et peut faire l'objet d'un recours direct devant le tribunal administratif, sans préjudice de la possibilité d'introduire un recours interne avant le recours administratif.

6. Les fournisseurs à haut risque dont les équipements de télécommunications, le matériel, les logiciels ou les services auxiliaires fournis sont utilisés uniquement et exclusivement sur des réseaux privés 5G ou pour la fourniture de services 5G pour leur propre usage sont classés comme fournisseurs à risque moyen.

Article 12. Détermination des emplacements où l'équipement des fournisseurs classés comme présentant un risque élevé ne peut pas être installé.

1. Le Conseil national de sécurité, à la suite d'un rapport du ministère de la transformation numérique, peut déterminer les emplacements, les zones et les centres où les équipements des fournisseurs classés comme à risque élevé ne peuvent pas être installés.

2. La détermination de ces emplacements, zones et centres comprend les centrales nucléaires, les centres liés à la défense nationale et les emplacements, zones et centres qui, en raison de leur lien avec la sécurité nationale ou le maintien de certains services essentiels pour les secteurs communautaires ou stratégiques, sont déterminés par le conseil national de sécurité.

3. Dans les stations de radio qui assurent la couverture de ces emplacements, zones et centres, les opérateurs 5G ne peuvent pas utiliser dans le réseau d'accès d'un équipement de télécommunication du réseau public 5G, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources, permettant le transport de signaux, de matériel, de logiciels ou de services auxiliaires par des fournisseurs qui ont été classés comme présentant un risque élevé.

4. De même, pour l'installation, la modification ou l'adaptation de stations de radio qui assurent la couverture de ces sites, zones et centres précédemment déclarés, compte tenu de leur lien avec la sécurité nationale ou le maintien de certains services essentiels pour les secteurs communautaires ou stratégiques, les opérateurs 5G doivent demander l'autorisation du Secrétariat d'État aux télécommunications et aux infrastructures numériques. L'octroi de cette autorisation tient compte des équipements de télécommunications, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources permettant le transport de signaux, de matériel, de logiciels ou de services auxiliaires devant être installés, les conditions techniques d'utilisation du domaine radioélectrique public, ainsi que les caractéristiques et finalités intrinsèques à protéger dans les lieux, zones et centres précédemment déclarés.

Lors de l'octroi de ces autorisations, le Secrétariat d'État aux télécommunications et aux infrastructures numériques peut évaluer les plans que les opérateurs 5G peuvent soumettre pour le renouvellement technologique ou le remplacement des équipements de transmission radio et dans le réseau d'accès, qui affectent les emplacements, zones et centres précédemment déclarés pour lesquels l'autorisation est demandée.

Le délai d'octroi de ces autorisations est de trois mois, la demande étant réputée rejetée en l'absence de décision expresse. La décision, expresse ou présumée, met fin à la procédure administrative et peut faire l'objet d'un recours direct devant le tribunal administratif, sans préjudice de la possibilité d'introduire un recours interne avant le recours administratif.

5. La détermination et la diffusion de ces lieux sont traitées comme des questions classifiées conformément au règlement établi par la loi 9/1968 du 5 avril 1968 relative aux secrets officiels.

Article 13. Diversification de la chaîne d'approvisionnement.

1. Les opérateurs 5G doivent concevoir une stratégie de diversification de la chaîne d'approvisionnement des équipements de télécommunications, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources permettant le transport de signaux dans un réseau public 5G.

2. Dans le réseau d'accès, les opérateurs 5G doivent disposer d'équipements de transmission radio fournis par au moins deux fournisseurs différents afin de promouvoir la continuité des services 5G, de faciliter la le caractère substituable des équipements et d'éviter une dépendance exclusive à l'égard d'un seul fournisseur.

À ces fins, les fournisseurs sont réputés ne pas être différents s'ils appartiennent tous au même groupe de sociétés, conformément aux critères énoncés à l'article 42 du code de commerce.

3. Au cœur du réseau, dans les systèmes de contrôle et de gestion et les services de soutien, il peut y avoir un seul fournisseur.

4. Si, à la suite de fusions d'entreprises, le nombre de fournisseurs inclus dans la stratégie de diversification de la chaîne d'approvisionnement est réduit, ce qui signifie que la limite minimale de deux fournisseurs différents établie dans la section précédente n'est pas respectée, l'opérateur 5G doit en informer le ministère de la transformation numérique. Le ministère encourage le gouvernement, au moyen d'un accord adopté par le Conseil des ministres, après avoir entendu les opérateurs 5G et les fournisseurs 5G concernés, à décider s'il est possible de maintenir un fournisseur unique, en tenant compte des conditions spécifiques de la fusion, de la situation du marché des fournisseurs, des alternatives pour la fourniture d'équipements et de produits de remplacement viables, du déploiement de ces équipements et produits dans le réseau 5G de l'opérateur, en particulier dans les éléments critiques du réseau 5G, de la classification du fournisseur comme étant à haut risque, de la difficulté intrinsèque à effectuer le remplacement

des équipements, des cycles de mise à niveau des équipements, de la migration des réseaux non autonomes vers les réseaux 5G autonomes, ainsi que de l'impact économique.

5. Le ministère de la transformation numérique, s'il estime que la continuité de la fourniture des services 5G et l'intégrité physique ou logique du réseau 5G ne sont pas garantis, qu'il existe une exposition étendue aux équipements installés par un fournisseur qui, dans certaines circonstances, peuvent compromettre la fonctionnalité et l'opérabilité du réseau 5G, ou afin d'assurer la sécurité de la fourniture des services utilisés par la sécurité nationale, la défense nationale ou différentes administrations publiques, et en tenant compte de l'existence d'une classification des fournisseurs à haut risque, des solutions de rechange pour la fourniture d'équipements et de produits de remplacement viables, le déploiement de tels équipements et produits dans le réseau 5G de l'opérateur, en particulier dans les éléments critiques du réseau 5G, et les cycles de mise à niveau de l'équipement, peuvent modifier la stratégie en matière de diversification de la chaîne d'approvisionnement d'un opérateur 5G.

Avant d'approuver la modification, une procédure d'audition doit être menée avec l'opérateur 5G et le ou les fournisseurs 5G concernés pendant une période de quinze jours ouvrables. La décision met fin à la procédure administrative et peut faire l'objet d'un recours direct devant le tribunal administratif, sans préjudice de la possibilité d'introduire un recours interne avant le recours administratif.

## Chapitre IV

## Analyse des risques par les entités obligées

### Article 14. Analyse des risques par les opérateurs 5G.

1. Les opérateurs 5G doivent analyser les risques des réseaux et services 5G, en détectant les vulnérabilités et les menaces qui les affectent à la fois en tant qu'agent économique et à travers les éléments de réseau, l'infrastructure, les ressources, les installations et les services qu'ils

utilisent ou fournissent dans l'installation, le déploiement et l'exploitation des réseaux 5G ou dans la fourniture de services 5G.

2. Les opérateurs 5G qui possèdent ou gèrent des éléments de réseau d'un réseau public 5G doivent, dans leur analyse des risques, effectuer une étude détaillée et individualisée des menaces et des vulnérabilités affectant les éléments, infrastructures et ressources qui constituent un réseau 5G et qui figurent à l'annexe I.

3. L'analyse des risques effectuée par l'opérateur 5G tient compte au moins des facteurs suivants:

a) Le paramétrage et la configuration des éléments et fonctions du réseau.
b) L'intégrité du logiciel et politiques de mise à jour.
c) Les stratégies d'autorisation pour accéder à des actifs physiques et logiques.
d) La dépendance vis-à-vis de certains fournisseurs pour les éléments critiques du réseau 5G.
e) Les agents externes, y compris des groupes organisés capables d'attaquer le réseau.
f) Le matériel informatique et appareils connectés au réseau.
g) Les éléments d'utilisateurs en entreprise et de réseaux externes connectés au réseau 5G.
h) Les relations avec d'autres services essentiels à la société.

4. Afin de procéder à un traitement complet de la sécurité des réseaux et services 5G, l'opérateur 5G recueille auprès de ses fournisseurs les pratiques et mesures de sécurité adoptées dans les produits et services qu'ils ont fournis, en tenant compte des facteurs de risque indiqués dans le présent chapitre et du profil de risque du fournisseur. Ces informations doivent être fournies par les fournisseurs et leur traitement doit être confidentiel, de sorte qu'elles ne peuvent être utilisées que par les opérateurs 5G pour effectuer l'analyse et la gestion des risques, ainsi que par le ministère de la transformation numérique et les autres organismes publics chargés de la mise en œuvre des dispositions du décret-loi royal 7/2022 du 29 mars 2022 et du présent régime à des fins exclusives.

5. L’analyse des risques de l’opérateur 5G comprend une hiérarchisation et une hiérarchie des risques sur la base des paramètres suivants:

a) Impact sur un élément critique du réseau public 5G.
b) Type de ressource, d’infrastructure et de service susceptible d’être affecté.
c) Impact sur l’intégrité et la maintenance technique du réseau ou sur la continuité du service.
d) Capacité de détection et de récupération.
e) Nombre et type d’utilisateurs concernés.
f) Type d’information dont l’intégrité a pu être compromise.

6. Une nouvelle analyse des risques par l’opérateur 5G doit être effectuée et soumise au ministère de la transformation numérique au plus tard le 1er octobre 2024 et tous les deux ans par la suite.

Article 15. Analyse des risques par les fournisseurs 5G.

1. Les fournisseurs 5G doivent analyser les risques liés à l’équipement, au matériel et aux logiciels de télécommunications et aux services auxiliaires liés au fonctionnement ou à l’exploitation des réseaux 5G ou à la fourniture de services 5G, en détectant les vulnérabilités et les menaces qui affectent à la fois la gestion de l’entreprise et ces équipements, matériels, logiciels et services.

2. Les fournisseurs 5G doivent fournir cette analyse de risque au ministère de la transformation numérique, sur demande.

3. Nonobstant les dispositions du point précédent, les fournisseurs 5G qui ont été classés comme à risque élevé ou à risque moyen doivent soumettre au ministère de la transformation numérique une analyse des risques de leurs équipements, produits ou services impliqués dans les réseaux et services 5G dans les 6 mois suivant la classification comme risque élevé ou moyen.

4. Les fournisseurs 5G classés comme à risque élevé ou à risque moyen doivent effectuer l'analyse des risques tous les deux ans et la soumettre au ministère de la transformation numérique.

Article 16. Analyse des risques par les entreprises utilisatrices de la 5G.

1. Les entreprises utilisatrices 5G qui se sont vu accorder le droit d'utiliser le domaine radioélectrique public pour installer, déployer ou exploiter un réseau privé 5G, ou pour fournir des services 5G à des fins professionnelles ou à des fins propres, doivent analyser les risques des réseaux et services 5G, détecter les vulnérabilités et les menaces affectant les éléments du réseau, l'infrastructure, les ressources, les installations et les services qu'ils utilisent ou fournissent dans l'installation, le déploiement et l'exploitation de réseaux privés 5G ou dans la fourniture à des fins propres de services 5G.

2. Les entreprises utilisatrices de la 5G mentionnées dans la section précédente doivent fournir cette analyse de risque au ministère de la transformation numérique, sur demande.

Article 17. Confidentialité des informations relatives à l'analyse des risques.

1. Le ministère de la transformation numérique peut recueillir auprès des entités obligées les informations nécessaires à l'analyse des risques.

2. Les entités obligées doivent fournir les informations dans un délai de quinze jours ouvrables à compter du jour suivant la notification de la demande d'information.

3. Le non-respect des demandes d'information formulées conformément à la section précédente lorsqu'un mois s'est écoulé depuis la fin du délai de mise en conformité est qualifié d'infraction grave.

4. Les informations que les entités obligées fournissent sur l'analyse des risques sont considérées comme confidentielles et ne peuvent être utilisées à d'autres fins que la réalisation des objectifs et obligations établis dans le décret-loi royal 7/2022 du 29 mars 2022, dans le présent régime et dans les actes qui sont émis en application des deux dispositions.

## Chapitre V
## Gestion des risques par les entités obligées

### Article 18. Obligation de gérer les risques de sécurité.

Les entités obligées doivent prendre les mesures techniques et organisationnelles appropriées pour gérer les risques liés à l'installation, au déploiement et à l'exploitation des réseaux 5G et à la fourniture de services 5G, sur la base du décret-loi royal 7/2022 du 29 mars 2022, de ce régime et des actes qui sont adoptés en application des deux dispositions.

### Article 19. Gestion de la sécurité par les opérateurs 5G.

1. Les opérateurs 5G doivent assurer l'installation, le déploiement et l'exploitation sécurisés des réseaux publics 5G et la fourniture sécurisée de services 5G accessibles au public, en mettant en œuvre des techniques et des procédures d'exploitation et de surveillance pour assurer la sécurité des réseaux et services 5G, ainsi que le respect de la réglementation dans ce domaine.

2. Les opérateurs 5G ont les obligations de sécurité suivantes visant à atténuer les risques:

a) Adopter des mesures techniques et opérationnelles pour assurer l'intégrité physique et logique des réseaux 5G ou de l'un de leurs éléments, infrastructures et ressources, ainsi que la continuité de la fourniture des services 5G.
b) Adopter des plans d'urgence et des mesures spécifiques pour assurer la continuité d'autres services essentiels à la société qui dépendent des réseaux et services 5G.

c) Sélectionner et identifier les personnes qui peuvent accéder aux actifs physiques et logiques du réseau, et effectuer la maintenance des journaux d'accès.

d) Maintenir les identifiants d'utilisateur pour l'accès au réseau en possession de l'opérateur.

e) Utiliser uniquement des produits, ressources, services ou systèmes certifiés pour l'exploitation de réseaux 5G, ou n'importe quelle partie de ceux-ci.

   En particulier, le système GSMA Network Equipment Security Assurance Scheme (NESAS) s'applique.

f) Se conformer aux normes ou spécifications techniques applicables aux réseaux et aux systèmes d'information.

   En particulier, la norme technique ISO/IEC 27001 «Systèmes de management de la sécurité de l'information» s'applique.

g) Se conformer aux systèmes de certification européens pour les produits, services ou systèmes, spécifiques ou non à la technologie 5G, qui sont utilisés dans le fonctionnement des réseaux et services 5G.

h) Se soumettre, à leurs frais, à un audit de sécurité effectué par une entité publique ou une entité privée accréditée à cet effet.

   En particulier, les opérateurs 5G doivent soumettre chaque année au ministère de la transformation numérique un audit sur la mise en œuvre du système d'assurance de la sécurité des équipements de réseau GSMA (NESAS) et de la norme technique ISO/IEC 27001 «Systèmes de management de la sécurité de l'information».

i) Exiger les fournisseurs à respecter les normes de sécurité, de la conception des produits et services à leur mise en œuvre.

j) Contrôler leur propre chaîne d'approvisionnement et la stratégie de diversification qu'ils ont conçue.

3. En particulier, les opérateurs 5G qui possèdent ou exploitent des éléments critiques d'un réseau public 5G ont en outre les obligations supplémentaires suivantes:

a) Ils doivent concevoir une stratégie de diversification de la chaîne d'approvisionnement des équipements de télécommunications, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources permettant le transport de signaux dans un réseau public 5G, conformément aux dispositions de l'article 13.

b) Ils ne peuvent pas utiliser dans les éléments critiques du réseau des équipements de télécommunications, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources, permettant le transport de signaux, de matériel, de logiciels ou de services auxiliaires par des fournisseurs qui ont été classés comme présentant un risque élevé conformément aux dispositions de l'article 11.
c) Ils ne peuvent pas utiliser dans le réseau d'accès d'un réseau public 5G des équipements de télécommunications, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources, permettant le transport de signaux, de matériel, de logiciels ou de services auxiliaires par des fournisseurs classés comme présentant un risque élevé, dans les stations de radio qui assurent une couverture dans les lieux, zones et centres identifiés conformément aux dispositions de l'article 12.
d) Ils doivent implanter les éléments critiques d'un réseau public 5G sur le territoire national, sans préjudice des dispositions de l'article 5, paragraphe 4.

4. Les opérateurs 5G qui possèdent ou exploitent des éléments critiques d'un réseau public 5G doivent soumettre une nouvelle stratégie de diversification de la chaîne d'approvisionnement au ministère de la transformation numérique au plus tard le 1er octobre 2024.

En outre, la stratégie de diversification de la chaîne d'approvisionnement doit être soumise au ministère de la transformation numérique chaque fois qu'elle fait l'objet de modifications.

De même, les opérateurs 5G qui possèdent ou exploitent des éléments critiques d'un réseau public 5G doivent soumettre au ministère de la transformation numérique, au plus tard le 1er octobre de chaque année, des informations sur l'état de mise en œuvre de la stratégie de diversification de la chaîne d'approvisionnement.

5. Les opérateurs 5G doivent soumettre au ministère de la transformation numérique une description des mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques au plus tard le 1er octobre 2024 et tous les deux ans par la suite.

Article 20. Gestion de la sécurité par les fournisseurs de 5G.

1. Les fournisseurs de 5G doivent garantir la sécurité des équipements de télécommunications, du matériel, des logiciels ou des services auxiliaires qu'ils fournissent et qui sont utilisés par les réseaux et services 5G.

2. Les fournisseurs 5G ont les obligations de sécurité suivantes visant à atténuer les risques:

a) Respecter les normes de sécurité, de la conception des équipements, produits et services à leur mise en service.
   En particulier, la norme technique ISO/IEC 27001 «Systèmes de management de la sécurité de l'information» s'applique.
b) Renforcer l'intégrité logicielle, la mise à jour et la gestion des correctifs.
c) Accréditer la certification des produits et services informatiques utilisés dans les réseaux et services 5G.
   En particulier, le système GSMA Network Equipment Security Assurance Scheme (NESAS) s'applique.
d) Assurer la mise en œuvre de mesures de sécurité techniques et organisationnelles standard au moyen d'un système de certification.
e) Effectuer un audit de sécurité de leurs équipements, produits et services.
   En particulier, les fournisseurs 5G doivent soumettre chaque année au ministère de la transformation numérique un audit sur la mise en œuvre du système d'assurance de la sécurité des équipements réseau GSMA (NESAS) et de la norme technique ISO/IEC 27001 «Systèmes de management de la sécurité de l'information»
f) Fournir des informations sur d'éventuelles interférences de la part de tiers dans la conception, le fonctionnement et le fonctionnement de leurs équipements, produits et services.
g) Collaborer avec les opérateurs 5G et les entreprises utilisatrices de la 5G en fournissant des informations et en certifiant le respect des normes de sécurité des équipements, produits et services qu'ils fournissent.

3. Les fournisseurs 5G doivent fournir au ministère de la transformation numérique une description des mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques, sur demande.

4. Nonobstant les dispositions du paragraphe précédent, les fournisseurs 5G qui ont été classés comme à risque élevé ou à risque moyen doivent soumettre au ministère de la transformation numérique un rapport sur les mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques dans les six mois suivant la classification comme risque élevé ou risque moyen.

5. Tous les deux ans, les fournisseurs 5G à haut risque et à risque moyen doivent soumettre au ministère de la transformation numérique une description des mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques.

Article 21. Gestion de la sécurité par les entreprises utilisatrices de la 5G.

1. Les entreprises utilisatrices de la 5G qui ont obtenu le droit d'utiliser le domaine radioélectrique public pour installer, déployer ou exploiter un réseau privé 5G, ou pour fournir des services 5G à des fins professionnelles ou à des fins propres, doivent assurer l'installation, le déploiement et l'exploitation sécurisés de réseaux privés 5G et la fourniture à des fins propres sécurisée des services 5G, en mettant en œuvre des techniques et des procédures d'exploitation et de surveillance pour assurer la sécurité des réseaux et services 5G.

2. Les entreprises utilisatrices de la 5G susmentionnées ne peuvent pas utiliser dans les éléments critiques du réseau des équipements de télécommunications, des systèmes de transmission, des équipements de commutation ou d'acheminement et d'autres ressources, permettant le transport de signaux, de matériel, de logiciels ou de services auxiliaires par des fournisseurs classés comme présentant un risque moyen.

3. Les entreprises utilisatrices de la 5G susmentionnées doivent fournir au ministère de la transformation numérique une description des mesures techniques et organisationnelles conçues et mises en œuvre pour gérer et atténuer les risques, sur demande.

Article 22. Gestion de la sécurité par les administrations publiques.

1. Les administrations publiques adoptent des mesures techniques et organisationnelles appropriées pour gérer les risques liés à l'installation, au déploiement et à l'exploitation des réseaux 5G et à la fourniture de services 5G.

2. En particulier, les administrations publiques souhaitant réaliser l'installation, le déploiement et l'exploitation de réseaux 5G, publics ou privés, ou la fourniture de services 5G, qu'ils soient accessibles au public ou à des fins de fourniture propre, ne peuvent pas, pour des raisons de sécurité nationale, utiliser des équipements, des produits et des services fournis par des fournisseurs à haut risque ou à risque moyen.

Article 23. Conditions de respect des obligations.

Dans le respect des obligations prévues aux articles précédents, les entités obligées tiennent compte et appliquent ce qui est établi dans le décret-loi royal 7/2022 du 29 mars 2022, dans le présent régime et dans les actes qui sont adoptés en application des deux dispositions.

Article 24. Confidentialité des informations relatives à la gestion des risques.

1. Le ministère de la transformation numérique peut recueillir auprès des entités obligées les informations nécessaires à la gestion des risques.

2. Les entités obligées doivent fournir les informations dans un délai de quinze jours ouvrables à compter du jour suivant la notification de la demande d'information.

3. Le non-respect des demandes d'information formulées conformément à la section précédente lorsqu'un mois s'est écoulé depuis la fin du délai de mise en conformité est qualifié d'infraction grave.

4. Les informations que les entités obligées fournissent sur la gestion des risques sont considérées comme confidentielles et ne peuvent être utilisées à d'autres fins que la réalisation des objectifs et obligations établis dans le décret-loi royal 7/2022 du 29 mars 2022, dans le présent régime et dans les actes qui sont émis en application des deux dispositions.

## Chapitre VI
## Autres mesures de conformité pour la sécurité des réseaux et services 5G

### Article 25. Devoir de coopération dans la modification et la mise en œuvre de l'ENS5G.

Toutes les entités obligées, ainsi que les administrations publiques, les fabricants, les importateurs, les distributeurs et ceux qui mettent sur le marché et vendent des équipements et dispositifs terminaux pour se connecter à un réseau 5G et être en mesure de fournir des services 5G doivent coopérer et soumettre les informations nécessaires à la modification et à la mise en œuvre de l'ENS5G.

### Article 26. Certification des équipements et des produits.

Par ordre du ministre de la transformation numérique, l'utilisation d'un équipement, d'un système, d'un programme ou d'un service spécifique par des entités obligées peut être soumise à une certification préalable en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à la cybersécurité, ou au titre de systèmes de certification et de normes techniques pour la certification des équipements et produits 5G qui peuvent être approuvés au niveau européen ou international.

Article 27. Respect du droit des investissements étrangers et du droit de la concurrence.

Les obligations énoncées dans le décret-loi royal 7/2022 du 29 mars 2022, dans le présent régime et dans les actes qui sont adoptés en application des deux dispositions sont considérées comme sans préjudice de l'application des instruments de contrôle sur les investissements directs étrangers pour les parties assujetties de nationalité espagnole, ainsi que de l'application du droit de la concurrence.

Article 28. Équipements de terminaux de télécommunications.

La fabrication, l'importation, la distribution, la mise sur le marché et la vente d'équipements et de dispositifs terminaux pour se connecter à un réseau 5G et être en mesure de fournir des services 5G sont subordonnés au respect des exigences de sécurité applicables aux produits numériques et des exigences essentielles applicables en matière de cybersécurité, adoptées conformément à la législation européenne, notamment en ce qui concerne la protection des données à caractère personnel, la vie privée et la protection contre la fraude.

Article 29. Coopération internationale.

1. Le ministère de la transformation numérique coopère étroitement avec les institutions des autres États membres de l'Union européenne et avec les institutions de l'Union européenne dans la proposition de modification et de mise en œuvre du système national de sécurité des réseaux et services 5G et, en général, collabore avec les différentes organisations internationales spécialisées afin de pouvoir procéder à un traitement global et global de la sécurité des réseaux et services 5G.

2. En particulier, le ministère de la transformation numérique peut partager des informations relatives aux analyses effectuées par les institutions de l'Union européenne et avec d'autres États membres de l'Union européenne tout en préservant, comme l'exige la loi, la sécurité, les intérêts commerciaux et la confidentialité des informations recueillies lors de la préparation de l'analyse, et peut utiliser les informations qui lui sont transmises par d'autres États ou les institutions de l'Union européenne pour la mise en œuvre. Il peut également effectuer ces analyses conjointement avec d'autres États membres de l'Union européenne.

## Chapitre VII
## Mise en œuvre de l'ENS5G

### Article 30. Compétence pour la mise en œuvre de l'ENS5G.

1. Le ministère de la transformation numérique est le ministère responsable de la mise en œuvre de l'ENS5G et de l'exercice des autres fonctions qui lui sont conférées par le décret-loi royal 7/2022 du 29 mars 2022.

2. Le ministère de la transformation numérique assure la coordination avec les autres organismes chargés de la cybersécurité et des infrastructures critiques afin d'assurer la mise en œuvre cohérente de l'ENS5G.

### Article 31. Compétences pour la mise en œuvre de l'ENS5G.

Le ministère de la transformation numérique, dans l'exercice des fonctions qui lui sont confiées par le décret-loi royal 7/2022 du 29 mars 2022 et l'ENS5G, peut exercer, entre autres, les compétences suivantes:

a) Développer, préciser et détailler le contenu de l'ENS5G.

b) Autoriser l’installation, la modification ou l’adaptation de stations de radio qui assurent la couverture de certains lieux, zones et centres dans les conditions énoncées à l’article 12, paragraphe 4.
c) Formuler des demandes d’information aux entités obligées, auxquelles il convient de répondre dans un délai de quinze jours ouvrables à compter du jour suivant sa notification, afin de pouvoir exercer les fonctions qui lui sont assignées par le décret-loi royal 7/2022 du 29 mars 2022, l’ENS5G et leurs règlements d’application et, en particulier, de vérifier et de contrôler le respect des obligations respectives imposées aux entités obligées.
d) Effectuer des audits ou leur ordonner de vérifier et de contrôler le respect des obligations respectives que le décret-loi royal 7/2022 du 29 mars 2022, l’ENS5G et leurs règlements d’application imposent aux entités obligées.
e) Effectuer des inspections par des fonctionnaires affectés au Secrétariat d’État aux télécommunications et aux infrastructures numériques et exercer le pouvoir d’imposer des sanctions dans les conditions indiquées au chapitre suivant.
f) Accorder une aide publique.
g) Exercer ses autres fonctions en vertu de la législation applicable.

## Chapitre VIII
## Inspection et régime de sanction

### Article 32. Compétences en matière d’inspection.

Dans la mise en œuvre et le contrôle des dispositions du décret-loi royal 7/2022 du 29 mars 2022, de l’ENS5G et de leurs règlements d’application, le ministère de la transformation numérique exerce tous les pouvoirs de la fonction d’inspection prévue par lesdits règlements et par le titre VIII de la loi générale 11/2022 du 28 juin 2022 sur les télécommunications.

### Article 33. Régime de sanction.

Le régime de sanction prévu aux articles 30 et 31 du décret-loi royal 7/2022 du 29 mars 2022 s’applique.

ANNEXE I

Éléments, infrastructures et ressources qui composent un réseau 5G

1. Description de l'architecture du réseau 5G-SA.

Pour l'analyse requise dans ce système national de sécurité pour les réseaux et services 5G, une architecture de réseau de référence est utilisée, conformément à la recommandation du 3GPP et à la spécification ETSI TS 123 501.

La figure suivante montre un schéma simplifié d'une architecture 5G-SA pour les scénarios non itinérants (qui sera utilisé de manière générique comme base). Les éléments non indiqués dans la figure sont les suivants: UDR, UDSF, UCMF, CHF, 5G-EIR, NWDAF et SEPP.

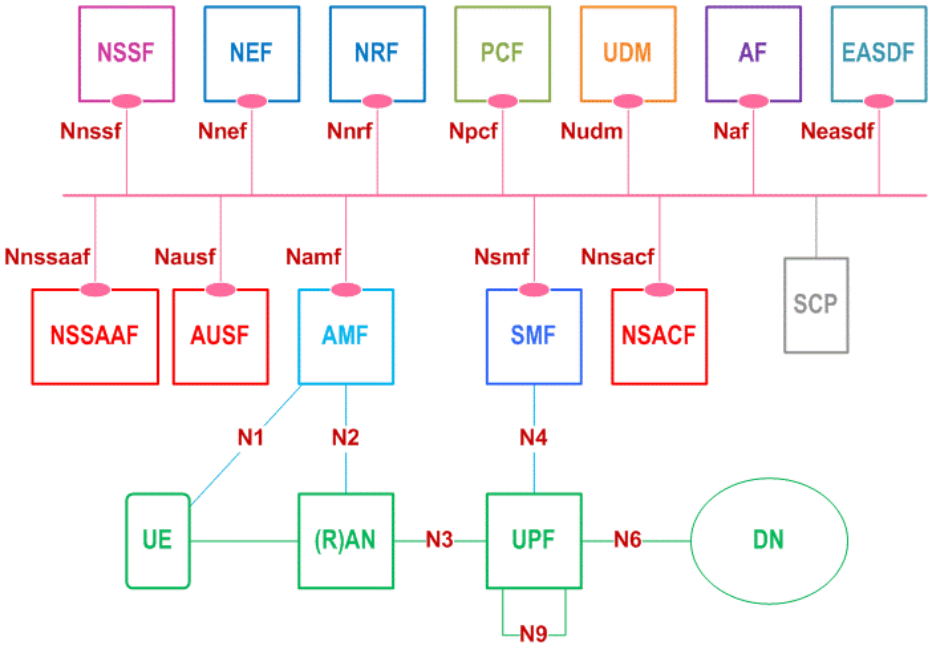



Figure 1: Architecture 5G selon la spécification ETSI TS 123 501

Ces éléments de réseau sont des fonctions logicielles qui sont déployées sur une infrastructure de virtualisation (elle-même composée de logiciels de virtualisation et de matériel), qui peuvent être dédiées et spécifiques à une fonction réseau, ou communes à plusieurs fonctions, y compris les fonctions réseau de plusieurs fournisseurs 5G. Dans ce scénario, l'infrastructure pour

héberger les fonctions réseau virtualisées peut être diversifiée à la fois géographiquement et par différents fournisseurs 5G, comme cela sera décrit plus loin dans le présent document.

En plus des éléments du réseau, un ensemble de systèmes pour l'exploitation et la gestion du réseau GER (également appelé OSS, Operations Support System) est déployé.

2. Identification et description des environnements réseau 5G-SA.

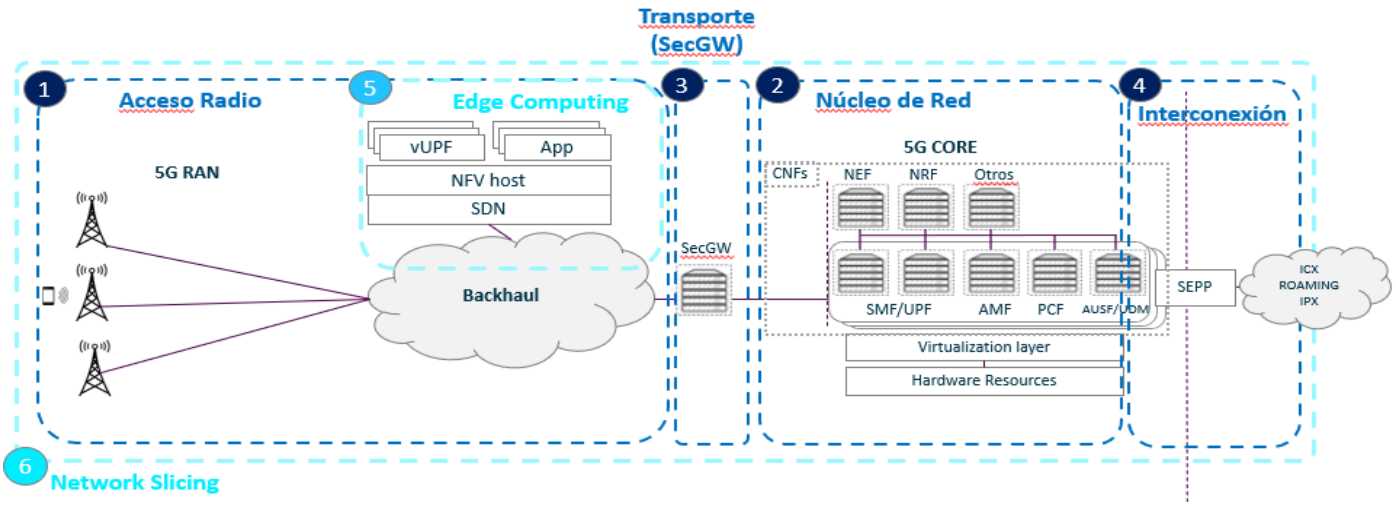
Afin de décomposer la complexité de l'architecture d'un réseau 5G-SA, il est divisé en environnements réseau.

Un environnement réseau est un ensemble d'actifs qui ont un rôle et des caractéristiques spécifiques au sein du réseau qui les différencient des autres environnements.

Deux types d'environnement peuvent être distingués:

a) Environnement primaire: Les environnements primaires sont considérés comme ceux qui sont spécifiques à la technologie ou à la nature de la 5G qui n'existeraient pas sans son déploiement.
b) Environnements secondaires: Les environnements secondaires sont considérés comme ceux qui sont communs chez un opérateur de télécommunications.

La figure suivante (figure 2) montre une classification du réseau 5G-SA par environnement:




| | |
|---|---|
| Acceso Radio | Accès radio |
| Transporte (SecGW) | Transport (SecGW) |
| Núcleo de Red | Cœur de réseau |
| Interconexión | Interconnexion |

3. Environnements réseau primaires.

Les environnements de réseau primaires comprennent l'accès radio, le réseau central, le transport-backhaul (SecGW), l'interconnexion d'itinérance et les systèmes de contrôle, de gestion et d'exploitation du réseau.

a) Accès radio: L'environnement d'accès radio (RAN) est responsable de la couverture des terminaux afin qu'ils puissent se connecter au réseau. On distingue les fonctions suivantes dans cet environnement:

i) Exploitation et maintenance du site radio. Le logiciel permet à chaque site d'être configuré avec un certain nombre de cellules par technologie pour pouvoir fournir un service aux utilisateurs et, pendant le fonctionnement de la station de base, surveille son état pour détecter d'éventuels problèmes ou défauts, dont l'apparition signalerait une alarme au système de gestion afin que l'opérateur soit conscient et résout le problème.

ii) Signalisation. Afin que les utilisateurs puissent s'inscrire sur le réseau et établir des services porteurs pour leurs communications, la signalisation est

nécessaire entre les terminaux, la station de base et le cœur du réseau, et une partie de ces fonctions est assurée par le logiciel de la station de base.

iii) Gestion des ressources radio. Les ressources radio d'une cellule donnée sont partagées entre différents utilisateurs et le logiciel de la station de base est responsable de les distribution entre ces utilisateurs (qualité de la liaison radio de chaque utilisateur, demande de vitesse, etc.). Le logiciel peut également répartir les utilisateurs entre les cellules de sa station de base (ou même avec les cellules des sites voisins), afin que la distribution des utilisateurs soit plus homogène entre les cellules voisines.

iv) Mobilité. Le logiciel de station de base gère le transfert des communications des utilisateurs entre différentes cellules, à partir de leur site ou de sites voisins, au fur et à mesure que les utilisateurs se déplacent à travers le réseau.

v) Transport. La communication physique avec le reste du réseau se fait au moyen de liaisons IP, électriques ou optiques, et la station de base doit être responsable de la gestion de ces liaisons (hiérarchisation entre les différents types de trafic passant par ces liaisons, configuration VLAN, suivi des liens, etc.).

Le réseau 5G, dans le réseau d'accès radio (RAN), est implémenté avec un seul type d'élément de réseau appelé génériquement gNodeB (gNB). La plupart des fournisseurs de réseaux d'accès radio 5G ont différents modèles gNB, adaptés à différents types de scénarios.

D'un point de vue général, il existe les types suivants:

i) Macro gNB: fournir une plus grande zone de couverture et une plus grande capacité de trafic. Ils sont généralement installés sur les toits de bâtiments ou de lieux à haute visibilité radio, dans le but de fournir une capacité et une couverture globales.

ii) Micro gNB: faible puissance, visant à fournir une couverture dans des endroits spécifiques, soit de petits espaces publics (tels que des places) ou

des espaces intérieurs (tels que les lieux d'événements, les petits bureaux, etc.), ou à fournir une capacité complémentaire à la couche générale ou macro. Ils sont installés principalement aux points de forte demande de capacité, pour absorber cette demande.

iii) Systèmes gNB intérieurs: spécialisé dans la couverture de grands espaces intérieurs, avec de nombreux points de rayonnement de faible puissance, pour distribuer la couverture 5G à travers ledit espace intérieur. Ils sont généralement installés dans de grands immeubles de bureaux, des stades sportifs, des métros, etc.

Dans ce contexte, un site réseau d'accès radio 5G se composera d'une bande de base et de plusieurs têtes distantes et/ou antennes actives. Le nombre de têtes éloignées et d'antennes actives dépendra du nombre de bandes présentes sur le site et du nombre de secteurs.

Le logiciel gNB est commun à la bande de base, aux têtes distantes et aux antennes actives, et est également commun parmi les différents systèmes de communications mobiles présents sur le site (2G, 3G, 4G et/ou 5G). La station de base communique avec le cœur du réseau via l'interface NG et avec les terminaux mobiles via l'interface aérienne.

b) Cœur de réseau: Le cœur du réseau 5G-SA se compose d'un certain nombre de fonctions réseau standardisées 3GPP qui communiquent entre elles par des connexions SBI (Service Based Interfaces), permettant un maillage complet en fonction des besoins de chacune d'entre elles.

Les principes clés de cette architecture 5G-SA sont les suivants:

i) Séparer les fonctions de plan utilisateur (UP) des fonctions de plan de contrôle (CP), permettant une extensibilité indépendante, l'évolution et des implémentations flexibles, par exemple emplacement centralisé ou un emplacement distribué (à distance).

ii) Modulariser la conception de la fonction, par exemple pour permettre un tranchage de réseau flexible et efficace.

iii) Permettre à chaque fonction réseau (et ses services associés) d'interagir avec d'autres fonctions réseau, directement ou indirectement via un proxy.

iv) Intégrer différents types d'accès, par exemple l'accès 3GPP et l'accès non-3GPP.

v) Permettre un cadre d'authentification unifié.

vi) Découpler dans les fonctions réseau les fonctions logiques sans état liées à la capacité de calcul des fonctions d'état liées aux capacités de stockage.

vii) Permettre l'exposition des données du réseau de manière sécurisée pour le développement de nouveaux services basés sur les données.

viii) Permettre l'accès simultané aux services locaux (à faible latence) et aux services centralisés.

ix) Autoriser et accepter le trafic en itinérance avec d'autres réseaux, selon différents modèles d'architecture.

L'ensemble des fonctions centrales du réseau définies par 3GPP est le suivant:

i. AMF – Access and Mobility Management Function: la fonction de plan de contrôle de réseau 5G. Ses principales fonctions sont la gestion de l'enregistrement, la gestion de la mobilité, la gestion des connexions et la gestion de divers aspects liés à la sécurité et à l'autorisation d'accès.

ii. SMF — Session Management Function: la fonction de plan de contrôle qui est responsable de la gestion des sessions (établissement, modification et version), de la gestion et de l'attribution des IP aux terminaux utilisateurs. En résumé, cette fonction est responsable de l'interaction avec le plan utilisateur en créant, en mettant à jour ou en supprimant des sessions PDU, tout en gérant le contexte de la session avec l'UPF.

iii. UPF — User Plane Function: cette fonction est responsable du transfert de paquets, du routage et de l'inspection, ainsi que de la gestion de la qualité du service. Elle représente le point d'interconnexion au réseau de données.

iv. PFC — Policy Control Function: cette fonction est chargés de fournir des règles de politique pour contrôler les fonctions de réseau du plan de contrôle, y compris le découpage du réseau, l'itinérance, la gestion de la mobilité et les politiques de

qualité de service 5G. Pour la mise en œuvre des politiques, elle accède aux informations d'abonnement UDR.

v. NRF — Network Repository Function: cette fonction est responsable de la découverte du service, et maintient le profil et les instances réseau disponibles. Ses principales fonctions sont la gestion des services, la découverte de service et les jetons d'accès, permettant à deux éléments de réseau 5G de communiquer.

vi. SEPP — Security Edge Protection Proxy: la fonction réseau qui permet une interconnexion sécurisée entre les réseaux 5G, garantissant la confidentialité de bout en bout et/ou l'intégrité entre le réseau source et le réseau de destination, pour tous les messages d'itinérance d'interconnexion 5G.

vii. UDM — Unified Data Management: fonction de plan de contrôle dont les principales missions sont la génération d'identifiants d'authentification, la gestion de l'identité de l'utilisateur, la gestion des abonnements, l'autorisation d'accès basée sur les données d'abonnement, et le stockage et la gestion des fonctions réseau qui servent l'utilisateur. L'UDM utilise les données d'abonnement stockées dans l'UDR.

viii. UDR — Unified Data Repository: répertoire unifié des données utilisateur. Ces données sont structurées en différentes catégories ou types, et sont accessibles aux différentes fonctions du réseau grâce à une série de services exposés pour leur gestion et leur consultation (par exemple UDM, PCR, NRF, etc.).

ix. AUSF – Authentication Server Function: la fonction de plan de contrôle du réseau 5G qui est responsable de l'authentification de l'utilisateur.

x. CHF — Charging Function: la fonctionnalité de charge se trouve dans le système de charge convergent (CCS), qui offre des fonctionnalités de charge en ligne et hors ligne. Ses fonctions comprennent l'OCF (Online Charging Function) pour effectuer le contrôle en ligne des sessions de données, le CDF (Charging Data Function) pour construire un CDR avec les informations de réseau reçues, l'ABMF (Account Balance Management Function) pour la gestion de l'équilibre et les contrôles de consommation, le RF (Rating Function) pour fixer un prix pour l'utilisation reçue (en ligne et hors ligne) et le CGF (Charging Gateway Function) pour générer des CDR tarifiés.

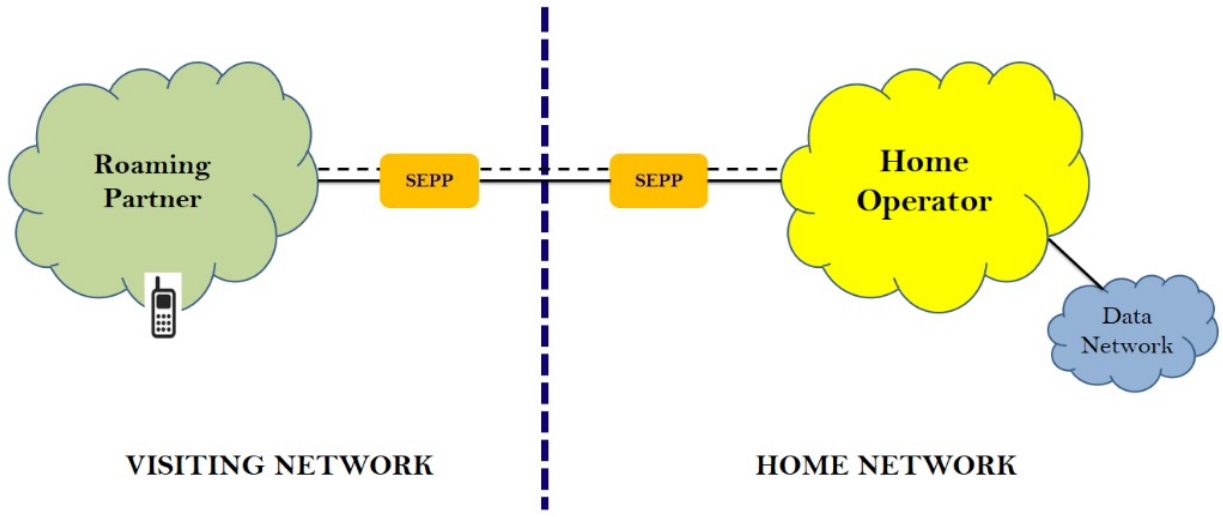
xi. NEF — Network Exposure Function: cette fonction fournit un moyen d'exposer en toute sécurité les services et les capacités offerts par les fonctions réseau 5G.

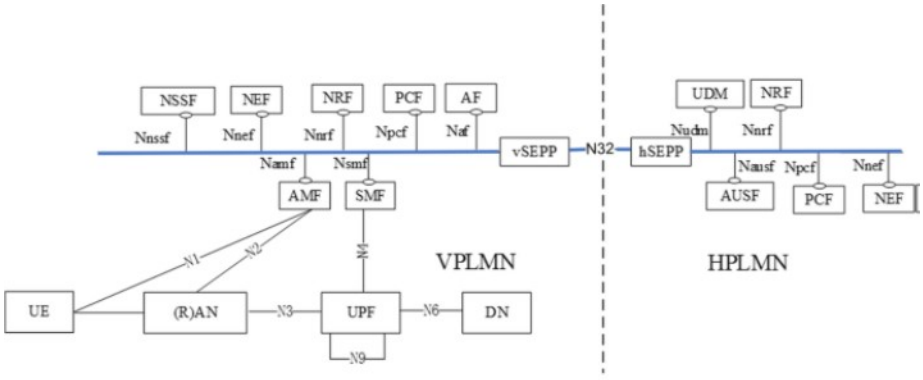
xii. 5G-EIR — 5G-Equipment Identity Register: une fonctionnalité optionnelle qui offre la possibilité de vérifier l'état de l'identité du terminal (IMEI) et de vérifier qu'il n'est pas sur liste noire.

c) Transport-Backhaul (SecGW): La fonction Security Gateway (SecGW) fournit le chiffrement du plan de contrôle et du trafic du plan utilisateur entre les environnements Radio Access et Network Core, tout en évitant l'exposition inutile des éléments critiques.

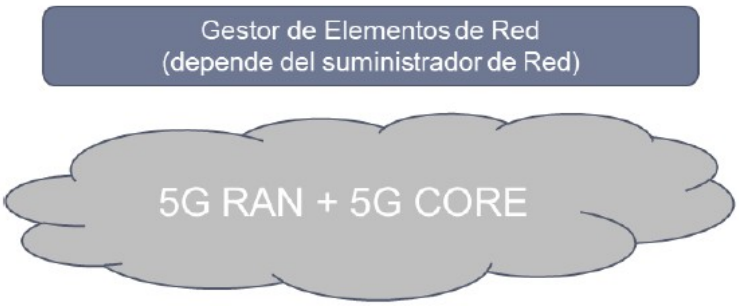
d) Interconnexion en itinérance: L'environnement d'interconnexion en itinérance est nécessaire pour la communication avec d'autres opérateurs afin de permettre à un utilisateur 5G de se déplacer à l'international sans interrompre son service vocal ou haut débit.

La figure suivante (figure 3) présente la représentation d'un environnement d'interconnexion en itinérance:






e) Systèmes de contrôle, de gestion et d'exploitation et services de soutien: Le processus d'assurance du cœur du réseau 5G est pris en charge par un ensemble de systèmes de soutien à l'exploitation (OSS) illustrés dans la figure ci-dessous (figure 4).




| | |
|---|---|
| Gestor de Elementos de Red (depende del suministrador de Red) | Gestionnaire des éléments du réseau (dépend du fournisseur de réseau) |

Ces systèmes OSS ne font pas partie de la prestation de services et, par conséquent, les défaillances dans leur fonctionnement n'affectent pas directement la disponibilité du réseau ou la qualité du service fourni sur celui-ci. Toutefois, l'indisponibilité de ces systèmes affecterait la capacité de surveillance, d'analyse, de configuration et de planification du réseau décrite au point précédent. Du point de vue de la sécurité, ces systèmes de gestion sont segmentés en fonction du fournisseur et donc un incident de sécurité dans l'un d'entre eux n'affecterait pas les fonctions réseau qui ne sont pas couvertes par cet OSS.

4. Environnements réseau secondaires.

Les environnements réseau secondaires comprennent les plates-formes de virtualisation, l'infrastructure physique, l'Edge Computing et le Network Slicing.

a) Plateformes de virtualisation et d'orchestration: Bon nombre des éléments d'un réseau 5G sont des fonctions «logicielles» déployées sur une infrastructure de virtualisation (elle-même composée de logiciels et de matériel de virtualisation), qui peuvent être dédiées et spécifiques à une fonction réseau, ou communes à plusieurs fonctions (y compris les fonctions réseau de plusieurs fournisseurs). Dans ce contexte, l'infrastructure permettant d'héberger les fonctions du réseau virtualisé est diversifiée à la fois géographiquement et par différents fournisseurs.

b) Infrastructure physique: Les éléments de réseau et les fonctions appartenant aux différents environnements nécessitent une infrastructure physique où les placer, dont la nature, la disponibilité et la sécurité dépendront évidemment du caractère critique de l'actif spécifique. Cette infrastructure physique fournit aux éléments et aux fonctions du réseau les besoins de base pour un bon fonctionnement.

c) Multi-Access Edge Computing (MEC): L'informatique de périphérie multiaccès est un type d'architecture ou d'environnement de réseau qui vise à amener les fonctions de traitement du trafic utilisateur et de cloud computing informatique à la périphérie du réseau afin d'assurer le fonctionnement de nouveaux cas d'utilisation nécessitant une latence minimale.

Dans son concept, il est défini en termes plus larges comme une évolution de l'informatique en nuage qui utilise les technologies mobiles et cloud pour séparer les hôtes d'applications du centre de données où ils se trouvent et les déplacer à la périphérie du réseau. Cela permet non seulement aux utilisateurs finaux d'être plus proches des applications, mais aussi aux services informatiques d'être plus proches des données qu'ils génèrent.

Dans ce Edge Computing, les applications tierces et les fonctions réseau pour traiter le trafic utilisateur à la périphérie coexistent.

d) Network Slicing: Il s’agit d’une forme d’architecture qui offre la possibilité de créer, sur une infrastructure commune de virtualisation physique partagée, plusieurs réseaux virtuels personnalisés et logiquement isolés les uns des autres, donnant à chacun d’eux un caractère critique spécifique en fonction des besoins spécifiques des applications, des services, des appareils, des clients ou des opérateurs.

Il est prévu qu’avec cette technologie, les opérateurs de réseau et de services 5G peuvent implémenter la segmentation du réseau pour créer plusieurs réseaux virtuels avec différentes tailles de connectivité, en s’adaptant aux besoins de connexion des différents utilisateurs, en allouant spécifiquement les ressources nécessaires pour assurer le bon service.

En général, dans le concept de network slicing, chaque réseau virtuel (ou partie du réseau) englobe un ensemble indépendant de fonctions logiques réseau qui prennent en charge les exigences du cas d’utilisation particulier. Chacun d’entre eux sera optimisé pour fournir les ressources réseau et le raisonnement mathématique pour le service et le trafic qui seront utilisés dans la segmentation.

Dans le cas de la technologie 5G-SA, la capacité, la connectivité, la variété, la vitesse, la couverture et la sécurité seront allouées pour répondre aux exigences spécifiques de chaque cas d’utilisation.

ANNEXE II

ANALYSE DES RISQUES AU NIVEAU NATIONAL

1. Méthodologie utilisée.

Une analyse des risques vise à identifier et catégoriser les principales menaces pour les réseaux et services 5G, afin de déterminer les mesures correctives qui peuvent réduire leurs conséquences voire les prévenir.

Connaissant cet objectif, la prochaine étape logique consiste à établir les moyens d'atteindre cet objectif. Une analyse des risques doit être effectuée en utilisant une méthodologie standardisée et globale et dans un ordre cohérent et logique, détaillant chacun des aspects qualitativement et quantitativement. Dans le cas contraire, le niveau de risque calculé pourrait être faussé et, avec lui, les critères et les priorités des mesures de protection et/ou des actions clés à mener.

Les étapes suivies pour l'analyse effectuée sont présentées ci-dessous, ainsi que les sources d'information utilisées pour la méthodologie utilisée.

1) Identification et description de l'architecture 5G, des environnements de réseau existants au sein de celle-ci et des actifs qui la composent, tous soumis à l'évolution technologique (voir annexe I).
2) Identification du caractère critique pour les actifs: afin d'identifier l'impact d'une menace sur le réseau, il est nécessaire de déterminer d'abord le caractère critique de chacun des actifs, en fonction des trois principaux axes de sécurité (**CIA**: *Confidentialité*, *Intégrité* et *Disponibilité*).
3) Identification des risques technologiques 5G et de leur impact sur les actifs identifiés: déterminer les menaces potentielles présentes dans cet environnement spécifique, les classer par actif et identifier leur niveau de risque.
4) Identification des mesures de sécurité techniques, organisationnelles et stratégiques pour atténuer ou réduire le niveau de risque des menaces identifiées pour chaque environnement de réseau. L'efficacité sera directement

proportionnelle au degré de diminution du niveau de risque pour une menace et un actif donnés.

5) Gestion des risques et des risques restants, dans les menaces dont le niveau est considérable et ne peut être réduit par aucune mesure supplémentaire dès la conception (voir annexe III).

2. Facteurs qui affectent le caractère critique d'un actif.

De manière standardisée et largement reconnue, trois facteurs ou concepts clés sont pris en compte lors de l'évaluation du caractère critique des actifs d'un scénario donné, lors de l'évaluation de la sécurité d'une solution est ce qui s'applique.

Les trois principaux facteurs ou concepts sont la confidentialité, l'intégrité et la disponibilité (pour *Confidentiality, Integrity & Availability* ou «CIA» en anglais).

a) Confidentialité: La confidentialité d'un actif ou d'un réseau implique d'évaluer la capacité d'empêcher les informations contenues dans l'actif, ou en transit sur le réseau, d'être exposées à des utilisateurs non autorisés, qui ne devraient pas y avoir accès. Les mesures de sécurité pour assurer la confidentialité sont diverses, allant de la segmentation et du contrôle d'accès au cryptage robuste des informations. Le principal facteur lors de l'évaluation de l'importance de la confidentialité dans un actif est la sensibilité de l'information qu'il stocke ou qui transite par celui-ci. Lors de la prise en compte de ce facteur, il est important de prendre en compte l'impact que la compromission de l'actif peut avoir sur le reste du réseau.

   Voici des exemples de risques susceptibles de compromettre la confidentialité: Espionnage/interception du trafic utilisateur/des données sur le réseau (Man-in-the-Middle/Eavesdropping), ou obtention d'informations d'identification de l'opérateur, soit en raison d'une mauvaise configuration du réseau, de l'absence de stratégie de segmentation et de contrôle d'accès, ou, par exemple, de l'absence de cryptage dans les interfaces très exposées.

b) Intégrité: L'intégrité est la capacité de s'assurer que les données d'un actif/utilisateur/réseau pendant son cycle de vie, qu'elles soient en transit ou en stockage, conservent leur authenticité et ne soient modifiées que par les agents autorisés à le faire, empêchant les sources indésirables de modifier ou de manipuler ces données. Les mesures visant à assurer l'intégrité peuvent inclure la segmentation et le contrôle d'accès, la vérification du hachage dans les paquets, la vérification de l'intégrité des versions à installer ou à stocker, etc.

   Voici des exemples de risques qui compromettent l'intégrité: Manipulation du trafic/des données (en transit ou stockées) sur des interfaces réseau 5G hautement exposées.

c) Disponibilité: La disponibilité est fondée sur le principe de veiller à ce que les utilisateurs légitimes aient un accès ininterrompu aux services et aux données dans l'environnement pour un bon fonctionnement. Ce concept vise à juger de l'importance de l'actif et de sa solution dans la continuité des activités d'un service, d'une ressource ou d'une infrastructure particulière. Le niveau d'impact sur la disponibilité d'un risque dépend généralement du nombre et du type d'utilisateurs affectés par le temps d'interruption du service causé par l'attaque.

   Pour assurer la disponibilité, diverses mesures peuvent être prises, y compris la création de solutions de sauvegarde, la redondance/résilience des actifs, la capacité d'atténuer les attaques DDoS et des procédures de restauration de service efficaces après les temps d'arrêt.

   Dans l'environnement, certains risques susceptibles de compromettre la disponibilité sont les suivants: Attaques telles que, par exemple, le déni de service de la fonction réseau, de l'infrastructure de virtualisation ou de l'infrastructure physique, ou les catastrophes naturelles, le terrorisme, etc.

3. Détermination du caractère critique des actifs.

Dans cette section, le caractère critique des actifs du réseau 5G-SA identifiés est identifiée, en tenant compte des facteurs et concepts clés (de la triade CIA) décrits au point précédent.

## a) Réseau d'accès.

- **gNB**: Criticité moyenne

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Red de acceso | Réseau d'accès |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| 2-Media | 2-Media |

Les nœuds d'accès radio se trouvent, pour la plupart, sur des sites situés dans des lieux publics non sécurisés. Cela augmente leur exposition aux attaques sur site. L'impact sur une cellule peut signifier l'interruption du service dans une zone limitée, affectant un petit nombre d'utilisateurs, et son trafic peut être soutenu par une autre station de base à proximité. Par conséquent, la criticité est considérée comme étant **faible** en ce qui concerne la **disponibilité**.

Ces nœuds ne stockent pas les données des utilisateurs. Malgré cela, si une attaque *Man-in-the-Middle* (*MITM*) se produit, le trafic non crypté pourrait être compromis (affectant seulement les quelques utilisateurs

connectés à ce nœud), ainsi que la possibilité de manipuler les paquets en cours s'il n'y a pas de contrôle d'intégrité. En raison de la difficulté de mener cette attaque dans le scénario décrit, la **confidentialité** et l'**intégrité** se voient attribuée une criticité **moyenne**.

**b) Cœur de réseau.**

- **AUSF, UDM et UDR:** Criticité élevée

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Núcleo de red | Cœur de réseau |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Alta | Élevée |

Une atteinte à la confidentialité/à l'intégrité de ces actifs peut impliquer l'exposition d'informations critiques de l'utilisateur sur le réseau (authentification, intégrité et clés de chiffrement, données de d'accès des utilisateurs et leurs identités, etc.).

L'obtention de ces informations aurait un impact très élevé parce qu'il s'agit d'informations directement associées aux cartes SIM des clients, et leur diffusion peut conduire non seulement à une exposition des communications des utilisateurs, mais aussi à une perte d'image pour le réseau 5G et l'opérateur de service, et peut impliquer le remplacement

des cartes SIM corrompues. Pour ces raisons, la criticité de l'actif en termes de **confidentialité** et d'**intégrité** est **élevée**.

En outre, étant un élément centralisé qui reçoit des demandes d'authentification de tous les utilisateurs du réseau, dans le cas où il n'est pas déployé avec une solution correcte qui garantit sa résilience et sa continuité d'activité, une perturbation de celui-ci peut provoquer un effondrement complet du réseau. Par conséquent, en ce qui concerne la **disponibilité**, sa criticité est elle aussi **élevée**.

- **AMF**, **NRF** et **NEF**: Criticité moyenne

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Núcleo de red | Cœur de réseau |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Alta | Élevée |
| Media | Moyenne |
| Baja | Faible |

  - **NRF**: Criticité moyenne

    Cet élément dispose d'une carte de l'ensemble du réseau, des nœuds et des services. L'accès non autorisé peut donner des détails sur le déploiement du réseau, le routage, les DNN, les tranches, les services, etc. En outre, la modification de la configuration peut entraîner des erreurs de communication internes

dans le réseau. Pour ces raisons, la **confidentialité** et l'**intégrité** du NRF sont considérés comme ayant une criticité **élevée**.
Cependant, le fait que le service puisse être configuré de sorte que, en cas de défaillance de l'élément, il existe une continuité temporaire du service entre les fonctions réseau signifie que sa **criticité** en ce qui concerne la disponibilité est **faible**.

- **AMF**: Criticité moyenne
  En étant en charge de la gestion de la mobilité des utilisateurs, une attaque ou un accès non autorisé peut permettre d'obtenir ou de diffuser des informations sensibles (identités de l'utilisateur, localisation au niveau de la zone de suivi, et même l'identifiant du nœud où se trouve le client lorsque le terminal est connecté).

  Pour cette raison, pour les risques de diffusion plutôt que pour l'altération de l'information, la criticité est considérée comme étant **élevée** en ce qui concerne la **confidentialité** et **moyenne** en ce qui concerne l'**intégrité**.

  D'autre part, puisqu'il ne sert qu'une partie des utilisateurs du réseau, la criticité en termes de **disponibilité** est considérée comme étant **moyenne**.

- **NEF**: Criticité moyenne/faible
  Cet élément est chargé d'assurer l'authentification, la confidentialité et l'intégrité des communications provenant d'entités externes au cœur du réseau, contre l'une quelconque des fonctions internes du cœur de réseau (interface *SBI*). L'accès non autorisé peut permettre la modification d'une politique de sécurité entre les fonctions externes au cœur du réseau et les fonctions internes. Cependant, cette fonction réseau n'est pas utilisée pour la fourniture de services généraux aux utilisateurs de la 5G. Pour

cette raison, la **confidentialité** et l'**intégrité** sont considérées comme étant de criticité **moyenne**.

En ce qui concerne la **disponibilité**, la défaillance de cet équipement, en l'absence de redondance, n'affecterait que les services qui ont besoin d'une communication externe avec les éléments du cœur du réseau, ce qui n'aurait pas d'impact considérable et c'est pourquoi il est considéré comme ayant une criticité **faible**.

- **SMF/UPF** et **PCF**: Criticité faible

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Núcleo de red | Cœur de réseau |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Baja | Faible |

Dans cette catégorie, les éléments suivants sont regroupés, dans lesquels, en général, un impact sur eux n'a pas d'incidence notable sur la fourniture du service 5G. Par conséquent, leur criticité est évaluée comme étant faible.

- **SMF/UPF**: Criticité faible

  Le SMF est responsable de l'établissement des sessions, et l'UPF est responsable de la gestion de l'avion utilisateur: il décapsule le

trafic utilisateur provenant de l'accès radio et l'achemine vers d'autres réseaux de données. L'accès non autorisé peut désactiver la session d'un utilisateur, mais il serait établi dans un autre SMF/UPF. En outre, l'utilisation du SecGW entre le réseau d'accès et le cœur du réseau rend une attaque *MITM* impossible, ce qui signifie que sa criticité en termes de **confidentialité** et d'**intégrité** est **faible**.

En outre, en termes de **disponibilité**, sa criticité est également considérée comme étant **faible**, étant donné qu'un utilisateur ne peut se trouver que dans un seul AMF, mais que ses sessions peuvent se trouver dans divers SMF/UPF.

- **PCF**: Criticité faible

  Cet élément n'est pas particulièrement critique pour les services de données. Bien qu'il existe des politiques relatives aux services et aux prix, les AMF/SMF sont toujours configurés pour pouvoir fournir un service sans cet élément. Un effet normal de la défaillance PCF dans le service de données n'est pas en mesure de facturer les clients en ligne. L'impact possible sur le service vocal peut être atténué par le service vocal 2G/3G. Pour ces raisons, la criticité de ses **différents critères** est considérée comme étant **faible**.

### c) Transport-Backhaul.

- **SecGW**: Criticité moyenne

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |

| | |
|---|---|
| Primario | Primaire |
| Transporte - Backhaul | Transport-Backhaul |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Media | Moyenne |

Le réseau de transport relie les éléments du noyau à ceux du réseau d'accès. Une éventuelle panne dans l'une de ses sections signifie que seule la zone des nœuds d'accès radio dans lequel une telle panne se produit est affectée et, temporairement, il est possible de forcer le trafic afin qu'il ne passe pas par cet élément dans ladite zone. Par conséquent, en ce qui concerne la **disponibilité**, la criticité est **moyenne**.

D'autre part, le fait de compromettre un site ou d'intercepter du trafic entraîne une fuite importante d'informations, car il s'agit de l'élément chargé de chiffrer les informations en transit qui arrivent à partir d'un grand nombre de nœuds. Pour cette raison, en ce qui concerne la **confidentialité**, il se voit attribuer une criticité **élevée**. Comme cette communication est cryptée, la modifier est compliqué. Par conséquent, la criticité en termes d'**intégrité** est considérée comme étant **moyenne**.

**d) Interconnexion en itinérance.**

- **SEPP**: Criticité moyenne

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |

| | |
|---|---|
| Primario | Primaire |
| Interconexión Roaming | Interconnexion en itinérance |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Alta | Élevée |
| Media | Moyenne |
| Baja | Faible |

Cet élément permet l'échange de signalisation avec d'autres réseaux dans des scénarios d'itinérance. Bien qu'il s'agisse d'un élément exposé à d'autres réseaux, il ne transporte que le trafic d'utilisateurs itinérants, et non celui des utilisateurs nationaux. Cela signifie que la criticité en ce qui concerne la **disponibilité** est **moyenne**.

D'autre part, la confidentialité des communications et leur intégrité sont des aspects importants (en particulier les premiers), puisqu'il s'agit d'un environnement dans lequel, en l'absence de protections adéquates, des informations sensibles peuvent être obtenues ou diffusée auprès des utilisateurs, même ceux qui ne sont pas en itinérance. Cela signifie que la criticité en ce qui concerne la **confidentialité** est **élevée**.

C'est un environnement que l'industrie et les organismes de normalisation ont pris très au sérieux, dans lequel, à la base, les fabricants vont inclure des capacités de cryptage et de configuration d'intégrité. Cela signifie que, si le trafic est crypté, attaquer l'**intégrité** est plus compliqué. Pour toutes ces raisons, sa criticité est **moyenne**.

**e) Systèmes de contrôle et de gestion et services de soutien.**

- **GER**: Criticité moyenne

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Sistemas de gestión/operación y servicios de soporte | Systèmes de contrôle et de gestion et services de soutien |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Alta | Élevée |
| Media | Moyenne |
| Baja | Faible |

Ces éléments permettent le bon fonctionnement des éléments qui composent l'environnement réseau 5G. Ils peuvent gérer tout un environnement réseau, échanger des messages de configuration qui peuvent donner des commandes frauduleuses à l'équipement, ou même transporter des informations d'identification.

Par conséquent, la criticité de l'**intégrité** et de la **confidentialité** de cet élément est considérée comme étant **élevée**.

Cependant, une interruption ou un manque de communication avec le réseau par les systèmes de gestion ne conduit pas à une défaillance du réseau, et la criticité en ce qui concerne la **disponibilité** est considéré comme étant **faible**.

**f) Infrastructure de virtualisation/d'orchestration.**

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Infraestructura de virtualización/orquestación | Infrastructure de virtualisation/d'orchestration |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Alta | Élevée |
| Media | Moyenne |
| Baja | Faible |

- **Infrastructure de virtualisation**: Criticité élevée

  Tous les éléments du cœur de réseau 5G sont déployés sur une infrastructure virtualisée. Cela signifie que toute attaque qui parvient à perturber son fonctionnement, à contrôler ses nœuds, à intercepter le trafic, à modifier son fonctionnement, etc. peut avoir de graves conséquences sur la fourniture du service, pouvant même conduire à son interruption totale. Pour les raisons exposées, la criticité en ce qui concerne la **confidentialité**, l'**intégrité** et la **disponibilité** est **élevée** et cela est considéré comme un atout essentiel au sein du réseau.

- **Gestion/orchestration de la virtualisation**: Criticité moyenne

  De la même manière que les systèmes de gestion/d'opération et les services de soutien, les aspects les plus critiques de cet atout sont les suivants: **confidentialité** et **intégrité** des communications et de l'accès, dont la criticité est considérée comme **élevée**. C'est parce que les *orchestrateurs de virtualisation* contrôlent tous les éléments de la plate-

forme de virtualisation, qui pourrait être violée ou attaquée (par exemple, suppression de *CNFS,* arrêt du matériel, etc.).

Cependant, une interruption ou un manque de communication avec le réseau par l'orchestration ne provoque pas de défaillance dans les plates-formes de virtualisation, et la criticité en ce qui concerne la **disponibilité** est considéré comme étant **faible**.

### g) Infrastructure physique.

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Infraestructura Física | Infrastructure physique |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Alta | Élevée |
| Media | Moyenne |
| Baja | Faible |

- **Infrastructure physique**: Criticité moyenne

  L'infrastructure physique est particulièrement vulnérable aux attaques qui causent des dommages physiques à l'équipement, au vol, aux pannes de courant, etc. Cette disponibilité est fondamentale pour le fonctionnement des réseaux et des services, car elle servira de base à de nombreuses fonctions réseau et systèmes de gestion sur l'ensemble du réseau. Par conséquent, la criticité, en termes de **disponibilité**, est **élevée**.

Le **confidentialité** et l'**intégrité** de cet actif sont considérées comme ayant une criticité **faible**, puisqu'il ne représente pas un risque pour l'information ou la communication elle-même, en fonction principalement des protocoles et des mécanismes de contrôle logique mis en œuvre dans les couches supérieures (infrastructure de virtualisation, applications, etc.) afin d'empêcher l'obtention d'informations si quelqu'un obtient un actif.

**Tableau récapitulatif: Tableau de criticité des actifs**

| 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 de l'actif |
| Entorno de red | Environnement réseau |
| Dominio | Domaine |
| Activo | Actif |
| Primario | Primaire |
| Secundario | Secondaire |
| Infraestructura Física | Infrastructure physique |
| Red de acceso | Réseau d'accès |
| Núcleo de red | Cœur de réseau |
| Transporte - Backhaul | Transport-Backhaul |
| Interconexión Roaming | Interconnexion en itinérance |
| Sistemas de gestión/operación y servicios de | Systèmes de contrôle et de gestion et services de |

| | |
|---|---|
| soporte | soutien |
| Infraestructura de virtualización/orquestación | Infrastructure de virtualisation/d'orchestration |
| Evaluación CIA | Évaluation de la triade CIA |
| Criticidad | Criticité |
| Alta | Élevée |
| Media | Moyenne |
| Baja | Faible |

4. Classification des actifs en fonction de leur criticité.

Sur la base des analyses précédentes et des contributions des opérateurs de réseau et de services 5G, un ensemble d'éléments a été identifié comme étant d'une importance critique pour le fonctionnement des réseaux 5G, pour leur configuration ou leur gestion, ou pour les services qu'ils fournissent.

Comme indiqué au point précédent, tous les actifs de haute criticité dans l'environnement de réseau principal appartiennent au cœur du réseau. Cependant, du point de vue de la criticité, il n'est pas possible de considérer le cœur du réseau comme un bloc homogène. Par conséquent, un traitement différencié est considéré comme applicable en ce qui concerne les mesures visant à garantir la disponibilité des services qu'ils offrent.

Ainsi, le cœur de réseau est composé de diverses fonctions réseau (NF) qui sont déployées dans des infrastructures virtualisées indépendantes de la fonction réseau elle-même. La classification considère lesquelles de ces entités sont les plus critiques non seulement du point de vue de la redondance, mais aussi de l'impact possible d'un accès non autorisé ou d'attaques provenant d'autres réseaux.

En outre, il prend en compte l'accès non autorisé possible à l'infrastructure virtualisée sur laquelle ces fonctions réseau sont déployées, et établit une importance relative entre les différentes entités, en soulignant que, pour obtenir un service complet, toutes sont nécessaires.

a) Criticité élevée

Le risque qui compromettrait le plus le service 5G serait l'accès non autorisé à l'environnement AUSF/UDM/UDR. L'AUSF dispose des clés d'authentification qui permettent l'accès à toute communication radio cryptée, et l'UDR dispose de toutes les données d'approvisionnement des utilisateurs et de leurs identités, et précisément le 3GPP a inclus l'utilisation de SUCI (identité IMSI cryptée) pour empêcher cette identité de voyager via l'interface radio, car avoir un SUPI d'un utilisateur est la première étape pour toute autre attaque. Celles-ci sont sans aucun doute considérées comme les fonctions réseau les plus critiques puisque l'impact de l'obtention de clés et d'entités est durable (étant associé aux clés SIM des clients). La perte d'image d'un opérateur de réseau et de service 5G en raison d'une intrusion dans ces fonctions de réseau serait énorme et pourrait impliquer le remplacement des cartes SIM corrompues. Cependant, la conception du réseau permet de fournir le service sans aucun impact face à la double défaillance des instances de l'un de ces nœuds.

b) Criticité moyenne

Cette catégorie, de la plus haute à la plus basse criticité, comprend:

i. NRF: cet élément a une carte de l'ensemble du réseau, des nœuds et des services. Avec les informations NRF, tous les détails du déploiement du réseau, du routage, des DNN, des tranches, des services, etc. sont disponibles. En outre, l'accès non autorisé permettrait de paralyser le service 5G puisque toutes les fonctions réseau consultent cette entité pour savoir quelles fonctions réseau de destination ont le service requis. Cependant, les fonctions réseau ont les informations NRF mise en cache, ce qui atténuerait temporairement l'attaque. En outre, la conception du réseau permet de fournir le service sans aucun impact face à la double défaillance des instances de ce nœud.

ii. SEPP: permet l'échange de signalisation avec d'autres réseaux pour des scénarios d'itinérance sur le réseau d'origine ou sur d'autres réseaux tiers. C'est un élément exposé, bien que les fournisseurs 5G aient développé un grand nombre de fonctionnalités pour assurer sa sécurité et son intégrité. En outre, l'isolement entre les domaines internes et externes doit être assuré.

iii. AMF: responsable de la gestion de la mobilité. Une attaque ou un accès non autorisé à celui-ci permettrait d'obtenir des informations très sensibles (identité de l'utilisateur, localisation au niveau de la zone de suivi, et même gNB-ID de l'endroit où se trouve le client lorsque son terminal est en mode connecté), avec la possibilité de suivre le mouvement des utilisateurs, et leurs procédures de signalisation liées à la mobilité et à la gestion des sessions. Ces éléments sont déployés en mode pool et sont dimensionnés pour supporter simultanément la défaillance d'un nœud dans chaque pool.

c) Criticité faible

Dans cette catégorie, là encore, la criticité est indiquée de la plus élevée à la plus faible et concerne:

i. SMF/UPF: SMF est responsable de la gestion des sessions (établissement, modification et version), de la gestion et de l'attribution des IP aux terminaux utilisateurs, etc. Il est également responsable d'interagir avec le plan utilisateur en créant, en mettant à jour ou en supprimant des sessions PDU, ainsi que de gérer le contexte de la session avec l'UPF, tandis que l'UPF gère le plan utilisateur. Ces éléments sont beaucoup plus redondants que les AMF décrits ci-dessus, et l'accès non autorisé pourrait désactiver la session d'un utilisateur, bien que cela soit établi dans un autre SMF/UPF. Le plan utilisateur ou le trafic client réel est acheminé, en général, vers d'autres réseaux (internet/intranet) qui sont de sécurité inférieure, de sorte que la personne qui attaque un plan utilisateur a plus de facilité à compromettre le service en attaquant le serveur cible ou même le terminal.

ii. PCF: pas particulièrement critique, puisque l'AMF/SMF sont configurés pour être en mesure de fournir un service sans cet élément, affectant, à terme, la tarification en ligne des clients.

d) Non critique

Les éléments CHF, NEF, NWADF et 5G-EIR ne sont pas considérés comme critiques pour la fourniture du service 5G car, en cas de défaillance partielle ou totale ou d'indisponibilité de l'un d'entre eux, les clients ne devraient pas être affectés dans le service.

5. Identification des menaces et des risques dans la technologie 5G.

L'article 9 du décret-loi royal 7/2022 du 29 mars 2022 précise la nécessité d'identifier les facteurs de risque à analyser en fonction des évolutions technologiques, l'incorporation de nouvelles avancées technologiques, fonctionnalités et normes, la situation du marché des communications électroniques et du marché de l'approvisionnement, ainsi que l'émergence de nouvelles menaces et vulnérabilités.

Les points suivante couvrent les tâches exécutées.

### 5.1. Critères d'identification du risque d'attaque

Pour calculer le niveau de risque de sécurité qu'une menace introduit, nous utilisons trois facteurs basés sur les formules suivantes:

***Niveau de risque = (Probabilité d'occurrence) x (Impact sur le réseau)***

où:

***(Impact sur le réseau) = (Criticité de l'actif) x (Facteur d'échelle)***

Les concepts utilisés sont définis ci-dessous:

***a) Probabilité d'occurrence***: Une évaluation est effectuée sur la base des paramètres suivants:

i. *Degré d'exposition de l'actif à la vulnérabilité*: donne une mesure de la façon dont l'élément analysé est exposé à un niveau physique ou

logique, et du niveau d'accessibilité/facilité que l'attaquant peut avoir pour exécuter la menace.

ii. *Complexité ou connaissances pour développer l'attaque*: la probabilité d'occurrence augmente dans le cas où l'attaque peut être menée sans beaucoup de connaissances techniques et lorsque l'environnement d'attaque est simple à mettre en œuvre ou lorsque des outils automatisés sont utilisés.

iii. *Connaissance par le public de la vulnérabilité*: une attaque est plus probable lorsque la possibilité d'entreprendre une telle attaque est plus connue du public. Dans le cas où la vulnérabilité n'est pas largement connue ou lorsqu'elle traitée uniquement dans certains milieux (tels que les fournisseurs 5G ou les opérateurs de réseau et de services 5G), son exploitation sera moins probable.

iv. *Trace de l'attaque*: si l'attaque est menée par une force brute ou laisse des traces sur les réseaux, il est moins probable qu'il y aura des attaquants prêts à exploiter la vulnérabilité. Il s'agit de cas dans lesquels l'usurpation d'identité ne peut être utilisée.

v. *Bénéfices obtenus par le succès de l'attaque*: valeur économique, reconnaissance, pertinence, etc. de la réalisation de l'attaque.

Les valeurs possibles de la ***probabilité d'occurrence*** sont: **très élevée**, **élevée**, **moyenne**, **faible**.

***b) Impact sur le réseau***: de façon similaire à la *probabilité d'occurrence*, une évaluation qualitative est utilisée pour mesurer l'impact que l'attaque pourrait avoir sur le réseau.

Les paramètres suivants sont utilisés pour évaluer le service et donner une analyse d'impact:

i. *Criticité de l'actif*: notion mentionnée ci-dessus, qui englobe la *confidentialité*, l'*intégrité* et la *disponibilité*.

ii. *Facteur de mise à l'échelle*: identifie l'importance et/ou la portée de l'attaque au niveau de l'impact du réseau. Il prend en considération à la fois la portée (le nombre d'utilisateurs qui peuvent être touchés) et le type d'impact de l'attaque (fuite de données d'identification, diminution de la disponibilité, etc.).

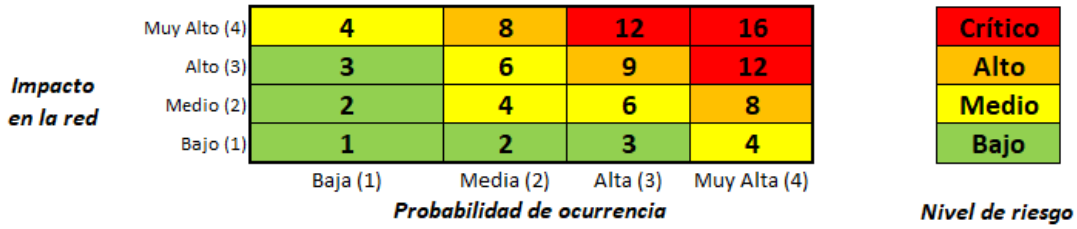
Les valeurs possibles de la criticité de l'impact sur réseau de l'attaque sont les suivantes: **très élevée, élevée**, **moyenne**, **faible**, en tenant compte des critères ci-dessus.

***c) Niveau de risque***: Il s'agit du résultat des deux variables précédentes suivant la formule décrite ci-dessus.

Les valeurs possibles de la criticité du niveau de risque sont les suivantes: **critique**, **élevée**, **moyenne**, **faible**.

### 5.2. Matrice de risque

Compte tenu des considérations du point précédent, la matrice générique qui caractérise les niveaux de risque analysés plus loin dans le présent document est présentée.




| Impacto en la red | Impact sur le réseau |
|---|---|
| Muy alto | Très élevé |
| Alto | Élevé |

| | |
|---|---|
| Medio | Moyen |
| Bajo | Faible |
| Probabilidad de ocurrencia | Probabilité d'occurrence |
| Baja | Faible |
| Media | Moyenne |
| Alta | Élevée |
| Muy alta | Très élevée |
| Nivel de riesgo | Niveau de risque |
| Crítico | Critique |
| Alto | Élevé |
| Medio | Moyen |
| Bajo | Faible |

6. Menaces ou risques dans un réseau 5G-SA.

Une fois les actifs identifiés et leur criticité caractérisée, l'étape suivante de l'analyse des risques consiste à évaluer les menaces ou les éventuelles attaques auxquelles chacun de ces actifs du réseau 5G-SA est exposé.

Il est important de souligner que la même menace peut présenter un niveau de risque différent en fonction de l'actif ou de l'environnement évalué, afin d'établir les priorités appropriées pour les actions d'atténuation qui permettent d'accroître, dans le même délai, la sécurité de la solution de la manière la plus efficace possible.

Les menaces ou les risques dans un réseau 5G-SA sont détaillés ci-dessous:

a) Activités malveillantes dues à un accès inapproprié ou malveillant à la gestion, à l'extraction d'informations sensibles ou à une modification non autorisée du paramétrage qui entraîne l'indisponibilité de l'élément.

Il s’agit des actions menées par des attaquants internes ou externes qui ciblent des éléments de réseau et d’infrastructure dans l’intention de voler des informations, de les modifier ou de détruire, par la configuration, un objectif spécifique.

Cet ensemble comprend, entre autres, les menaces suivantes:

i. Intrusions dans le réseau dans le but d’obtenir des informations, par l’accès malveillant, les mouvements latéraux, l’escalade des privilèges, en raison de l’absence de politiques de sécurité robustes (absence de contrôle d’accès, d’authentification, d’autorisation, de segmentation, de durcissement, etc.). On y distingue, entre autres, l’obtention des identifiants d’utilisateur de l’opérateur, des informations sensibles sur les clients (données, identifiants d’utilisateur et authentification, clés de chiffrement et d’intégrité), ou des informations utiles sur la configuration du réseau (ports, versions, etc.) qui servent de vecteur d’informations supplémentaires pour effectuer des attaques d’un plus grand impact.

ii. Modification malveillante et non autorisée de la configuration du réseau ou paramétrage susceptible de provoquer une indisponibilité partielle ou totale du service dans l’actif ou le réseau, ainsi que d’encourager la découverte du trafic mentionné au point précédent.

   A. Manipulation de configuration ou paramétrage qui affecte le fonctionnement de l’équipement (politiques de routage de trafic, configuration DNS, sessions utilisateur, images de fonctions réseau virtuelles, etc.).
   B. Manipulation de la configuration de sécurité de l’équipement (politiques de sécurité, services offerts dans l’application et le système d’exploitation, algorithmes cryptographiques, règles d’accès) et création de portes dérobées.
   C. Exécution intentionnelle ou involontaire de logiciels/codes malveillants (injection SQL ou XSS, rootkits, malware/ransomware, etc.).

iii. Exploitation des vulnérabilités dans le matériel ou les logiciels, qui permettent un accès simple et efficace pour pouvoir exécuter les menaces évoquées dans les deux points

précédents (les vulnérabilités connues ou CVE, les nouvelles vulnérabilités et les vulnérabilités de type «zero-day»).

b) Compromission des communications ou des données de l'utilisateur par la capture, l'interception, le détournement de trafic de service ou sa modification:

Cette catégorie comprend les actions entreprises pour écouter, interrompre ou modifier les communications ou les données de l'utilisateur dans le plan de service, sans le consentement de l'utilisateur.

Les principales menaces au sein de cette catégorie seraient les suivantes:

i. Écoute des communications d'un utilisateur donné dans des environnements à haut niveau d'exposition tels que l'accès radio ou l'interconnexion en itinérance.
ii. Obtenir des informations sensibles sur les utilisateurs (identifiants de l'utilisateur, localisation, services, etc.) dans des interfaces exposées qui peuvent être utilisées comme vecteurs d'information pour effectuer des attaques d'impact plus important.
iii. Manipulation de communications dans des interfaces exposées par le biais d'activités Man-in-the-Middle (MITM) et/ou de données utilisateur, avec des actions illégales possibles telles que la fraude, l'usurpation d'identité, etc.

c) Déni de service (DoS).

Cette catégorie comprend les actions, activités ou incidents, malveillants ou non, qui peuvent causer une perturbation totale ou partielle de l'équipement, affectant les utilisateurs du réseau. Les principales menaces au sein de cette catégorie seraient les suivantes:

i. Attaques volumétriques de déni de service (DoS/DDoS): Inondation du trafic vers les interfaces exposées des actifs (appareils utilisateurs, interconnexions, etc.) à la recherche de la surcharge des capacités des éléments, dans le but de provoquer un dysfonctionnement/une perturbation du réseau.

ii. Attaques ciblées sur des utilisateurs spécifiques dans le but de provoquer leur indisponibilité sur le réseau (par exemple, les attaques de brouillage ou la désinscription du réseau).

iii. Dommages involontaires causés par les opérateurs en raison d'erreurs de configuration: Il s'agit des actions non intentionnelles d'un opérateur ayant accès à la gestion d'un actif pouvant entraîner une défaillance ou une fonctionnalité réduite de l'actif, telles que, par exemple, une mauvaise configuration/erronée des actifs du réseau et leurs capacités de sécurité (isolation, durcissement, segmentation, etc.) ou une erreur de gestion ou de manipulation due à un manque de connaissances, de formation ou de diligence.

iv. Dysfonctionnement de l'élément: Cela inclut les dysfonctionnements «naturels» (pour des raisons allant au-delà de la configuration de l'actif) qui peuvent causer une perturbation totale ou partielle de son service.

d) Menaces physiques.

Celles-ci visent à détruire, à rendre inutilisables, à altérer ou à voler des actifs physiques de l'infrastructure physique qui héberge les fonctions/éléments du réseau.

Parmi les principales menaces figurent le sabotage ou les actes de terrorisme contre des éléments critiques de l'équipement de réseau, les catastrophes naturelles, le dysfonctionnement du réseau énergétique et le possible vol d'équipements de réseau pour l'extraction d'informations sensibles en vue de leur exploitation ultérieure.

e) Manque de formation et de sensibilisation des employés sur la cybersécurité, ainsi que des fautes professionnelles dans la gestion de l'évolution des risques identifiés.

En effet, un manque de sensibilisation à la sécurité parmi les employés augmente la probabilité de survenance d'incidents tels que des attaques de ransomwares et d'autres logiciels malveillants. Le manque de sécurité et de formation opérationnelle augmente la probabilité d'erreurs de configuration dues au manque de connaissances, ce qui expose les actifs à des risques inutiles.

En plus de tout cela, si une bonne procédure de gestion des risques n'est pas réalisée, le suivi de son évolution dans le réseau, il sera impossible de formuler un plan prioritaire et de mettre en œuvre efficacement des mesures de sécurité.

ANNEXE III

GESTION DES RISQUES AU NIVEAU NATIONAL

Une fois que les différentes menaces qui affectent les réseaux et services 5G ont été identifiées à l'annexe II, et avec cette situation de risque initiale, l'étape suivante consiste à envisager les mesures de sécurité nécessaires pour faire face, réduire ou atténuer les risques identifiés.

Ces mesures sont:

1. Mesures de sécurité génériques:

1.1. Configurations de sécurité des équipements:

1.1.1. Configurations liées à l'identification, l'authentification, le contrôle, l'audit et le suivi de l'accès aux nœuds. Les nœuds doivent être configurés avec les éléments suivants:

a) Des politiques de gestion de l'identité, permettant de garantir à la fois l'authentification (afin de vérifier que quiconque y accède est bien cette personne) et l'autorisation (un accès uniquement avec les privilèges strictement nécessaires) lors de l'accès aux nœuds.
b) Des politiques de gestion du cycle de vie de l'utilisateur.
c) Des capacités de traçabilité et les politiques d'audit permettant d'enregistrer tous les accès (qui se connecte et se déconnecte des nœuds et quand) ainsi que les commandes et alarmes exécutées qui identifient les éventuelles défaillances de l'équipement.
d) De bonnes pratiques de sécurité lors de la définition et de la gestion des identifiants d'utilisateur et de l'accès, forçant toujours les informations d'identification à être robustes.

e) La possibilité de les configurer de manière à ce qu'aucune information détaillée ne soit fournie dans le cas où l'accès échoue et que des stratégies de blocage puissent être établies, rendant difficile l'obtention d'informations d'identification.

1.1.2. Durcissement:

a) Autoprotection des nœuds, en veillant à ce que seuls les services nécessaires à leur bon fonctionnement soient actifs.
b) Les nœuds doivent avoir la capacité de séparer l'interface de gestion de l'interface de service, que ce soit par le biais d'une interface physique ou logique.
c) Les nœuds doivent être capables de détecter et de gérer les paquets mal formés tout en gardant les services intacts.
d) Les nœuds doivent être capables de faire face à des volumes/points de trafic élevés en ayant des mécanismes d'autorégulation pour empêcher leur CPU de cesser de fonctionner.
e) Capacité à protéger les données et informations stockées.
f) Les nœuds/éléments réseau doivent être configurés de telle sorte que le démarrage via des périphériques mémoire non autorisés n'est pas autorisé.
g) Les nœuds doivent être configurés de telle sorte que l'exploitation malveillante des API qu'ils exposent soit impossible.

1.1.3. Réalisation de tests de sécurité périodiques. Ceux-ci sont nécessaires pour déterminer si de nouvelles vulnérabilités sont apparues pour les composantes de l'actif.

1.2. Sécurité architecturale et fonctionnelle.

1.2.1. Différents plans de réseau, ainsi que des zones de réseau ou des environnements avec des niveaux d'exposition différents, doivent être isolés.

1.2.2. Contrôle des flux: Possibilité de limiter le trafic à certaines adresses IP, protocoles, applications, pour éviter de surcharger le lien, ce qui rend une attaque plus compliquée à effectuer.

1.3. Mesures de sécurité dans l'infrastructure physique:

a) Enregistrement, validation et contrôle des autorisations d'accès physique aux sites.

b) Contrôles physiques d'accès, par voie électronique et/ou mécanique, aux installations de réseau et aux bâtiments concernés.

c) Surveillance physique et sécurité électronique du site.

d) Systèmes de sécurité électroniques installés et entretenus.

1.4. Sensibilisation à la sécurité des employés et de la chaîne de commandement.

1.5. Formation des employés à la technologie, à la sécurité et aux processus.

1.6. Mise en œuvre de processus clairs de gestion des incidents, ayant un historique des incidents et une connaissance actualisée des incidents de l'industrie.

2. Mesures de sécurité spécifiques liées à un réseau 5G.

2.1. Contrôle logiciel:

a) Assurer l'intégrité de la mise à jour du logiciel avant son installation, en évitant l'injection d'un code malveillant, de chevaux de Troie ou de versions non légitimes (manipulées par un tiers).

b) S'assurer qu'il n'y a pas de portes dérobées.

c) S'assurer qu'il n'y a pas de vulnérabilités à haut risque (CVE) connues au moment du déploiement du produit sur site.

d) Se conformer aux certifications de sécurité internationalement reconnues pour les équipements.

2.2. Le cryptage et l'intégrité des communications entre le terminal et le réseau doivent être configurés aux niveaux AS (Access Stratum) et NAS (Non-Access Stratum) afin de protéger la confidentialité des utilisateurs dans l'interface aérienne. Cette mesure est activée à la fois dans le RAN (AS) et dans le nœud du réseau (NAS).

2.3. Le chiffrement et l'intégrité des communications du plan de contrôle et du plan utilisateur entre le nœud d'accès radio (RAN) et le réseau central doivent être configurés.

2.4. La confidentialité de l'utilisateur doit être garantie dans l'interface aérienne.

2.5. Les améliorations des algorithmes d'authentification entre le terminal de l'utilisateur et le réseau qui viennent nativement avec la technologie 5G-SA doivent être corroborées.

2.6. Améliorations natives des algorithmes d'authentification entre l'appareil de l'utilisateur et le réseau, afin de s'assurer mutuellement que la communication est légitime.

2.7. Les différents éléments qui gèrent le trafic de signalisation doivent avoir des mesures pour empêcher l'usurpation d'identité des éléments du réseau eux-mêmes dans le réseau d'itinérance, ainsi que des utilisateurs qui ne sont pas en itinérance.

2.8. La confidentialité, l'intégrité et l'authentification doivent être assurées dans les communications entre un opérateur source et un opérateur de destination, en utilisant des protocoles/équipements/solutions sécurisés (SEPP).

2.9. Il est nécessaire d'établir les politiques de sécurité correspondantes afin d'exposer dans l'interconnexion uniquement les interfaces et les messages nécessaires au service, en évitant de fournir des informations inutiles qui pourraient être utilisées frauduleusement.

2.10. Isolement des fonctions réseau virtualisées: Classification des différents éléments virtualisés dans l'infrastructure en fonction des différents niveaux d'exposition et de criticité de l'élément.

2.11. Isolement du trafic: Conception sécurisée de l'architecture de virtualisation pour garantir le trafic nécessaire au fonctionnement de la couche de virtualisation, de sorte que l'opération/le fonctionnement du réseau sera garanti.

2.12. Il est nécessaire de suivre les consignes des Exigences/Configurations/Configurations de sécurité des équipements et de sécurité architecturale pour chacun des éléments qui composent l'architecture de virtualisation.

2.13. Surveillance et détection: Surveiller la traçabilité des accès et des commandes exécutés sur des éléments critiques du réseau, afin de pouvoir identifier les activités illégitimes au moment de leur exécution et aussi pour l'analyse médico-légale d'éventuelles attaques.

2.14. Atténuation: Capacité d'atténuer les éventuelles attaques volumétriques visant le déni de service dans des interfaces très exposées.

2.15. Environnements critiques: Les tests de performance de redondance/récupération (sauvegarde) dans des environnements critiques doivent être effectués avant le déploiement de la solution.